Model Checking Real-Time Systems

Vincent Trélat

Technical University of Munich

December 12, 2022

Set of *time values*: $\mathbb{R}_{\geq 0}$

Timed words over $\Sigma \times \mathbb{R}_{\geq 0}$

Set of *valuations* over a set of clocks C: $\mathbb{R}_{\geq 0}^{C}$

Constraints over C: $\varphi ::= x \odot k \mid \varphi \wedge \varphi$ where $x \in C$, $k \in \mathbb{Z}$ and $\odot \in \{<, \leq, =, \geq, >\}$

Set of valuations *satisfying* φ: $[\![\varphi]\!]_C = \{v \in \mathbb{R}_{\geq 0}^{C} \mid v \models \varphi\}$

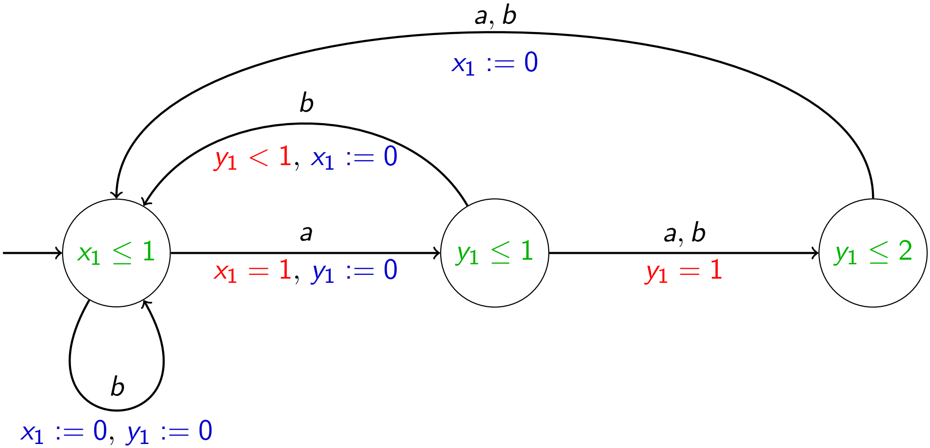
Definition 1

A *Timed Automaton* (TA) $\mathcal{A}$ is the tuple $(L, \ell_0, C, \Sigma, I, E)$ where:

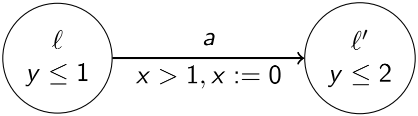
- L is a finite set of *locations* with initial location $\ell_0 \in L$
- C is a finite set of *clocks*
- Σ is a finite set of *actions*
- $I : L \to \Phi(C)$ is an *invariant mapping*
- $E \subseteq L \times \Phi(C) \times \Sigma \times 2^C \times L$ is a set of edges.

Edges are denoted by $\ell \xrightarrow{\varphi, a, r} \ell'$.

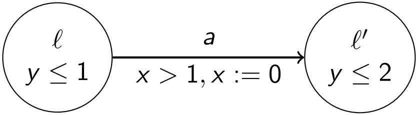
Example of a TA with 3 locations, 2 clocks and 2 actions (letters):



Operational Semantics



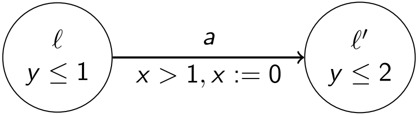
Operational Semantics



$$\begin{cases} v(x) = 1.2 \\ v(y) = 0.8 \end{cases}$$

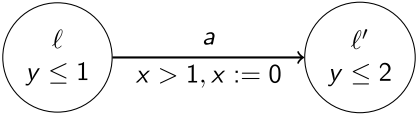
 Timed Automata

Operational Semantics



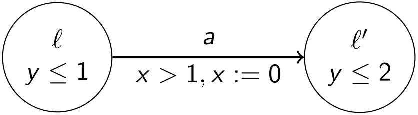
$$\begin{cases} v(x) = {\color{red}1.2} \\ v(y) = {\color{red}0.8} \end{cases} \qquad (\ell, v) \xrightarrow{{\color{red}0.5},\ a} (\ell', v')$$

Operational Semantics



$$\begin{cases} v(x) = 1.2 \\ v(y) = 0.8 \end{cases} \qquad (\ell, v) \xrightarrow{0.5,\ a} (\ell', v') \qquad \begin{cases} v'(x) = 0 \\ v'(y) = 1.3 \end{cases}$$

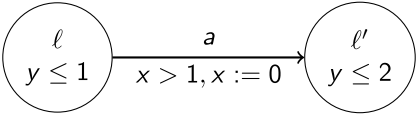
Operational Semantics



$$\begin{cases} v(x) = 1.2 \\ v(y) = 0.8 \end{cases} \qquad (\ell, v) \xrightarrow{0.5,\ a} (\ell', v') \qquad \begin{cases} v'(x) = 0 \\ v'(y) = 1.3 \end{cases}$$

$$\begin{cases} v(x) = 1.2 \\ v(y) = 0.8 \end{cases}$$

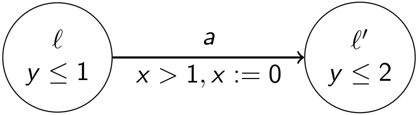
Operational Semantics



$$\begin{cases} v(x) = 1.2 \\ v(y) = 0.8 \end{cases} \qquad (\ell, v) \xrightarrow{0.5,\ a} (\ell', v') \qquad \begin{cases} v'(x) = 0 \\ v'(y) = 1.3 \end{cases}$$

$$\begin{cases} v(x) = 1.2 \\ v(y) = 0.8 \end{cases} \qquad (\ell, v) \xrightarrow{1.2,\ a} (\ell', v')$$

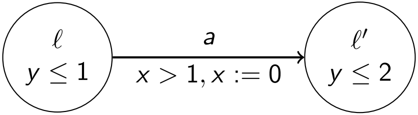
Operational Semantics



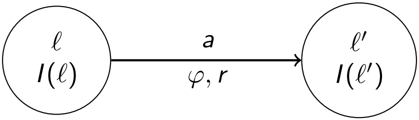
$$\begin{cases} v(x) = 1.2 \\ v(y) = 0.8 \end{cases} \quad (\ell, v) \xrightarrow{0.5,\ a} (\ell', v') \quad \begin{cases} v'(x) = 0 \\ v'(y) = 1.3 \end{cases}$$

$$\begin{cases} v(x) = 1.2 \\ v(y) = 0.8 \end{cases} \quad (\ell, v) \xrightarrow{1.2,\ a} (\ell', v') \quad \begin{cases} v'(x) = 0 \\ v'(y) = 2 \end{cases}$$

Operational Semantics

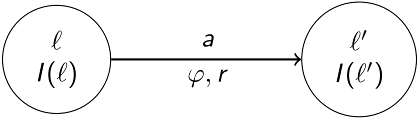


Operational Semantics



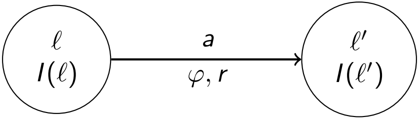
 Timed Automata

Operational Semantics



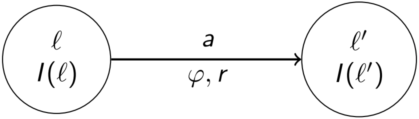
$$(\ell, v) \xrightarrow{d,\ a} (\ell', v')$$

Operational Semantics



$$(\ell, v) \xrightarrow{d,\ a} (\ell', (v + d)[r])$$

Operational Semantics



$$(\ell, v) \xrightarrow{d,\ a} (\ell', (v+d)[r])$$

provided that:

$$\ell \xrightarrow{\varphi,a,r} \ell' \text{ is a transition in the TA}$$

$$\forall t \in [0, d],\ \ v + t \models I(\ell)$$

$$v + d \models I(\ell')$$

Operational Semantics

Definition 2

The *operational semantics* of a TA $A = (L, \ell_0, C, \Sigma, I, E)$ is the infinite-state timed transition system $[\![A]\!] = (S, s_0, \Sigma \times \mathbb{R}_{\geq 0}, T)$, where

$$S := \{(\ell, v) \in L \times \mathbb{R}^C_{\geq 0} \mid v \models I(\ell)\}, \quad s_0 := (\ell_0, \mathbf{0}_C),$$

$$T := \{(\ell, v) \xrightarrow{d,a} (\ell', (v + d)[r]) \mid d \in \mathbb{R}_{\geq 0},$$
$$\forall d' \in [0, d], v + d' \models I(\ell) \wedge \exists \ell \xrightarrow{\varphi,a,r} \ell' \in E, v + d \models \varphi\}$$

References