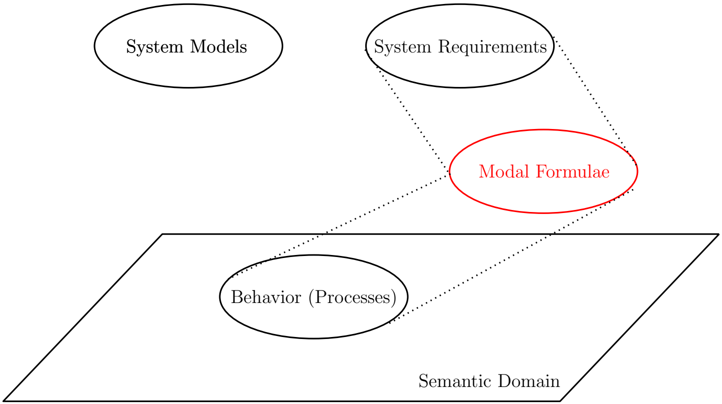
System Validation: Modal μ-calculus Semantics

Mohammad Mousavi and Jeroen Keiren

HALMSTAD UNIVERSITY

Open Universiteit

General Overview



Modal μ-calculus

Some properties for which we need the μ-calculus:

- For some execution φ holds everywhere

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

Modal μ-calculus

Some properties for which we need the μ-calculus:

- For some execution φ holds everywhere

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

- Eventually φ will hold (in every execution)

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

Semantics of μ-calculus
Environment

- With each formula associate a set of states for which it is satisfied
$$[\![\varphi]\!] \subseteq S$$

Semantics of μ-calculus
Environment

- With each formula associate a set of states for which it is satisfied
$$[\![\varphi]\!] \subseteq S$$
- How to deal with recursion variable X?

Semantics of μ-calculus
Environment

- With each formula associate a set of states for which it is satisfied

$$[\![\varphi]\!] \subseteq S$$

- How to deal with recursion variable X?
- Make an assumption on states satisfying X, record assumption in environment $\eta\colon \mathrm{X} \to 2^S$.

Semantics of μ-calculus
Environment

- With each formula associate a set of states for which it is satisfied
$$[\![\varphi]\!] \subseteq S$$
- How to deal with recursion variable X?
- Make an assumption on states satisfying X, record assumption in environment $\eta\colon \mathsf{X} \to 2^S$.
- $\eta[X := T](X) = T$, $\eta[X := T](Y) = \eta(Y)$ if $X \neq Y$

- With each formula associate a set of states for which it is satisfied
$$[\![\varphi]\!] \subseteq S$$
- How to deal with recursion variable X?
- Make an assumption on states satisfying X, record assumption in environment $\eta \colon \mathsf{X} \to 2^S$.
- $\eta[X := T](X) = T$, $\eta[X := T](Y) = \eta(Y)$ if $X \neq Y$
- Use this assumption to compute solution

Semantics of formula

$[\![\varphi]\!]_L^\eta$ is set of states satisfying φ in environment η. Similar

to semantics of HML, but:

Semantics of formula

$[\![\varphi]\!]^{\eta}_{L}$ is set of states satisfying φ in environment η. Similar

to semantics of HML, but:

$$[\![X]\!]^{\eta}_{L} = \eta(X)$$

Semantics of formula

$[\![\varphi]\!]_L^\eta$ is set of states satisfying φ in environment η. Similar

to semantics of HML, but:

$$
\begin{aligned}
[\![X]\!]_L^\eta &= \eta(X) \\
[\![\mu X.\varphi]\!]_L^\eta &= \mu T \subseteq S.\Phi_\eta(T)
\end{aligned}
$$

Semantics of formula

$[\![\varphi]\!]^{\eta}_{L}$ is set of states satisfying φ in environment η. Similar

to semantics of HML, but:

$$
\begin{aligned}
[\![X]\!]^{\eta}_{L} &= \eta(X) \\
[\![\mu X.\varphi]\!]^{\eta}_{L} &= \mu T \subseteq S.\Phi_{\eta}(T) \\
[\![\nu X.\varphi]\!]^{\eta}_{L} &= \nu T \subseteq S.\Phi_{\eta}(T)
\end{aligned}
$$

Semantics of formula

$[\![\varphi]\!]_L^\eta$ is set of states satisfying φ in environment η. Similar

to semantics of HML, but:

$$
\begin{aligned}
[\![X]\!]_L^\eta &= \eta(X) \\
[\![\mu X.\varphi]\!]_L^\eta &= \mu T \subseteq S.\Phi_\eta(T) \\
[\![\nu X.\varphi]\!]_L^\eta &= \nu T \subseteq S.\Phi_\eta(T)
\end{aligned}
$$

$\Phi_\eta(T) = [\![\varphi]\!]_L^{\eta[X:=T]}$

Semantics of recursion

$$\Phi_\eta(T) = [\![\varphi]\!]_L^{\eta[X:=T]}$$

Semantics of recursion

$\Phi_\eta(T) = [\![\varphi]\!]_L^{\eta[X:=T]}$

Observe

- monotonic $(U \subseteq V \implies \Phi_\eta(U) \subseteq \Phi_\eta(V))$
- S finite

Semantics of recursion

$\Phi_\eta(T) = [\![\varphi]\!]_L^{\eta[X:=T]}$

Observe

- monotonic $(U \subseteq V \implies \Phi_\eta(U) \subseteq \Phi_\eta(V))$
- S finite

Therefore (Knaster-Tarski):

$$[\![\mu X.\varphi]\!]_L^\eta = \bigcup_i \Phi_\eta^i(\emptyset)$$

$$[\![\nu X.\varphi]\!]_L^\eta = \bigcap_i \Phi_\eta^i(S)$$

Computing fixed points

Due to Knaster-Tarski, use fixed point iteration

- $\Phi_\eta(T) = [\![\varphi]\!]_L^{\eta[X:=T]}$

Computing fixed points

Due to Knaster-Tarski, use fixed point iteration

- $\Phi_\eta(T) = [\![\varphi]\!]_L^{\eta[X:=T]}$
- $\Phi^0(T) = T$

Computing fixed points

Due to Knaster-Tarski, use fixed point iteration

- $\Phi_\eta(T) = [\![\varphi]\!]_L^{\eta[X:=T]}$
- $\Phi^0(T) = T$
- $\Phi^{n+1} = \Phi(\Phi^n(T))$

Computing fixed points

Due to Knaster-Tarski, use fixed point iteration

- $\Phi_\eta(T) = [\![\varphi]\!]_L^{\eta[X:=T]}$
- $\Phi^0(T) = T$
- $\Phi^{n+1} = \Phi(\Phi^n(T))$
- there exists m s.t. $\Phi^{m+1}(T) = \Phi^m(T)$

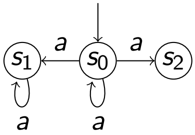
Computing fixed points

Due to Knaster-Tarski, use fixed point iteration

- $\Phi_\eta(T) = [\![\varphi]\!]_L^{\eta[X:=T]}$
- $\Phi^0(T) = T$
- $\Phi^{n+1} = \Phi(\Phi^n(T))$
- there exists m s.t. $\Phi^{m+1}(T) = \Phi^m(T)$
- For μ, start with $T = \emptyset$, for ν start with $T = S$; iterate until m is found

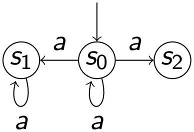
Example

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



Example

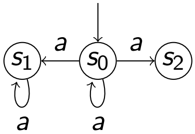
$$\mu X.[a]\mathit{false} \vee \langle \mathit{true} \rangle X$$



$$\Phi(T) = [\![[a]\mathit{false} \vee \langle \mathit{true} \rangle]\!]^{\eta[X:=T]}$$

Example

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

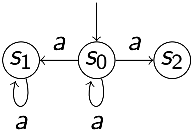


$$\Phi(T) = [\![[a]\mathit{false} \vee \langle \mathit{true} \rangle]\!]^{\eta[X:=T]}$$

$$\Phi^0(\emptyset) = \emptyset$$

Example

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

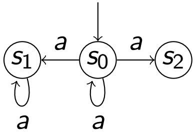


$$\Phi(T) = [\![[a]\mathit{false} \vee \langle \mathit{true} \rangle]\!]^{\eta[X:=T]}$$

$$\begin{aligned}
\Phi^0(\emptyset) &= \emptyset \\
\Phi^1(\emptyset) &= [\![[a]\mathit{false} \vee \langle \mathit{true} \rangle]\!]^{\eta[X:=\emptyset]} \\
&= [\![[a]\mathit{false}]\!]^{\eta[X:=\emptyset]} \cup [\![\langle \mathit{true} \rangle X]\!]^{\eta[X:=\emptyset]} \\
&= \{s_2\} \cup \emptyset \\
&= \{s_2\}
\end{aligned}$$

Example

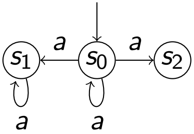
$$\mu X.[a]\mathit{false} \vee \langle \mathit{true}\rangle X$$



$$
\begin{aligned}
\Phi(T) &= [\![[a]\mathit{false} \vee \langle \mathit{true}\rangle]\!]^{\eta[X:=T]} \\
\Phi^1(\emptyset) &= \{s_2\} \\
\Phi^2(\emptyset) &= [\![[a]\mathit{false} \vee \langle \mathit{true}\rangle]\!]^{\eta[X:=\{s_2\}]} \\
&= [\![[a]\mathit{false}]\!]^{\eta[X:=\{s_2\}]} \cup [\![\langle \mathit{true}\rangle X]\!]^{\eta[X:=\{s_2\}]} \\
&= \{s_2\} \cup \{s_0\} \\
&= \{s_0, s_2\}
\end{aligned}
$$

Example

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



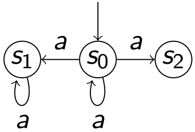
$$\Phi(T) = [\![[a]\mathit{false} \vee \langle \mathit{true} \rangle]\!]^{\eta[X:=T]}$$

$$\Phi^2(\emptyset) = \{s_0, s_2\}$$

$$\begin{aligned}
\Phi^3(\emptyset) &= [\![[a]\mathit{false} \vee \langle \mathit{true} \rangle]\!]^{\eta[X:=X^2]} \\
&= [\![[a]\mathit{false}]\!]^{\eta[X:=X^2]} \cup [\![\langle \mathit{true} \rangle X]\!]^{\eta[X:=X^2]} \\
&= \{s_2\} \cup \{s_0\} \qquad\qquad = \{s_0, s_2\} \\
&= \Phi^2(\emptyset)
\end{aligned}$$

Example

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

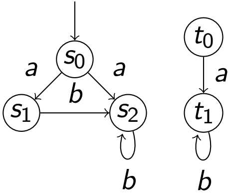


$$\Phi(T) = [\![[a]\mathit{false} \vee \langle \mathit{true} \rangle]\!]^{\eta[X:=T]}$$

$$\Phi^2(\emptyset) = \{s_0, s_2\}$$
$$\Phi^3(\emptyset) = \Phi^2(\emptyset)$$

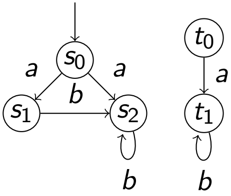
Example

$\nu X . \langle b \rangle true \wedge [b]X$



Example

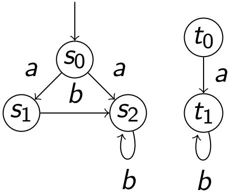
$\nu X.\langle b\rangle true \wedge [b]X$



$\Phi(T) = \langle b\rangle true \wedge [b]X$

Example

$\nu X.\langle b\rangle true \wedge [b]X$

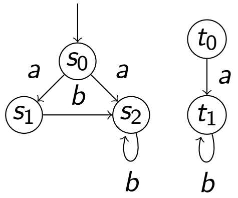


$\Phi(T) = \langle b\rangle true \wedge [b]X$

$$\Phi^0(S) = S$$

Example

$\nu X.\langle b\rangle \mathit{true} \wedge [b]X$

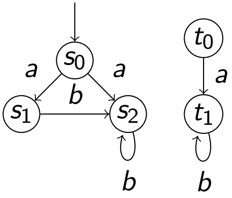


$$\Phi(T) = \langle b\rangle \mathit{true} \wedge [b]X$$

$$\begin{aligned}
\Phi^0(S) &= S \\
\Phi^1(S) &= [\![\langle b\rangle \mathit{true} \wedge [b]X]\!]^{\eta[X:=S]} \\
&= [\![\langle b\rangle \mathit{true}]\!]^{\eta[X:=S]} \cap [\![[b]X]\!]^{\eta[X:=S]} \\
&= \{s_1, s_2, t_1\} \cap \{s_0, s_1, s_2, t_0, t_1\} \\
&= \{s_1, s_2, t_1\}
\end{aligned}$$

Example

$\nu X.\langle b\rangle true \wedge [b]X$



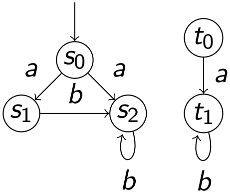
$\Phi(T) = \langle b\rangle true \wedge [b]X$

$$\Phi^1(S) = \{s_1, s_2, t_1\}$$

$$\Phi^2(S) = \ldots = [\![\langle b\rangle true]\!]^{\eta[X:=\{s_1,s_2,t_1\}]} \cap [\![[b]X]\!]^{\eta[X:=\{s_1,s_2,t_1\}]}$$
$$= \{s_1, s_2, t_1\} \cap \{s_0, s_1, s_2, t_0, t_1\}$$

Example

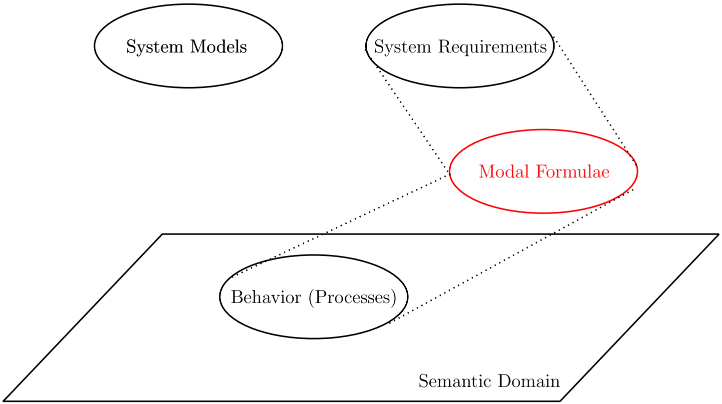
$\nu X.\langle b\rangle true \wedge [b]X$



$\Phi(T) = \langle b\rangle true \wedge [b]X$

$$\Phi^1(S) = \{s_1, s_2, t_1\}$$
$$\Phi^2(S) = \Phi^1(S)$$

General Overview



Thank you very much.