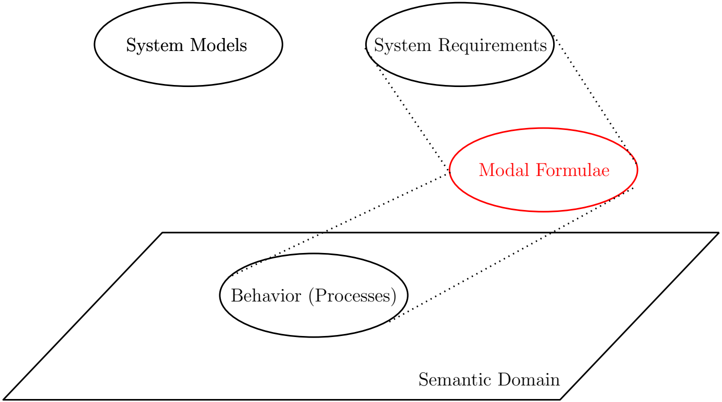
System Validation: Modal μ-calculus

Mohammad Mousavi and Jeroen Keiren

HALMSTAD UNIVERSITY

Open Universiteit

General Overview



Limitations of Regural Hennessy-Milner Logic

Using regular HML we cannot express some intuitive properties:

- all computations inevitably reach a state which satisfies φ
- for some execution φ holds everywhere

Modal μ-calculus

Extend syntax of regular HML with fixed points:

$$\begin{array}{l} \mathit{true} \\ \mathit{false} \\ \neg\varphi \\ \varphi \wedge \psi \\ \varphi \vee \psi \\ \varphi \implies \psi \\ \langle\beta\rangle\varphi \\ [\beta]\varphi \end{array}$$

Modal μ-calculus

Extend syntax of regular HML with fixed points:

true	
false	
$\neg\varphi$	
$\varphi \wedge \psi$	
$\varphi \vee \psi$	
$\varphi \implies \psi$	
$\langle\beta\rangle\varphi$	
$[\beta]\varphi$	
X	a variable representing a set of states
$\mu X.\varphi$	the least set of states satisfying $X = \varphi$
$\nu X.\varphi$	the greatest set of states satisfying $X = \varphi$

X may only appear under even number of negations

Modal μ-calculus: Equation

Examples

Any set of states T satisfies the set-equation $X = X$

- $\mu X.X$ is the least such set, $\emptyset$
- $\nu X.X$ is the largest such set, S

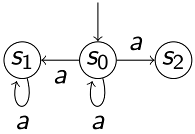
Example

A state can be reached where a cannot be executed:

Example

A state can be reached where *a* cannot be executed:

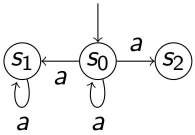
$$\{\mu, \nu\}X.[a]false \vee \langle true \rangle X$$



Example

A state can be reached where a cannot be executed:

$$\{\mu, \nu\}X.[a]\mathit{false} \vee \langle \mathit{true} \rangle X$$



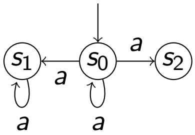
Solutions:

- $\mu X.[a]\mathit{false} \vee \langle \mathit{true} \rangle X$: $\{s_0, s_2\}$

Example

A state can be reached where a cannot be executed:

$$\{\mu, \nu\}X.[a]\mathit{false} \vee \langle \mathit{true} \rangle X$$



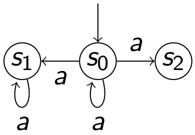
Solutions:

- $\mu X.[a]\mathit{false} \vee \langle \mathit{true} \rangle X$: $\{s_0, s_2\}$
- $\nu X.[a]\mathit{false} \vee \langle \mathit{true} \rangle X$: $\{s_0, s_1, s_2\}$

Example

A state can be reached where a cannot be executed:

$$\{\mu, \nu\}X.[a]\mathit{false} \vee \langle \mathit{true} \rangle X$$



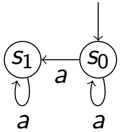
Solutions:

- $\mu X.[a]\mathit{false} \vee \langle \mathit{true} \rangle X$

Example

A state can be reached where *a* cannot be executed:

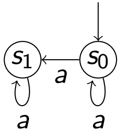
$$\mu X.[a]\mathit{false} \vee \langle \mathit{true} \rangle X$$



Example

A state can be reached where a cannot be executed:

$$\mu X.[a]\mathit{false} \vee \langle \mathit{true} \rangle X$$

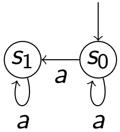


Unique least solution for this equation is $\emptyset$

Example

A state can be reached where *a* cannot be executed:

$$\mu X.[a]\mathit{false} \vee \langle \mathit{true} \rangle X$$



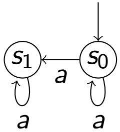
Unique least solution for this equation is $\emptyset$

Property does not hold in the LTS

Example

A state can be reached where *a* cannot be executed:

$$\mu X.[a]false \vee \langle true \rangle X$$



Unique least solution for this equation is $\emptyset$

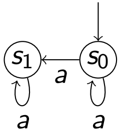
Property does not hold in the LTS

Note: this property is equivalent to $\langle true^* \rangle [a] false$

Example

There is an infinite path along which an *a*-transition is always possible

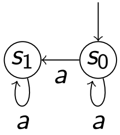
$$\{\mu, \nu\} X . \langle a \rangle true \wedge \langle true \rangle X$$



Example

There is an infinite path along which an a-transition is always possible

$$\{\mu, \nu\}X.\langle a\rangle true \wedge \langle true\rangle X$$

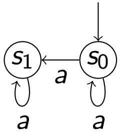


Three solutions to $X = \langle a\rangle true \wedge \langle true\rangle X$:
$\{s_0\}$, $\{s_1\}$, and $\{s_0, s_1\}$

Example

There is an infinite path along which an *a*-transition is always possible

$$\{\mu, \nu\}X.\langle a\rangle \mathit{true} \wedge \langle \mathit{true}\rangle X$$



Three solutions to $X = \langle a\rangle \mathit{true} \wedge \langle \mathit{true}\rangle X$:
$\{s_0\}$, $\{s_1\}$, and $\{s_0, s_1\}$

We intended to describe the greatest solution!

$$\nu X.\langle a\rangle \mathit{true} \wedge \langle \mathit{true}\rangle X$$

Some temporal properties

- *Safe*(φ): for some execution φ holds everywhere

$$\nu X.\varphi \wedge ([\mathit{true}]\mathit{false} \vee \langle \mathit{true} \rangle X)$$

Some temporal properties

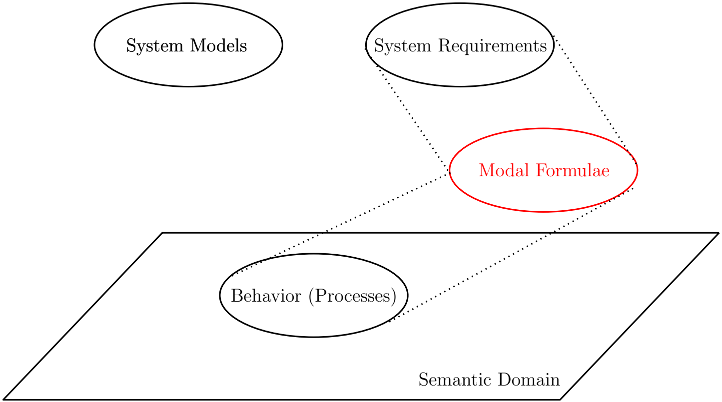
- *Safe*(φ): for some execution φ holds everywhere

$$\nu X.\varphi \wedge ([\mathit{true}]\mathit{false} \vee \langle \mathit{true} \rangle X)$$

- *Even*(φ): eventually φ will hold (in every execution)

$$\mu X.\varphi \vee (\langle \mathit{true} \rangle \mathit{true} \wedge [\mathit{true}]X)$$

General Overview



Thank you very much.