System Validation:
Hennessy-Milner Logic

Mohammad Mousavi and Jeroen Keiren
General Overview

System Models

System Requirements

Semantic Domain

Modal Formulae

Behavior (Processes)

Behavioral Equivalences

Semantic Domain
General Overview

System Models
System Requirements
Modal Formulae
Behavior (Processes)
Semantic Domain
Motivation

**Drawbacks** of verification using behavioural equivalences:

- **Complex behaviour of specification**
Motivation

Drawbacks of verification using behavioural equivalences:

- Complex behaviour of specification
- Concise specification hard to establish
Motivation

**Drawbacks** of verification using behavioural equivalences:

- Complex behaviour of specification
- Concise specification hard to establish
- Why is specification correct?
Motivation

**Drawbacks** of verification using behavioural equivalences:

- **Complex** behaviour of specification
- **Concise** specification hard to establish
- Why is specification correct?
- Full behaviour unknown in early stages of development
Motivation

**Drawbacks** of verification using behavioural equivalences:

- Complex behaviour of specification
- Concise specification hard to establish
- Why is specification correct?
- Full behaviour unknown in early stages of development
Motivation

**Drawbacks** of verification using behavioural equivalences:
- Complex behaviour of specification
- Concise specification hard to establish
- Why is specification correct?
- Full behaviour unknown in early stages of development

**Solution**: express properties outside of behaviour
Observable Events

- Fix observable events (interactions with external world)

©Krauss (CC BY-SA 4.0)
Observable Events

- Fix observable events (interactions with external world)

- Describe temporal properties using these
Observable Events

- Fix observable events (interactions with external world)

- Describe temporal properties using these

- Verify correctness of properties with respect to some LTS

©Krauss (CC BY-SA 4.0)
Observable Events: Examples

A scientist interacts with environment

- *coffee* for taking coffee in
Observable Events: Examples

A scientist interacts with environment

- *coffee* for taking coffee in
- *coin* for producing a coin
Observable Events: Examples

A scientist interacts with environment

- *coffee* for taking coffee in
- *coin* for producing a coin
- *pub* for producing a publication
Observable Events: Examples

A scientist interacts with environment

- *coffee* for taking coffee in
- *coin* for producing a coin
- *pub* for producing a publication
- ...
Observable Events: Examples

A scientist interacts with environment

- *coffee* for taking coffee in
- *coin* for producing a coin
- *pub* for producing a publication
- ...
Observable Events: Examples

A scientist interacts with environment

- *coffee* for taking coffee in
- *coin* for producing a coin
- *pub* for producing a publication
- ...

Properties of interest

- the scientist is not willing to drink coffee now
Observable Events: Examples

A scientist interacts with environment

- coffee for taking coffee in
- coin for producing a coin
- pub for producing a publication
- ... 

Properties of interest

- the scientist is not willing to drink coffee now
- the scientist is willing to drink both coffee and tea now
Observable Events: Examples

A scientist interacts with environment

- coffee for taking coffee in
- coin for producing a coin
- pub for producing a publication
- ...

Properties of interest

- the scientist is not willing to drink coffee now
- the scientist is willing to drink both coffee and tea now
- the scientist will always produce a publication immediately after drinking two coffees in a row
For \( a \in \text{Act} \), Hennessy-Milner formulas \( \varphi, \psi \) are the following:

- **true** holds in every state
For \( a \in \text{Act} \), Hennessy-Milner formulas \( \varphi, \psi \) are the following:

- \( \text{true} \) holds in every state
- \( \text{false} \) holds nowhere
For $a \in Act$, Hennessy-Milner formulas $\varphi, \psi$ are the following:

- $true$ holds in every state
- $false$ holds nowhere
- $\neg \varphi$ holds if $\varphi$ does not hold
Hennessy-Milner logic
Syntax

For $a \in Act$, Hennessy-Milner formulas $\varphi, \psi$ are the following:

- **true** holds in every state
- **false** holds nowhere
- $\neg \varphi$ holds if $\varphi$ does not hold
- $\varphi \land \psi$ holds if both $\varphi$ and $\psi$ hold
For $a \in \text{Act}$, Hennessy-Milner formulas $\varphi, \psi$ are the following:

- $true$ holds in every state
- $false$ holds nowhere
- $\neg \varphi$ holds if $\varphi$ does not hold
- $\varphi \land \psi$ holds if both $\varphi$ and $\psi$ hold
- $\varphi \lor \psi$ holds if $\varphi$ or $\psi$ holds
For $a \in \text{Act}$, Hennessy-Milner formulas $\varphi, \psi$ are the following:

- $true$ holds in every state
- $false$ holds nowhere
- $\neg \varphi$ holds if $\varphi$ does not hold
- $\varphi \land \psi$ holds if both $\varphi$ and $\psi$ hold
- $\varphi \lor \psi$ holds if $\varphi$ or $\psi$ holds
- $\varphi \Rightarrow \psi$ holds if $\neg \varphi \lor \psi$ holds
For $a \in Act$, Hennessy-Milner formulas $\varphi, \psi$ are the following:

- $true$ holds in every state
- $false$ holds nowhere
- $\neg \varphi$ holds if $\varphi$ does not hold
- $\varphi \land \psi$ holds if both $\varphi$ and $\psi$ hold
- $\varphi \lor \psi$ holds if $\varphi$ or $\psi$ holds
- $\varphi \implies \psi$ holds if $\neg \varphi \lor \psi$ holds
- $\langle a \rangle \varphi$ holds if it is possible to perform action $a$ to a state satisfying $\varphi$
For $a \in \text{Act}$, Hennessy-Milner formulas $\varphi, \psi$ are the following:

- $true$ holds in every state
- $false$ holds nowhere
- $\neg \varphi$ holds if $\varphi$ does not hold
- $\varphi \land \psi$ holds if both $\varphi$ and $\psi$ hold
- $\varphi \lor \psi$ holds if $\varphi$ or $\psi$ holds
- $\varphi \implies \psi$ holds if $\neg \varphi \lor \psi$ holds
- $\langle a \rangle \varphi$ holds if it is possible to perform action $a$ to a state satisfying $\varphi$
- $[a] \varphi$ holds if all successors reached by performing action $a$ satisfy $\varphi$
Hennessy-Milner logic
Syntax

For $a \in \text{Act}$, Hennessy-Milner formulas $\varphi, \psi$ are the following:

- $\text{true}$ holds in every state
- $\text{false}$ holds nowhere
- $\neg \varphi$ holds if $\varphi$ does not hold
- $\varphi \land \psi$ holds if both $\varphi$ and $\psi$ hold
- $\varphi \lor \psi$ holds if $\varphi$ or $\psi$ holds
- $\varphi \implies \psi$ holds if $\neg \varphi \lor \psi$ holds
- $\langle a \rangle \varphi$ holds if it is possible to perform action $a$ to a state satisfying $\varphi$
- $[a] \varphi$ holds if all successors reached by performing action $a$ satisfy $\varphi$
Examples

- the scientist is not willing to drink coffee now
Examples

- the scientist is not willing to drink coffee now

\[ \neg \langle \text{coffee} \rangle \text{true} \]
Examples

- the scientist is not willing to drink coffee now

\[\neg \langle \text{coffee}\rangle \text{true} \quad \text{or} \quad [\text{coffee}]\text{false} \]
Examples

- the scientist is not willing to drink coffee now

\[ \neg \langle \text{coffee} \rangle \text{true} \quad \text{or} \quad [\text{coffee}] \text{false} \]

- the scientist is willing to drink both coffee and tea now
Examples

- the scientist is not willing to drink coffee now
  \[\neg \langle \text{coffee} \rangle \text{true} \quad \text{or} \quad [\text{coffee}] \text{false}\]

- the scientist is willing to drink both coffee and tea now
  \[\langle \text{coffee} \rangle \text{true} \land \langle \text{tea} \rangle \text{true}\]
Typical formulas

Let $Act = \{a, b\}$

- the process is deadlocked

$\text{false} \land \text{false}$
Typical formulas

Let $Act = \{a, b\}$

- the process is deadlocked
  
  $[a]false \land [b]false$

- the process can execute some action
  
  $\langle a \rangle true \lor \langle b \rangle true$

- $a$ must happen next
  
  $\langle a \rangle true \land [b]false$
Let $Act = \{a, b\}$

- the process is deadlocked
  
  \[ [a]false \land [b]false \]

- the process can execute some action
Typical formulas

Let $Act = \{a, b\}$

- the process is deadlocked
  
  $[a]false \land [b]false$

- the process can execute some action
  
  $\langle a \rangle true \lor \langle b \rangle true$
Typical formulas

Let $Act = \{a, b\}$

- the process is deadlocked
  \[ [a]false \land [b]false \]

- the process can execute some action
  \[ \langle a \rangle true \lor \langle b \rangle true \]

- $a$ must happen next
Typical formulas

Let $Act = \{a, b\}$

- the process is deadlocked
  \[ [a]false \land [b]false \]

- the process can execute some action
  \[ \langle a \rangle true \lor \langle b \rangle true \]

- $a$ must happen next
  \[ \langle a \rangle true \land [b]false \]
Algorithm

- Identify all subformulas
- Label states with subformulas they satisfy, starting from the smallest subformula (*true*)
Examples

Is the HML formula $\langle a \rangle \langle b \rangle true$ satisfied by the labelled transition system (i.e., by its initial state)?

Subformulas

$true$  $\langle b \rangle true$  $\langle a \rangle \langle b \rangle true$
Examples

Is the HML formula $\langle a \rangle \langle b \rangle true$ satisfied by the labelled transition system (i.e., by its initial state)?

Subformulas

$true$  $\langle b \rangle true$  $\langle a \rangle \langle b \rangle true$
Examples

Is the HML formula $\langle a \rangle \langle b \rangle \text{true}$ satisfied by the labelled transition system (i.e., by its initial state)?

Subformulas

$\text{true}$ $\langle b \rangle \text{true}$ $\langle a \rangle \langle b \rangle \text{true}$
Examples

Is the HML formula $\langle a \rangle \langle b \rangle true$ satisfied by the labelled transition system (i.e., by its initial state)?

Subformulas

$true$  $\langle b \rangle true$  $\langle a \rangle \langle b \rangle true$
Is the HML formula \([a]⟨b⟩true\) satisfied?

\[
\begin{array}{c}
S_0 \\
S_1 \\
S_2 \\
S_3
\end{array}
\]

\[
\begin{array}{c}
a \\
a \\
b
\end{array}
\]
Examples

Is the HML formula $[a]\langle b \rangle true$ satisfied?

![Diagram](attachment://hml_formula_diagram.png)
Is the HML formula \([a] \langle b \rangle true\) satisfied?
Assume $Act = \{\text{coffee}, \text{pub}\}$

- the scientist will produce a publication immediately after having drunk two coffees in a row
Restrictions

Assume $Act = \{coffee, pub\}$

- the scientist will produce a publication immediately after having drunk two coffees in a row

$$[coffee][coffee](\langle pub \rangle true \land [coffee]false)$$
Restrictions

Assume $\text{Act} = \{\text{coffee}, \text{pub}\}$

- the scientist will produce a publication immediately after having drunk two coffees in a row

\[
[\text{coffee}][\text{coffee}](⟨\text{pub}⟩\text{true} ∧ [\text{coffee}]\text{false})
\]

- the scientist will always produce a publication immediately after having drunk two coffees in a row
Assume $\text{Act} = \{\text{coffee}, \text{pub}\}$

- the scientist will produce a publication immediately after having drunk two coffees in a row

$$[\text{coffee}][\text{coffee}](\langle \text{pub} \rangle \text{true} \land [\text{coffee}] \text{false})$$

- the scientist will always produce a publication immediately after having drunk two coffees in a row not expressible in HML

Observations

There are relevant properties that cannot be expressed in HML. HML is restricted to a finite depth.
Assume $Act = \{coffee, pub\}$

- the scientist will produce a publication immediately after having drunk two coffees in a row

$$[coffee][coffee](\langle pub\rangle true \land [coffee]false)$$

- the scientist will always produce a publication immediately after having drunk two coffees in a row not expressible in HML

Observations
There are relevant properties that cannot be expressed in HML. HML is restricted to a finite depth.
Summary

- Behavioural equivalences not always suitable for verification
- Hennessy-Milner logic provides alternative way to describe properties
- Only properties of finite depth can be described
General Overview

- System Models
- System Requirements
- Modal Formulae
- Behavior (Processes)

Semantic Domain
Thank you very much.