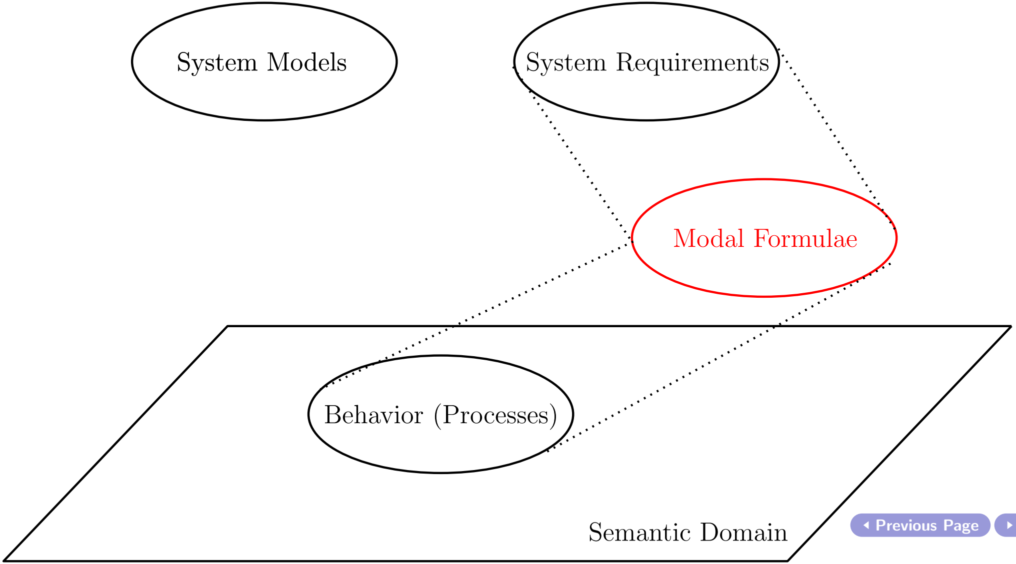
System Validation: Extensions of Hennessy-Milner Logic

Mohammad Mousavi and Jeroen Keiren

General Overview



Limitations of Hennessy-Milner Logic

- Properties like "the system is deadlocked" require reasoning about all actions
- Properties of infinite depth cannot be expressed, for example:

Limitations of Hennessy-Milner Logic

- Properties like "the system is deadlocked" require reasoning about all actions
- Properties of infinite depth cannot be expressed, for example:
  - all reachable states satisfy φ

$$Inv(\varphi) = \varphi \wedge [true]\varphi \wedge [true][true]\varphi \wedge \cdots$$

Limitations of Hennessy-Milner Logic

- Properties like "the system is deadlocked" require reasoning about all actions
- Properties of infinite depth cannot be expressed, for example:
  - all reachable states satisfy φ

$$Inv(\varphi) = \varphi \wedge [true]\varphi \wedge [true][true]\varphi \wedge \cdots$$

  - there is a reachable state which satisfies φ

$$Pos(\varphi) = \varphi \vee \langle true\rangle\varphi \vee \langle true\rangle\langle true\rangle\varphi \vee \cdots$$

Extending HML to Sets of Actions

For $A = \{a_1, \cdots, a_n\} \subseteq Act$ with $n \geq 1$

- $\langle A \rangle \varphi$ denotes $\langle a_1 \rangle \varphi \vee \cdots \vee \langle a_n \rangle \varphi$ and $\langle \emptyset \rangle \varphi = \mathit{false}$

Extending HML to Sets of Actions

For $A = \{a_1, \cdots, a_n\} \subseteq Act$ with $n \geq 1$

- $\langle A \rangle \varphi$ denotes $\langle a_1 \rangle \varphi \vee \cdots \vee \langle a_n \rangle \varphi$ and $\langle \emptyset \rangle \varphi = \mathit{false}$
- $[A]\varphi$ denotes $[a_1]\varphi \wedge \cdots \wedge [a_n]\varphi$ and $[\emptyset]\varphi = \mathit{true}$

Action formula

A described using the following syntax ($a \in Act$):

$$A, B ::= \mathit{false} \mid \mathit{true} \mid a \mid \overline{A} \mid A \cup B \mid A \cap B$$

where $\overline{A} = Act \setminus A$, *true* matches all actions, *false* matches no action.

Typical Formulas

- the process is deadlocked

Typical Formulas

- the process is deadlocked

$$[true]false$$

Typical Formulas

- the process is deadlocked

$$[\mathit{true}]\mathit{false}$$

- the process can execute some action

Typical Formulas

- the process is deadlocked

$$[\mathit{true}]\mathit{false}$$

- the process can execute some action

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

Typical Formulas

- the process is deadlocked

$$[true]false$$

- the process can execute some action

$$\langle true \rangle true$$

- a must happen next

Typical Formulas

- the process is deadlocked

$$[\mathit{true}]\mathit{false}$$

- the process can execute some action

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

- a must happen next

$$\langle a \rangle \mathit{true} \wedge [\overline{a}]\mathit{false}$$

Typical Formulas

- the process is deadlocked

$$[\mathit{true}]\mathit{false}$$

- the process can execute some action

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

- a must happen next

$$\langle a \rangle \mathit{true} \wedge [\overline{a}]\mathit{false}$$

- φ holds after every step

Typical Formulas

- the process is deadlocked

$$[\mathit{true}]\mathit{false}$$

- the process can execute some action

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

- a must happen next

$$\langle a \rangle \mathit{true} \wedge [\overline{a}]\mathit{false}$$

- φ holds after every step

$$[\mathit{true}]\varphi \wedge \langle \mathit{true} \rangle \mathit{true}$$

Regular Hennessy-Milner Logic

Idea: use regular expressions inside modalities

- $\langle \varepsilon \rangle \varphi = [\varepsilon] = \varphi$

Regular Hennessy-Milner Logic

Idea: use regular expressions inside modalities

- $\langle \varepsilon \rangle \varphi = [\varepsilon] = \varphi$
- $\langle \beta_1 \cdot \beta_2 \rangle \varphi = \langle \beta_1 \rangle \langle \beta_2 \rangle \varphi$
- $[\beta_1 \cdot \beta_2] \varphi = [\beta_1][\beta_2] \varphi$

Regular Hennessy-Milner Logic

Idea: use regular expressions inside modalities

- $\langle \varepsilon \rangle \varphi = [\varepsilon] = \varphi$
- $\langle \beta_1 \cdot \beta_2 \rangle \varphi = \langle \beta_1 \rangle \langle \beta_2 \rangle \varphi$
- $[\beta_1 \cdot \beta_2] \varphi = [\beta_1][\beta_2] \varphi$
- $\langle \beta_1 + \beta_2 \rangle \varphi = \langle \beta_1 \rangle \varphi \vee \langle \beta_2 \rangle \varphi$
- $[\beta_1 + \beta_2] \varphi = [\beta_1] \varphi \wedge [\beta_2] \varphi$

Regular Hennessy-Milner Logic

Idea: use regular expressions inside modalities

- $\langle\varepsilon\rangle\varphi = [\varepsilon] = \varphi$
- $\langle\beta_1 \cdot \beta_2\rangle\varphi = \langle\beta_1\rangle\langle\beta_2\rangle\varphi$
- $[\beta_1 \cdot \beta_2]\varphi = [\beta_1][\beta_2]\varphi$
- $\langle\beta_1 + \beta_2\rangle\varphi = \langle\beta_1\rangle\varphi \vee \langle\beta_2\rangle\varphi$
- $[\beta_1 + \beta_2]\varphi = [\beta_1]\varphi \wedge [\beta_2]\varphi$
- $\langle\beta_1^*\rangle\varphi = \varphi \vee \langle\beta_1\rangle\langle\beta_1^*\rangle\varphi$

Regular Hennessy-Milner Logic

Idea: use regular expressions inside modalities

- $\langle \varepsilon \rangle \varphi = [\varepsilon] = \varphi$
- $\langle \beta_1 \cdot \beta_2 \rangle \varphi = \langle \beta_1 \rangle \langle \beta_2 \rangle \varphi$
- $[\beta_1 \cdot \beta_2] \varphi = [\beta_1][\beta_2] \varphi$
- $\langle \beta_1 + \beta_2 \rangle \varphi = \langle \beta_1 \rangle \varphi \vee \langle \beta_2 \rangle \varphi$
- $[\beta_1 + \beta_2] \varphi = [\beta_1] \varphi \wedge [\beta_2] \varphi$
- $\langle \beta_1^* \rangle \varphi = \varphi \vee \langle \beta_1 \rangle \langle \beta_1^* \rangle \varphi$
- $[\beta_1^*] \varphi = \varphi \wedge [\beta_1][\beta_1^*] \varphi$

Limitations of HML revisited

Formulas for properties that cannot be expressed in HML

- the scientist always produces a publication after drinking two coffees in a row

$$[\mathit{true}^* \cdot \mathit{coffee} \cdot \mathit{coffee}](\langle \mathit{pub} \rangle \mathit{true} \wedge [\overline{\mathit{pub}}]\mathit{false})$$

Limitations of HML revisited

Formulas for properties that cannot be expressed in HML

- the scientist always produces a publication after drinking two coffees in a row

$$[\mathit{true}^* \cdot \mathit{coffee} \cdot \mathit{coffee}](\langle \mathit{pub} \rangle \mathit{true} \wedge [\overline{\mathit{pub}}]\mathit{false})$$

- the scientist never drinks beer

$$[\mathit{true}^* \cdot \mathit{beer}]\mathit{false}$$

Limitations of HML revisited

Formulas for properties that cannot be expressed in HML

- the scientist always produces a publication after drinking two coffees in a row

$$[\mathit{true}^* \cdot \mathit{coffee} \cdot \mathit{coffee}](\langle \mathit{pub} \rangle \mathit{true} \wedge [\overline{\mathit{pub}}]\mathit{false})$$

- the scientist never drinks beer

$$[\mathit{true}^* \cdot \mathit{beer}]\mathit{false}$$

- $\mathit{Inv}(\varphi)$

$$[\mathit{true}^*]\varphi$$

Limitations of HML revisited

Formulas for properties that cannot be expressed in HML

- the scientist always produces a publication after drinking two coffees in a row

$$[\mathit{true}^* \cdot \mathit{coffee} \cdot \mathit{coffee}](\langle \mathit{pub} \rangle \mathit{true} \wedge [\overline{\mathit{pub}}]\mathit{false})$$

- the scientist never drinks beer

$$[\mathit{true}^* \cdot \mathit{beer}]\mathit{false}$$

- $\mathit{Inv}(\varphi)$

$$[\mathit{true}^*]\varphi$$

- $\mathit{Pos}(\varphi)$

$$\langle \mathit{true}^* \rangle \varphi$$

Limitations of regular HML

Using regular HML we still cannot express some intuitive properties:

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

Limitations of regular HML

Using regular HML we still cannot express some intuitive properties:

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

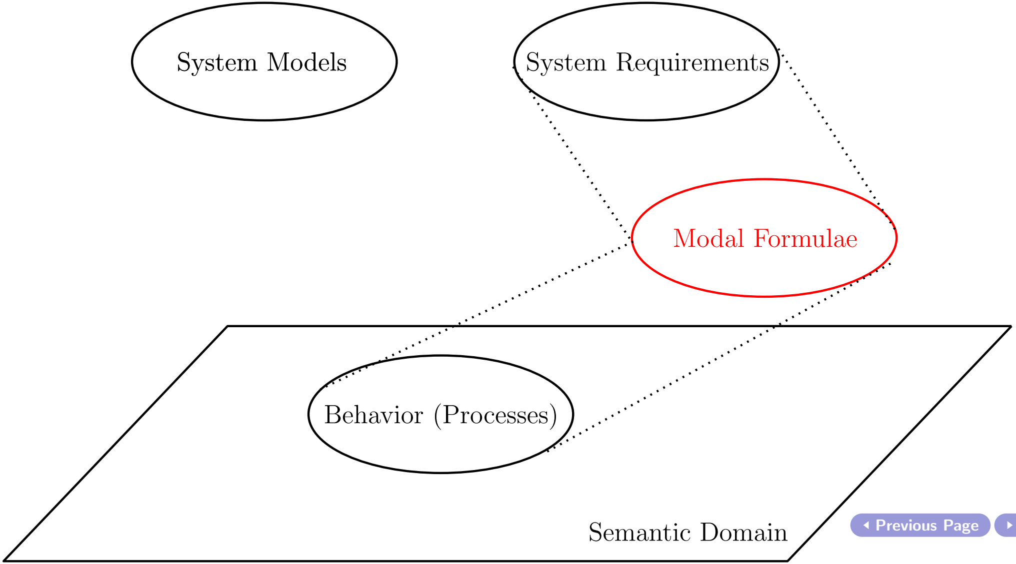
Why not use recursion?

- $\mathit{Inev}(\varphi)$ expressed by $X \stackrel{\text{def}}{=} \varphi \vee [\mathit{true}]X$
- $\mathit{Safe}(\varphi)$ expressed by $X \stackrel{\text{def}}{=} \varphi \wedge \langle \mathit{true} \rangle X$

Summary

- Allowing sets inside modalities $\implies$ more compact formulas
- Regular HML allows describing properties of infinite depth
- Some desirable properties cannot be described using regular HML

General Overview



Thank you very much.