

# Refinement and Consistency of Timed Modal Specifications

N. Bertrand<sup>1</sup>, S. Pinchinat<sup>2</sup>, J.-B. Raclet<sup>3</sup>

<sup>1</sup>INRIA Rennes Bretagne Atlantique – France

<sup>2</sup>Université de Rennes 1 – France

<sup>3</sup>INRIA Grenoble Rhône-Alpes – France

Supported by COMBEST (IST STREP 215543)

# 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
- 4 Conclusion

# 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
- 4 Conclusion

# Modal specifications: Definition

## Modal specification (MS)

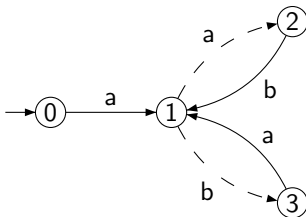
A MS is a structure  $\mathcal{R} = (P, p^0, Act, \Delta^m, \Delta^M)$  where:

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



- ▶ must transitions: plain arrows
- ▶ may transitions: dashed arrows

# Models of MS

## Models of MS

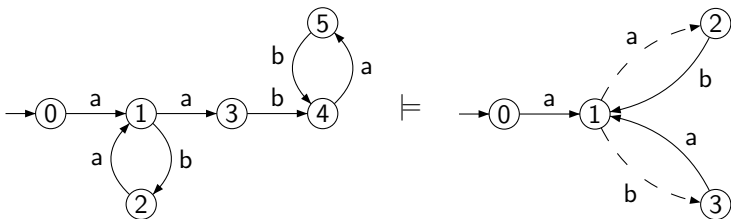
$\mathcal{M} = (M, m^0, Act, \Delta)$  is a model of a MS  $\mathcal{R} = (P, p^0, Act, \Delta^m, \Delta^M)$ , noted  $\mathcal{M} \models \mathcal{R}$ , if  $\exists \rho \subseteq (M \times P)$  s.t.  $(m^0, p^0) \in \rho$ , and  $\forall (m, p) \in \rho$ :

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

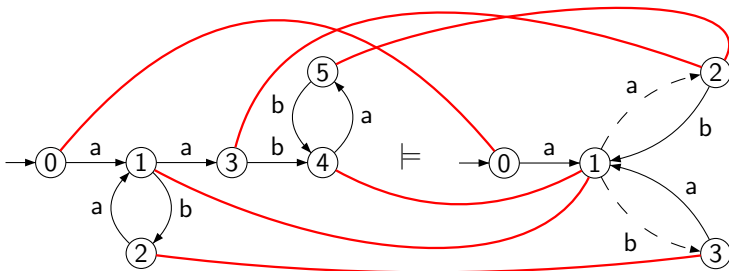
Let  $out(m) = \{a \in Act \mid (m, a, m') \in \Delta\}$ :

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

# Example



# Example



# 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  $(p'_1, p'_2) \in \rho$ .

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

## Refinement is sound and complete

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

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

# Consistency of MS

## Conjunction of MS

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

$\rightsquigarrow_1 \wedge \rightsquigarrow_2$	$-\!\!\rightarrow$	$\rightarrow$	$\nrightarrow$
$-\!\!\rightarrow$	$-\!\!\rightarrow$	$\rightarrow$	$\nrightarrow$
$\rightarrow$	$\rightarrow$	$\rightarrow$	$\downarrow$
$\nrightarrow$	$\nrightarrow$	$\downarrow$	$\nrightarrow$

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

## Properties of $\wedge$

- ▶  $\mathcal{R}_1 \wedge \mathcal{R}_2$  is the greatest lower bound of  $\mathcal{R}_1$  and  $\mathcal{R}_2$  for  $\preceq$ .
- ▶  $\text{Mod}(\mathcal{R}_1 \wedge \mathcal{R}_2) = \text{Mod}(\mathcal{R}_1) \cap \text{Mod}(\mathcal{R}_2)$ .

→ Application in 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:

$\rightsquigarrow_1 \otimes \rightsquigarrow_2$	$---$	$\rightarrow$	$\nrightarrow$
$---$	$---$	$---$	$\nrightarrow$
$\rightarrow$	$---$	$\rightarrow$	$\nrightarrow$
$\nrightarrow$	$\nrightarrow$	$\nrightarrow$	$\nrightarrow$

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

## Properties of the product

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

# Quotient of MS

## Quotient of MS

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

$\rightsquigarrow_1 / \rightsquigarrow_2$	$\dashrightarrow$	$\rightarrow$	$\nrightarrow$
$\dashrightarrow$	$\dashrightarrow$	$\dashrightarrow$	$\dashrightarrow \top$
$\rightarrow$	$\downarrow$	$\rightarrow$	$\downarrow$
$\nrightarrow$	$\nrightarrow$	$\nrightarrow$	$\dashrightarrow \top$

where,  $may(\top) = Act$ ,  $must(\top) = \emptyset$ .

## Properties of the quotient

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

→ Application in interface theory: contract-based design

# Recap on modal specifications

## Relations and operators on MS

- ▶ refinement (inclusion of models)
- ▶ consistency (consistency of viewpoints in interface theory)
- ▶ product (composition of specifications)
- ▶ quotient (contract-based design in interface theory)

→ Incremental design of component-based systems

**Reference** *Jean-Baptiste Raclet, Eric Badouel, Albert Benveniste, Benoît Caillaud, Roberto Passerone*

Why are modalities good for Interface Theories? (ACSD 2009)

# 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
- 4 Conclusion

# Towards a timed version of modal specifications

- ▶ Timing of the events cannot be constrained
- ▶ Goal: extend this algebraic framework to a timing setting  
⇒ *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)
  - ▶ Semantics in terms of timed games
  - ▶ Reactivity (deadlock-freeness) is studied

# 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
- 4 Conclusion

# Definition of timed modal specifications

→ Timed automata equipped with may and must transitions.

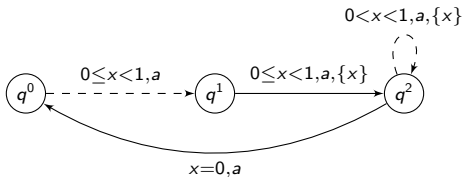
## Timed modal specification (TMS)

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

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

# A basic example

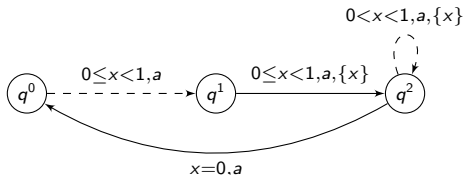
A timed modal specification  $\mathcal{S}$



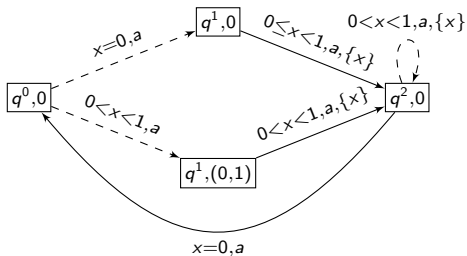


# A basic example

A timed modal specification  $\mathcal{S}$



and its region automaton  $R(\mathcal{S})$



$R(\mathcal{S})$  can be seen as:

- ▶ a MS over  $\hat{\Sigma} := \text{Reg} \times \Sigma \times 2^{\mathcal{X}}$ ,
- ▶ a TMS over  $\Sigma$ .

# 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
- 4 Conclusion

# Semantics of timed modal specifications

→ Collection of (infinite-state) timed automata.

## Models of TMS

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

$\forall q \xrightarrow{g, a, r} q' \in \delta^M, \exists g_1, \dots, g_n \in \xi[\mathcal{X}], \exists c_1 \dots c_n \in C$  with

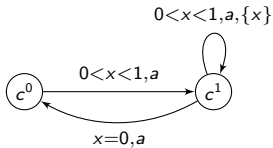
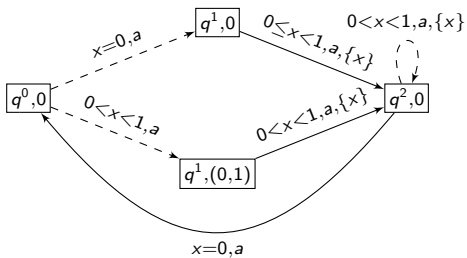
- ▶  $g \subseteq \bigcup g_i,$
- ▶  $c \xrightarrow{g_i, a, r} c_i \in \delta,$
- ▶  $(c_i, q') \in \rho.$

- ▶ Any transition in  $\mathcal{C}$ , is allowed in  $\mathcal{S}$

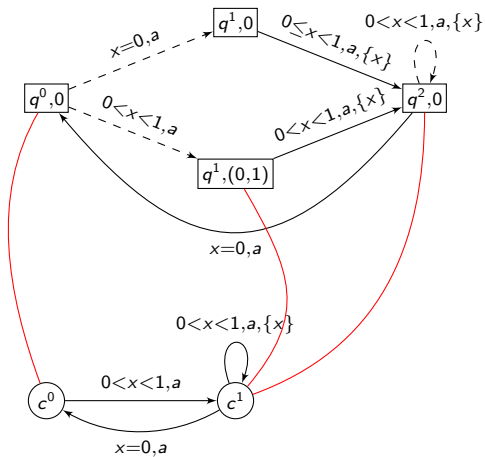
$\forall c \xrightarrow{g, a, r} c' \in \delta, \exists g' \in \xi[\mathcal{X}], \exists q' \in Q$  with

- ▶  $g \subseteq g',$
- ▶  $q \xrightarrow{g', a, r} q' \in \delta^m,$
- ▶  $(c', q') \in \rho.$

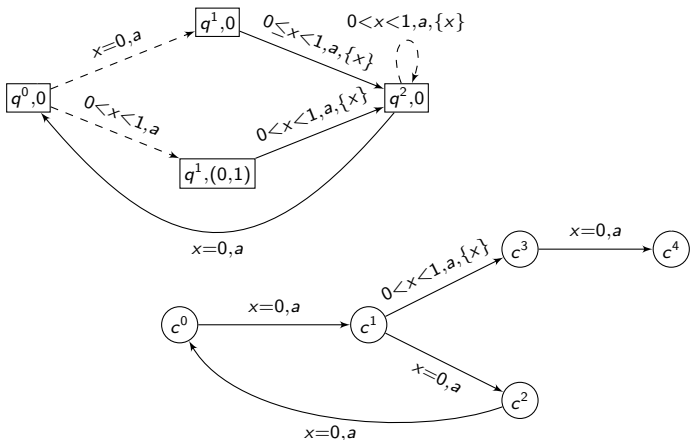
# Back to the example



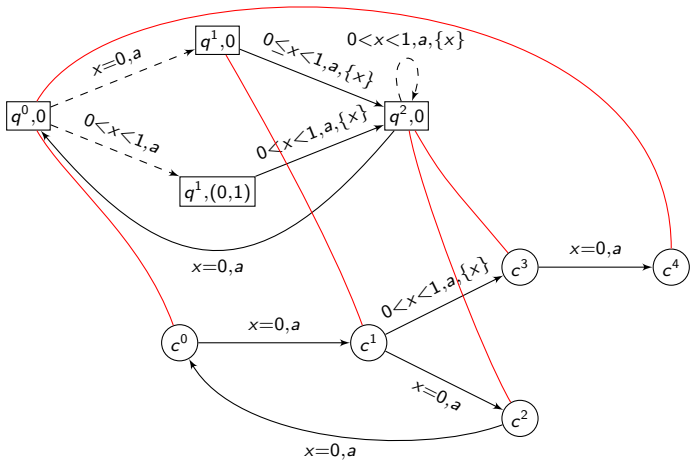
# Back to the example



# Back to the example



# 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
- 4 Conclusion

# Refinement of TMS

→ inherited from refinement of MS via region graph

## Refinement preorder on TMS

$\mathcal{S}_1 \preceq_{\text{TMS}} \mathcal{S}_2$  if  $R(\mathcal{S}_1) \preceq_{\text{MS}} R(\mathcal{S}_2)$ .

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  $\text{Mod}(\mathcal{S}_1) \subseteq \text{Mod}(\mathcal{S}_2)$ .

# 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
- 4 Conclusion

# Consistency of TMS

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

## Conjunction on TMS

$$\mathcal{S}_1 \wedge_{\text{TMS}} \mathcal{S}_2 := R^{-1}(R(\mathcal{S}_1) \wedge_{\text{MS}} R(\mathcal{S}_2))$$

## Properties of $\wedge$

- ▶  $\mathcal{S}_1 \wedge \mathcal{S}_2$  is the greatest lower bound of  $\mathcal{S}_1$  and  $\mathcal{S}_2$  for  $\preceq$ ;
- ▶  $\text{Mod}(\mathcal{S}_1 \wedge \mathcal{S}_2) = \text{Mod}(\mathcal{S}_1) \cap \text{Mod}(\mathcal{S}_2)$ .

# 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
- 4 Conclusion

# Conclusion

- ▶ Recap:
  - ▶ Definition of timed modal specifications
  - ▶ Decidability of refinement and consistency
  
- ▶ Future work:
  - ▶ Product and quotient of timed modal specifications
  - ▶ Relation with timed interfaces
  - ▶ Reactivity (deadlock-freeness) and refinement