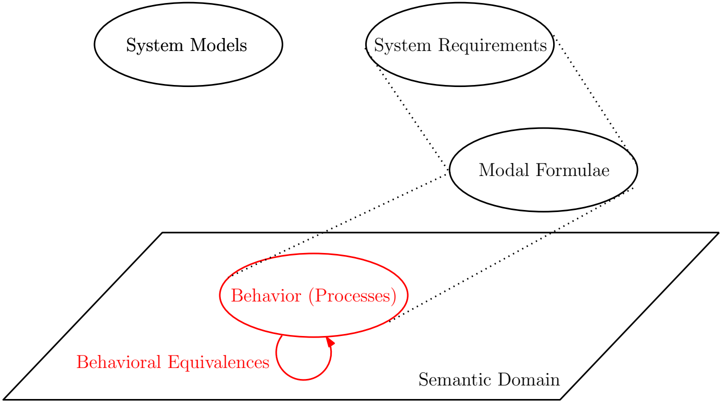
System Validation: Hennessy-Milner Logic

Mohammad Mousavi and Jeroen Keiren

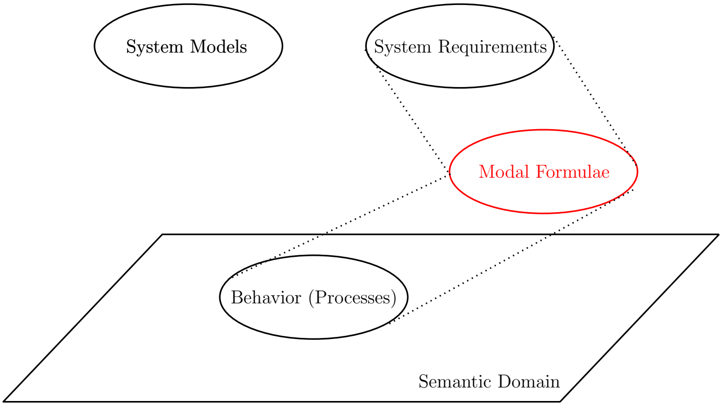
HALMSTAD UNIVERSITY

Open Universiteit

General Overview



General Overview



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)

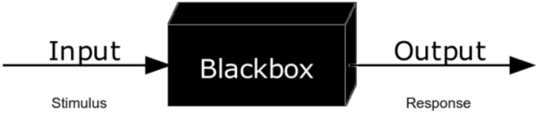
Observable Events

- 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

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 $a \in Act$, Hennessy-Milner formulas φ, ψ are the following:

true	holds in every state

Hennessy-Milner logic
Syntax

For $a \in Act$, Hennessy-Milner formulas φ, ψ are the following:

true	holds in every state
false	holds nowhere

Hennessy-Milner logic
Syntax

For $a \in Act$, Hennessy-Milner formulas φ, ψ are the following:

true	holds in every state
false	holds nowhere
$\neg\varphi$	holds if φ does not hold

For $a \in Act$, Hennessy-Milner formulas φ, ψ are the following:

true	holds in every state
false	holds nowhere
$\neg\varphi$	holds if φ does not hold
$\varphi \wedge \psi$	holds if both φ and ψ hold

For $a \in Act$, Hennessy-Milner formulas φ, ψ are the following:

true	holds in every state
false	holds nowhere
$\neg\varphi$	holds if φ does not hold
$\varphi \wedge \psi$	holds if both φ and ψ hold
$\varphi \vee \psi$	holds if φ or ψ holds

Hennessy-Milner logic
Syntax

For $a \in Act$, Hennessy-Milner formulas φ, ψ are the following:

true	holds in every state
false	holds nowhere
$\neg\varphi$	holds if φ does not hold
$\varphi \wedge \psi$	holds if both φ and ψ hold
$\varphi \vee \psi$	holds if φ or ψ holds
$\varphi \implies \psi$	holds if $\neg\varphi \vee \psi$ holds

Hennessy-Milner logic
Syntax

For $a \in Act$, Hennessy-Milner formulas φ, ψ are the following:

true	holds in every state
false	holds nowhere
$\neg\varphi$	holds if φ does not hold
$\varphi \land \psi$	holds if both φ and ψ hold
$\varphi \lor \psi$	holds if φ or ψ 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 φ

Hennessy-Milner logic
Syntax

For $a \in Act$, Hennessy-Milner formulas φ, ψ are the following:

true	holds in every state
false	holds nowhere
$\neg\varphi$	holds if φ does not hold
$\varphi \wedge \psi$	holds if both φ and ψ hold
$\varphi \vee \psi$	holds if φ or ψ holds
$\varphi \implies \psi$	holds if $\neg\varphi \vee \psi$ holds
$\langle a \rangle\varphi$	holds if it is possible to perform action a to a state satisfying φ
$[a]\varphi$	holds if all successors reached by performing action a satisfy φ

For $a \in Act$, Hennessy-Milner formulas φ, ψ are the following:

true	holds in every state
false	holds nowhere
$\neg\varphi$	holds if φ does not hold
$\varphi \wedge \psi$	holds if both φ and ψ hold
$\varphi \vee \psi$	holds if φ or ψ holds
$\varphi \implies \psi$	holds if $\neg\varphi \vee \psi$ holds
$\langle a \rangle \varphi$	holds if it is possible to perform action a to a state satisfying φ
$[a]\varphi$	holds if all successors reached by performing action a satisfy φ

Examples

- the scientist is not willing to drink coffee now

Examples

- the scientist is not willing to drink coffee now

$$\neg \langle \mathit{coffee} \rangle \mathit{true}$$

Examples

- the scientist is not willing to drink coffee now

$$\neg\langle \mathit{coffee}\rangle \mathit{true} \qquad \text{or} \qquad [\mathit{coffee}]\mathit{false}$$

Examples

- the scientist is not willing to drink coffee now

$$\neg\langle \mathit{coffee}\rangle \mathit{true} \qquad \text{or} \qquad [\mathit{coffee}]\mathit{false}$$

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

Examples

- the scientist is not willing to drink coffee now

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

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

$$\langle coffee\rangle true \wedge \langle tea\rangle true$$

Typical formulas

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

- the process is deadlocked

Typical formulas

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

- the process is deadlocked

$$[a]\mathit{false} \wedge [b]\mathit{false}$$

Typical formulas

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

- the process is deadlocked

$$[a]false \wedge [b]false$$

- the process can execute some action

Typical formulas

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

- the process is deadlocked

$$[a]\mathit{false} \wedge [b]\mathit{false}$$

- the process can execute some action

$$\langle a \rangle \mathit{true} \vee \langle b \rangle \mathit{true}$$

Typical formulas

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

- the process is deadlocked

$$[a]\mathit{false} \wedge [b]\mathit{false}$$

- the process can execute some action

$$\langle a \rangle \mathit{true} \vee \langle b \rangle \mathit{true}$$

- a must happen next

Typical formulas

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

- the process is deadlocked

$$[a]false \wedge [b]false$$

- the process can execute some action

$$\langle a \rangle true \vee \langle b \rangle true$$

- a must happen next

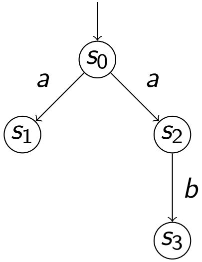
$$\langle a \rangle true \wedge [b]false$$

Algorithm

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

Examples

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

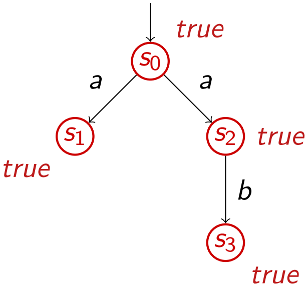


Subformulas

true $\quad \langle b \rangle \mathit{true}$ $\quad \langle a \rangle \langle b \rangle \mathit{true}$

Examples

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

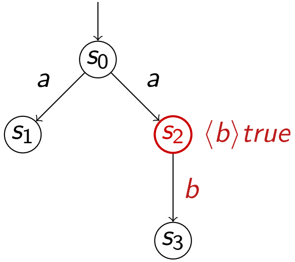


Subformulas

$true$ $\quad \langle b \rangle true$ $\quad \langle a \rangle \langle b \rangle true$

Examples

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

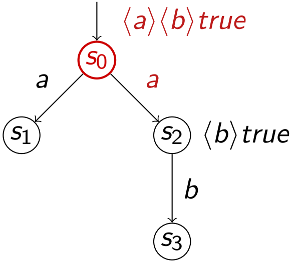


Subformulas

$true \qquad \langle b \rangle true \qquad \langle a \rangle \langle b \rangle true$

Examples

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

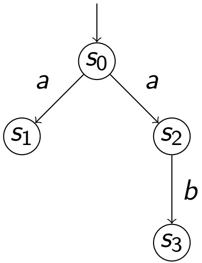


Subformulas

$true \qquad \langle b \rangle true \qquad \langle a \rangle \langle b \rangle true$

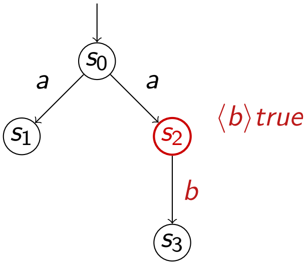
Examples

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



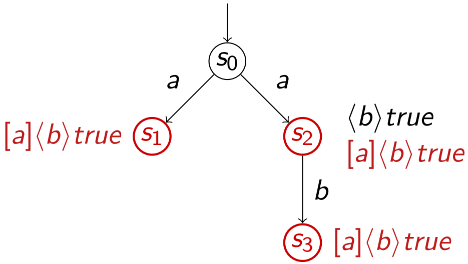
Examples

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



Examples

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



Restrictions

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

- 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

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

Restrictions

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

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

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

- the scientist will always 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

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

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

Restrictions

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

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

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

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

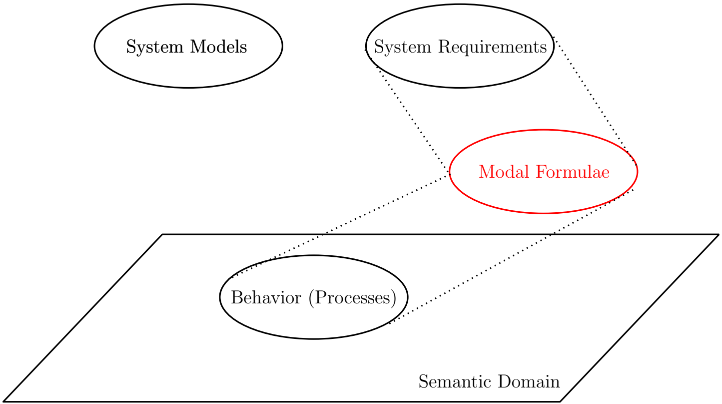
Observations

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



Thank you very much.