About Timed Modal Specifications

N. Bertrand[1], S. Pinchinat[1], J.-B. Raclet[2]

[1]INRIA Rennes Bretagne Atlantique – France

[2]INRIA Grenoble Rhône-Alpes – France

COMBEST Meeting – March 3rd 2009

Outline

Outline

Modal specifications: Definition

Modal specification (MS)

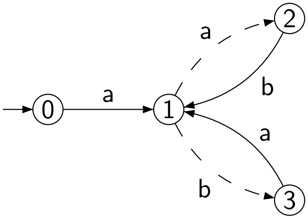
A MS is a structure $\mathcal{R} = (P, p^0, Act, \Delta^m, \Delta^M)$ where:

- P set of states, and p^0 initial state;
- Act set of actions;
- $\Delta^m, \Delta^M \subseteq Q \times \Sigma \times Q$ sets of transitions s.t. $\Delta^M \subseteq \Delta^m$, and Δ^m, Δ^M deterministic.
  - Δ^m: *may*-transitions representing the allowed transitions.
  - Δ^M: *must*-transitions representing the required transitions.

Notations:

- $may(p) = \{a \in Act \mid (p, a, p') \in \Delta^m\}$;
- $must(p) = \{a \in Act \mid (p, a, p') \in \Delta^M\}$.

Example



Models of MS

Models of MS

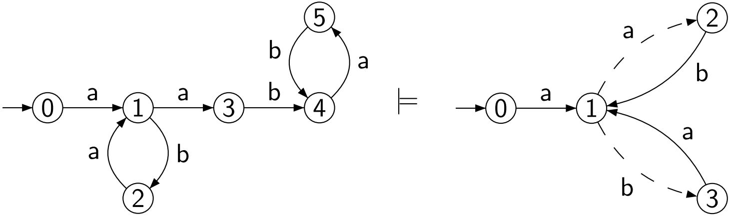
$\mathcal{M} = (M, m^0, Act, \Delta)$ is a model of a MS $\mathcal{R} = (P, p^0, Act, \Delta^m, \Delta^M)$, noted $\mathcal{M} \models \mathcal{R}$, if $\exists \rho \subseteq (M \times P)$ s.t. $(m^0, p^0) \in \rho$, and $\forall (m, p) \in \rho$:

- $p \xrightarrow{a} p' \in \Delta^M \Rightarrow m \xrightarrow{a} m' \in \Delta$ and $(m', p') \in \rho$;
- $m \xrightarrow{a} m' \in \Delta \Rightarrow p \xrightarrow{a} p' \in \Delta^m$ and $(m', p') \in \rho$.

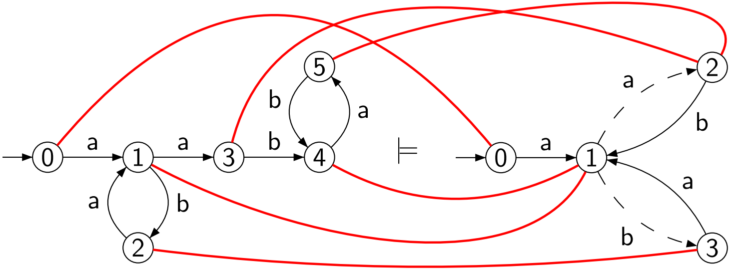
Let $out(m) = \{a \in Act \mid (m, a, m') \in \Delta\}$:

$$(m, p) \in \rho \Rightarrow must(p) \subseteq out(m) \subseteq may(p)$$

Example



Example



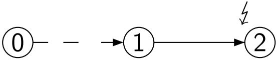
Pseudo-modal specifications pMS

- To represent inconsistencies between spec., we let $\Delta^M \nsubseteq \Delta^m$ be possible. $\Rightarrow$ *pseudo-modal specifications* pMS.

Inconsistent state

A state p s.t. $a \in must(p)$ but $a \notin may(p)$ is said *inconsistent*: $\lightning q$.

- An inconsistent state p can't belong to a ρ stating $\models$
  (ie. be a state s.t. $must(p) \subseteq out(m) \subseteq may(p)$).
- Reduction: θ : pMS $\rightarrow$ MS



Reduction preserves Mod

$\mathrm{Mod}(p\mathcal{R}) = \mathrm{Mod}(\theta(p\mathcal{R}))$

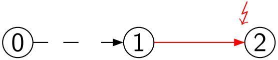
Pseudo-modal specifications pMS

- To represent inconsistencies between spec., we let $\Delta^M \not\subseteq \Delta^m$ be possible. $\Rightarrow$ *pseudo-modal specifications* pMS.

Inconsistent state

A state p s.t. $a \in must(p)$ but $a \notin may(p)$ is said *inconsistent*: $\lightning q$.

- An inconsistent state p can't belong to a ρ stating $\models$ (ie. be a state s.t. $must(p) \subseteq out(m) \subseteq may(p)$).
- Reduction: θ : pMS $\longrightarrow$ MS



Reduction preserves Mod

$\mathrm{Mod}(p\mathcal{R}) = \mathrm{Mod}(\theta(p\mathcal{R}))$

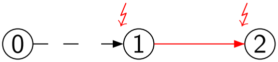
Pseudo-modal specifications pMS

- To represent inconsistencies between spec., we let $\Delta^M \not\subseteq \Delta^m$ be possible. $\Rightarrow$ *pseudo-modal specifications* pMS.

Inconsistent state

A state p s.t. $a \in must(p)$ but $a \notin may(p)$ is said *inconsistent*: $\lightning q$.

- An inconsistent state p can't belong to a ρ stating $\models$
  (ie. be a state s.t. $must(p) \subseteq out(m) \subseteq may(p)$).
- Reduction: $\theta : \mathrm{pMS} \rightarrow \mathrm{MS}$



Reduction preserves Mod

$\mathrm{Mod}(p\mathcal{R}) = \mathrm{Mod}(\theta(p\mathcal{R}))$

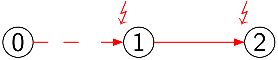
Pseudo-modal specifications pMS

- To represent inconsistencies between spec., we let $\Delta^M \not\subseteq \Delta^m$ be possible. $\Rightarrow$ *pseudo-modal specifications* pMS.

Inconsistent state

A state p s.t. $a \in must(p)$ but $a \notin may(p)$ is said *inconsistent*: $\lightning q$.

- An inconsistent state p can't belong to a ρ stating $\models$ (ie. be a state s.t. $must(p) \subseteq out(m) \subseteq may(p)$).
- Reduction: $\theta : \text{pMS} \rightarrow \text{MS}$



Reduction preserves Mod

$\text{Mod}(p\mathcal{R}) = \text{Mod}(\theta(p\mathcal{R}))$

Pseudo-modal specifications pMS

- To represent inconsistencies between spec., we let $\Delta^M \nsubseteq \Delta^m$ be possible. $\Rightarrow$ *pseudo-modal specifications* pMS.

Inconsistent state

A state p s.t. $a \in must(p)$ but $a \notin may(p)$ is said *inconsistent*: $\lightning q$.

- An inconsistent state p can't belong to a ρ stating $\models$
  (ie. be a state s.t. $must(p) \subseteq out(m) \subseteq may(p)$).
- Reduction: θ : pMS $\rightarrow$ MS

0

Reduction preserves Mod

$\text{Mod}(p\mathcal{R}) = \text{Mod}(\theta(p\mathcal{R}))$

Refinement of MS

Refinement of MS

A MS $\mathcal{R}_1 = (P_1, p_1^0, Act, \Delta_1^m, \Delta_1^M)$ is a refinement of a MS $\mathcal{R}_2 = (P_2, p_2^0, Act, \Delta_2^m, \Delta_2^M)$, noted $\mathcal{R}_1 \preceq \mathcal{R}_2$, if $\exists \rho \subseteq (P_1 \times P_2)$ s.t. $(p_1^0, p_2^0) \in \rho$, and $\forall (p_1, p_2) \in \rho$:

- $p_2 \xrightarrow{a} p_2' \in \Delta_2^M \Rightarrow p_1 \xrightarrow{a} p_1' \in \Delta_1^M$ and $(p_1', p_2') \in \rho$;
- $p_1 \xrightarrow{a} p_1' \in \Delta_1^m \Rightarrow p_2 \xrightarrow{a} p_2' \in \Delta_2^m$ and $(p_1', p_2') \in \rho$.

$(p_1, p_2) \in \rho \Rightarrow must(p_1) \supseteq must(p_2)$ and $may(p_1) \subseteq may(p_2)$.

Refinement is sound and complete

- Given two pMS $p\mathcal{R}_1$ and $p\mathcal{R}_2$:

$$\mathrm{Mod}(p\mathcal{R}_1) \subseteq \mathrm{Mod}(p\mathcal{R}_2) \Leftrightarrow \theta(p\mathcal{R}_1) \preceq \theta(p\mathcal{R}_2)$$

- Given two MS $\mathcal{R}_1$ and $\mathcal{R}_2$:

$$\mathrm{Mod}(\mathcal{R}_1) \subseteq \mathrm{Mod}(\mathcal{R}_2) \Leftrightarrow \mathcal{R}_1 \preceq \mathcal{R}_2$$

Consistency of MS

Conjunction of MS

$\mathcal{R}_1 \& \mathcal{R}_2$ is the pMS $(P_1 \times P_2, (p_1^0, p_2^0), Act, \Delta^m, \Delta^M)$ with:

$\rightsquigarrow_1 \& \rightsquigarrow_2$	$\dashrightarrow$	$\longrightarrow$	$\not\rightarrow$
$\dashrightarrow$	$\dashrightarrow$	$\longrightarrow$	$\not\rightarrow$
$\longrightarrow$	$\longrightarrow$	$\longrightarrow$	$\lightning$
$\not\rightarrow$	$\not\rightarrow$	$\lightning$	$\not\rightarrow$

Let $\mathcal{R}_1 \wedge \mathcal{R}_2 = \theta(\mathcal{R}_1 \& \mathcal{R}_2)$.

$$\begin{cases} may(\mathcal{R}_1 \& \mathcal{R}_2)(p_1, p_2) = may(\mathcal{R}_1)(p_1) \cap may(\mathcal{R}_2)(p_2) \\ must(\mathcal{R}_1 \& \mathcal{R}_2)(p_1, p_2) = must(\mathcal{R}_1)(p_1) \cup must(\mathcal{R}_2)(p_2) \end{cases}$$

Properties of $\wedge$

- $\mathcal{R}_1 \wedge \mathcal{R}_2$ is the glb of $\mathcal{R}_1$ and $\mathcal{R}_2$ for $\preceq$.
- $\mathrm{Mod}(\mathcal{R}_1 \wedge \mathcal{R}_2) = \mathrm{Mod}(\mathcal{R}_1) \cap \mathrm{Mod}(\mathcal{R}_2)$.

$\longrightarrow$ Application in an interface theory: consistency of viewpoints.

Product of MS

Product of MS

$\mathcal{R}_1 \otimes \mathcal{R}_2$ is the MS $(P_1 \times P_2, (p_1^0, p_2^0), Act, \Delta^m, \Delta^M)$ with:

$\rightsquigarrow_1 \otimes \rightsquigarrow_2$	$\dashrightarrow$	$\longrightarrow$	$\not\rightarrow$
$\dashrightarrow$	$\dashrightarrow$	$\dashrightarrow$	$\not\rightarrow$
$\longrightarrow$	$\dashrightarrow$	$\longrightarrow$	$\not\rightarrow$
$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$

$$\begin{cases} may(\mathcal{R}_1 \otimes \mathcal{R}_2)(p_1, p_2) = may(\mathcal{R}_1)(p_1) \cap may(\mathcal{R}_2)(p_2) \\ must(\mathcal{R}_1 \otimes \mathcal{R}_2)(p_1, p_2) = must(\mathcal{R}_1)(p_1) \cap must(\mathcal{R}_2)(p_2) \end{cases}$$

Properties of the product

- $\mathcal{M}_i \models \mathcal{R}_i \Longrightarrow \mathcal{M}_1 \otimes \mathcal{M}_2 \models \mathcal{R}_1 \otimes \mathcal{R}_2$;
- $(\mathcal{R}_1 \preceq \mathcal{R}_2 \text{ and } \mathcal{R}_1' \preceq \mathcal{R}_2') \Longrightarrow \mathcal{R}_1 \otimes \mathcal{R}_1' \preceq \mathcal{R}_2 \otimes \mathcal{R}_2'$.

Quotient of MS

Quotient of MS

$\mathcal{R}_1 /\!\!/ \mathcal{R}_2$ is the pMS $((P_1 \times P_2) \cup \{\top\}, (p_1^0, p_2^0), Act, \Delta^m, \Delta^M)$ with:

$\rightsquigarrow_1 /\!\!/ \rightsquigarrow_2$	$\dashrightarrow$	$\longrightarrow$	$\not\longrightarrow$
$\dashrightarrow$	$\dashrightarrow$	$\dashrightarrow$	$\dashrightarrow \top$
$\longrightarrow$	$\lightning$	$\longrightarrow$	$\lightning$
$\not\longrightarrow$	$\not\longrightarrow$	$\not\longrightarrow$	$\dashrightarrow \top$

and, $may(\top) = Act$, $must(\top) = \emptyset$.
Let $\mathcal{R}_1 / \mathcal{R}_2 = \theta(\mathcal{R}_1 /\!\!/ \mathcal{R}_2)$.

Properties of the quotient

- $\mathcal{R}_1 \otimes \mathcal{R}_2 \preceq \mathcal{R} \Leftrightarrow \mathcal{R}_2 \preceq \mathcal{R}/\mathcal{R}_1$
- $\mathcal{M}_2 \models \mathcal{R}/\mathcal{R}_1 \Leftrightarrow \forall \mathcal{M}_1 . \mathcal{M}_1 \models \mathcal{R}_1 \Rightarrow \mathcal{M}_1 \otimes \mathcal{M}_2 \models \mathcal{R}$.

$\longrightarrow$ Application in an interface theory: contract-based design

Outline

Towards a timed version of modal specifications

- Timing of the events cannot be constrained
- Goal: extend this algebraic framework to a timing setting
  $\Rightarrow$ *Timed modal specifications*
  - Generalize modal specifications
  - Generalize timed automata

Related work

- *Karlis Cerans, Jens Chr. Godskesen, Kim Guldstrand Larsen:* Timed Modal Specification - Theory and Tools. (CAV 1993).
  - Timed CCS (durations) + modalities
  - Several types of refinement relations are studied
- *Luca de Alfaro, Thomas A. Henzinger, Mariëlle Stoelinga:* Timed Interfaces. (EMSOFT 2002).
  - Semantic in terms of timed games
  - Reactivity (deadlock-freeness) is studied

Outline

Definition of timed modal specifications

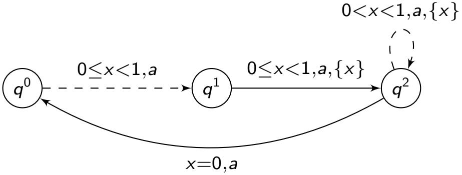
$\longrightarrow$ Timed automata equipped with may and must transitions.

Timed modal specification (TMS)

A TMS is a structure $\mathcal{S} = (Q, q^0, \mathcal{X}, \Sigma, \delta^m, \delta^M)$ where

- Q set of states, and $q^0 \in Q$ initial state;
- $\mathcal{X}$ set of clocks, Σ alphabet of actions;
- $\delta^m, \delta^M \subseteq Q \times \xi[\mathcal{X}] \times \Sigma \times 2^{\mathcal{X}} \times Q$ sets of transitions s.t. $\delta^M \subseteq \delta^m$, and δ^m, δ^M deterministic.
  - δ^m: *may*-transitions representing the allowed transitions.
  - δ^M: *must*-transitions representing the required transitions.

A basic example



Outline

Semantics of timed modal specifications

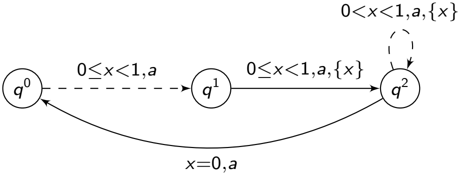
$\longrightarrow$ Collection of (infinite state) timed automata.

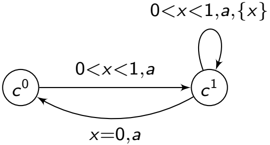
Models of TMS

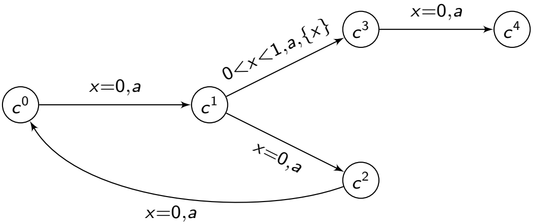
Let $\mathcal{C} = (C, c^0, \mathcal{X}, \Sigma, \delta)$ be a TA and $\mathcal{S} = (Q, q^0, \mathcal{X}, \Sigma, \delta^m, \delta^M)$ be a TMS.
$\mathcal{C} \models \mathcal{S}$ if $\exists \rho \subseteq C \times Q$ with $(c^0, q^0) \in \rho$, and for all $(c, q) \in \rho$:

- Any must-transition of $\mathcal{S}$ appears in $\mathcal{C}$, potentially split
  $\forall q \xrightarrow{g,a,r} q' \in \delta^M$, $\exists c_1 \cdots c_n \in C$, $\exists g_1, \cdots, g_n \in \xi[\mathcal{X}]$ with
  - $g \subseteq \bigcup_{i=1}^n g_i$,
  - $c \xrightarrow{g_i,a,r} c_i \in \delta$, $\forall 1 \leq i \leq n$, and
  - $(c_i, q') \in \rho$, $\forall 1 \leq i \leq n$.
- Any transition in $\mathcal{C}$, is allowed in $\mathcal{S}$
  $\forall c \xrightarrow{g,a,r} c' \in \delta$, $\exists q' \in Q$, $\exists g' \in \xi[\mathcal{X}]$ with
  - $g \subseteq g'$,
  - $q \overset{g,a,r}{\dashrightarrow} q' \in \delta^m$, and
  - $(c', q') \in \rho$.

Back to the example







Outline

1. Introduction
   - Modal specifications
   - Motivations for timed modal specifications
2. Preliminaries on Timed modal specifications
   - Definition
   - Semantics
3. Operators on Timed modal specifications
   - Refinement
   - Consistency
   - Product and quotient
4. Conclusion

Refinement of TMS

$\longrightarrow$ inherited from refinement of MS via region graph

Refinement preorder on TMS

$\mathcal{S}_1 \preceq \mathcal{S}_2$ whenever $R(\mathcal{S}_1) \preceq R(\mathcal{S}_2)$.

For any $\mathcal{C}$ TA and $\mathcal{S}$ TMS, $\mathcal{C} \models \mathcal{S}$ if and only if $\mathcal{C} \preceq \mathcal{S}$.

Decidability and characterization

Given $\mathcal{S}_1$ and $\mathcal{S}_2$, one can decide whether $\mathcal{S}_1 \preceq \mathcal{S}_2$.
Moreover $\mathcal{S}_1 \preceq \mathcal{S}_2$ if and only if $\mathrm{Mod}(\mathcal{S}_1) \subseteq \mathrm{Mod}(\mathcal{S}_2)$.

Note that for any TMS $\mathcal{S}$, $\mathcal{S}_\perp \preceq \mathcal{S} \preceq \mathcal{S}_\top$.

Outline

1. Introduction
   - Modal specifications
   - Motivations for timed modal specifications
2. Preliminaries on Timed modal specifications
   - Definition
   - Semantics
3. Operators on Timed modal specifications
   - Refinement
   - Consistency
   - Product and quotient
4. Conclusion

Consistency of TMS

$\mathcal{S}_1$ and $\mathcal{S}_2$ consistent = they share a common model
$\longrightarrow$ inherited from consistency of MS via region graph

Conjunction on TMS

$\mathcal{S}_1 \wedge \mathcal{S}_2 = T(R(\mathcal{S}_1) \wedge R(\mathcal{S}_2))$

Properties of $\wedge$

$\mathcal{S}_1 \wedge \mathcal{S}_2$ is the glb of $\mathcal{S}_1$ and $\mathcal{S}_2$ for $\preceq$.
$\mathsf{Mod}(\mathcal{S}_1 \wedge \mathcal{S}_2) = \mathsf{Mod}(\mathcal{S}_1) \cap \mathsf{Mod}(\mathcal{S}_2)$.

Outline

1. Introduction
   - Modal specifications
   - Motivations for timed modal specifications
2. Preliminaries on Timed modal specifications
   - Definition
   - Semantics
3. Operators on Timed modal specifications
   - Refinement
   - Consistency
   - Product and quotient
4. Conclusion

Product of TMS

Product

$\mathcal{S}_1 \otimes \mathcal{S}_2$ is a TMS over $\mathcal{X}_1 \uplus \mathcal{X}_2$ where:

$$(q_1 \xrightarrow{g_1,a,r_1}_1 q_1' \text{ and } q_2 \xrightarrow{g_2,a,r_2}_2 q_2') \Longrightarrow (q_1, q_2) \xrightarrow{g_1 \wedge g_2, a, r_1 \cup r_2} (q_1', q_2').$$

The modalities are derived according to the untimed case.

$\rightsquigarrow_1 \otimes \rightsquigarrow_2$	$\dashrightarrow$	$\longrightarrow$	$\nrightarrow$
$\dashrightarrow$	$\dashrightarrow$	$\dashrightarrow$	$\nrightarrow$
$\longrightarrow$	$\dashrightarrow$	$\longrightarrow$	$\nrightarrow$
$\nrightarrow$	$\nrightarrow$	$\nrightarrow$	$\nrightarrow$

Properties of the product

- $\mathcal{C}_i \models \mathcal{S}_i \Longrightarrow \mathcal{C}_1 \otimes \mathcal{C}_2 \models \mathcal{S}_1 \otimes \mathcal{S}_2$;
- $(\mathcal{S}_1 \preceq \mathcal{S}_2 \text{ and } \mathcal{S}_1' \preceq \mathcal{S}_2') \Longrightarrow \mathcal{S}_1 \otimes \mathcal{S}_1' \preceq \mathcal{S}_2 \otimes \mathcal{S}_2'$.

Quotient of TMS

Quotient - naive definition

$\mathcal{S}/\mathcal{S}_1$ is a TMS over $\mathcal{X} \setminus \mathcal{X}_1$ where:

$(q \xrightarrow{g,a,r} q'$ and $q_1 \xrightarrow{g_1,a,r_1} q_1') \Longrightarrow (q, q_1) \xrightarrow{g_1 \Rightarrow g, a, r \setminus r_1} (q', q_1')$.

Subtleties

- $g_1 \Rightarrow g$ is not a guard over $\mathcal{X}_2 = \mathcal{X} \setminus \mathcal{X}_1$. It is replaced by $g_{|\mathcal{X}_2}$.
- $r \setminus r_1$ is not necessarily included in $\mathcal{X}_2$. So we rather deal with $r_{|\mathcal{X}_2}$.

Quotient

$\mathcal{S}/\mathcal{S}_1$ is a TMS over $\mathcal{X}_2 = \mathcal{X} \setminus \mathcal{X}_1$ where:

$(q \xrightarrow{g,a,r} q'$ and $q_1 \xrightarrow{g_1,a,r_1} q_1') \Longrightarrow (q, q_1) \xrightarrow{g_{|\mathcal{X}_2}, a, r_{|\mathcal{X}_2}} (q', q_1')$.

Properties of the quotient

$(\mathcal{S}/\mathcal{S}_1) \otimes \mathcal{S}_1 \preceq \mathcal{S}$

Note: $\mathcal{S}/\mathcal{S}_1$ might be nondeterministic!

Outline

Conclusion

- Recap:
  - definition of timed modal specifications
  - decidability of refinement and consistency
  - notions of product and quotient

- Future works:
  - Relation with timed interfaces
  - Reactivity (deadlock-freeness) and refinement