

# *Real-Time Systems*

## *Lecture 12: Location Reachability (or: The Region Automaton)*

2013-06-12

Dr. Bernd Westphal

Albert-Ludwigs-Universität Freiburg, Germany

- 12 - 2013-06-12 - main -

### Contents & Goals

#### **Last Lecture:**

- Networks of Timed Automata
- Uppaal Demo

#### **This Lecture:**

- **Educational Objectives:** Capabilities for following tasks/questions.
  - What are decidable problems of TA?
  - How can we show this? What are the essential premises of decidability?
  - What is a region? What is the region automaton of this TA?
  - What's the time abstract system of a TA? Why did we consider this?
  - What can you say about the complexity of Region-automaton based reachability analysis?
- **Content:**
  - ~~Timed Transition System of network of timed automata~~
  - Location Reachability Problem
  - Constructive, region-based decidability proof

- 12 - 2013-06-12 - Prelim -

## The Location Reachability Problem

### The Location Reachability Problem

**Given:** A timed automaton  $\mathcal{A}$  and one of its control locations  $l$ .

**Question:** Is  $l$  **reachable**?

That is, is there a transition sequence of the form

$$\langle l_{ini}, \nu_0 \rangle \xrightarrow{\lambda_1} \langle l_1, \nu_1 \rangle \xrightarrow{\lambda_2} \langle l_2, \nu_2 \rangle \xrightarrow{\lambda_3} \dots \xrightarrow{\lambda_n} \langle l_n, \nu_n \rangle \stackrel{!}{=} \langle l, \nu \rangle$$

in the labelled transition system  $\mathcal{T}(\mathcal{A})$ ?

- **Note:** Decidability is not **soo** obvious, recall that
  - clocks range over real numbers, thus infinitely many configurations,
  - at each configuration, uncountably many transitions  $\xrightarrow{t}$  may originate
- **Consequence:** The timed automata as we consider them here **cannot** encode a 2-counter machine, and they are strictly less expressive than DC.

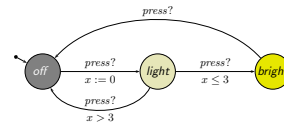
## Decidability of The Location Reachability Problem

### Claim: (Theorem 4.33)

The location reachability problem is **decidable** for timed automata.

### Approach: Constructive proof.

- Observe: clock constraints are **simple**  
— w.l.o.g. assume constants  $c \in \mathbb{N}_0$ .
- **Def. 4.19: time-abstract transition system**  $\mathcal{U}(\mathcal{A})$  — abstracts from uncountably many delay transitions, still infinite-state.
- **Lem. 4.20:** location reachability of  $\mathcal{A}$  is **preserved** in  $\mathcal{U}(\mathcal{A})$ .
- **Def. 4.29: region automaton**  $\mathcal{R}(\mathcal{A})$  — equivalent configurations collapse into regions
- **Lem. 4.32:** location reachability of  $\mathcal{U}(\mathcal{A})$  is **preserved** in  $\mathcal{R}(\mathcal{A})$ .
- **Lem. 4.28:**  $\mathcal{R}(\mathcal{A})$  is **finite**.



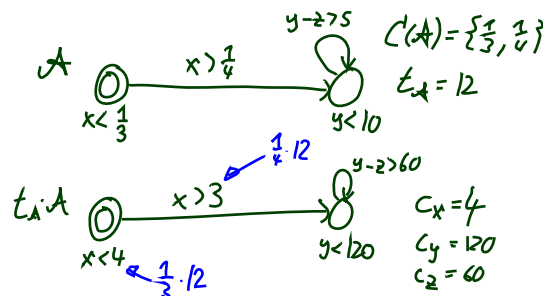
- 12 - 2013-06-12 - 5dec -

5/33

## Without Loss of Generality: Natural Constants

**Recall:** Simple clock constraints are  $\varphi ::= x \sim c \mid x - y \sim c \mid \varphi \wedge \varphi$  with  $x, y \in X$ ,  $c \in \mathbb{Q}_0^+$ , and  $\sim \in \{<, >, \leq, \geq\}$ .

- Let  $C(\mathcal{A}) = \{c \in \mathbb{Q}_0^+ \mid c \text{ appears in } \mathcal{A}\}$  —  $C(\mathcal{A})$  is **finite!** (Why?)
- Let  $t_{\mathcal{A}}$  be the **least common multiple of the denominators** in  $C(\mathcal{A})$ .
- Let  $t_{\mathcal{A}} \cdot \mathcal{A}$  be the TA obtained from  $\mathcal{A}$  by **multiplying** all constants by  $t_{\mathcal{A}}$ .



- 12 - 2013-06-12 - 5dec -

6/33

## Without Loss of Generality: Natural Constants

**Recall:** Simple clock constraints are  $\varphi ::= x \sim c \mid x - y \sim c \mid \varphi \wedge \varphi$   
with  $x, y \in X$ ,  $c \in \mathbb{Q}_0^+$ , and  $\sim \in \{<, >, \leq, \geq\}$ .

- Let  $C(\mathcal{A}) = \{c \in \mathbb{Q}_0^+ \mid c \text{ appears in } \mathcal{A}\}$  —  $C(\mathcal{A})$  is **finite!** (Why?)
- Let  $t_{\mathcal{A}}$  be the **least common multiple of the denominators** in  $C(\mathcal{A})$ .
- Let  $t_{\mathcal{A}} \cdot \mathcal{A}$  be the TA obtained from  $\mathcal{A}$  by **multiplying** all constants by  $t_{\mathcal{A}}$ .
- Then:
  - $C(t_{\mathcal{A}} \cdot \mathcal{A}) \subset \mathbb{N}_0$ .
  - A location  $\ell$  is reachable in  $t_{\mathcal{A}} \cdot \mathcal{A}$  if and only if  $\ell$  is reachable in  $\mathcal{A}$ .
- That is: we can **without loss of generality** in the following consider only timed automata  $\mathcal{A}$  with  $C(\mathcal{A}) \subset \mathbb{N}_0$ .

**Definition.** Let  $x$  be a clock of timed automaton  $\mathcal{A}$  (with  $C(\mathcal{A}) \subset \mathbb{N}_0$ ). We denote by  $c_x \in \mathbb{N}_0$  the **largest time constant**  $c$  that appears together with  $x$  in a constraint of  $\mathcal{A}$ .

## Decidability of The Location Reachability Problem

**Claim:** (**Theorem 4.33**)

The location reachability problem is **decidable** for timed automata.

**Approach:** Constructive proof.

- ✓ Observe: clock constraints are **simple**  
— w.l.o.g. assume constants  $c \in \mathbb{N}_0$ .
- ✗ **Def. 4.19: time-abstract transition system**  $\mathcal{U}(\mathcal{A})$  — abstracts from uncountably many delay transitions, still infinite-state.
- ✗ **Lem. 4.20:** location reachability of  $\mathcal{A}$  is **preserved** in  $\mathcal{U}(\mathcal{A})$ .
- ✗ **Def. 4.29: region automaton**  $\mathcal{R}(\mathcal{A})$  — equivalent configurations collapse into regions
- ✗ **Lem. 4.32:** location reachability of  $\mathcal{U}(\mathcal{A})$  is **preserved** in  $\mathcal{R}(\mathcal{A})$ .
- ✗ **Lem. 4.28:**  $\mathcal{R}(\mathcal{A})$  is **finite**.

## Helper: Relational Composition

**Recall:**  $\mathcal{T}(\mathcal{A}) = (\text{Conf}(\mathcal{A}), \text{Time} \cup B_{?}, \{\xrightarrow{\lambda} \mid \lambda \in \text{Time} \cup B_{?}\}, C_{ini})$

- Note: The  $\xrightarrow{\lambda}$  are binary relations on configurations.

**Definition.** Let  $\mathcal{A}$  be a TA. For all  $\langle \ell_1, \nu_1 \rangle, \langle \ell_2, \nu_2 \rangle \in \text{Conf}(\mathcal{A})$ ,

$$\langle \ell_1, \nu_1 \rangle \xrightarrow{\lambda_1} \circ \xrightarrow{\lambda_2} \langle \ell_2, \nu_2 \rangle$$

if and only if there **exists some**  $\langle \ell', \nu' \rangle \in \text{Conf}(\mathcal{A})$  such that

$$\langle \ell_1, \nu_1 \rangle \xrightarrow{\lambda_1} \langle \ell', \nu' \rangle \text{ and } \langle \ell', \nu' \rangle \xrightarrow{\lambda_2} \langle \ell_2, \nu_2 \rangle.$$

## Helper: Relational Composition

**Recall:**  $\mathcal{T}(\mathcal{A}) = (\text{Conf}(\mathcal{A}), \text{Time} \cup B_{?}, \{\xrightarrow{\lambda} \mid \lambda \in \text{Time} \cup B_{?}\}, C_{ini})$

- Note: The  $\xrightarrow{\lambda}$  are binary relations on configurations.

**Definition.** Let  $\mathcal{A}$  be a TA. For all  $\langle \ell_1, \nu_1 \rangle, \langle \ell_2, \nu_2 \rangle \in \text{Conf}(\mathcal{A})$ ,

$$\langle \ell_1, \nu_1 \rangle \xrightarrow{\lambda_1} \circ \xrightarrow{\lambda_2} \langle \ell_2, \nu_2 \rangle$$

if and only if there **exists some**  $\langle \ell', \nu' \rangle \in \text{Conf}(\mathcal{A})$  such that

$$\langle \ell_1, \nu_1 \rangle \xrightarrow{\lambda_1} \langle \ell', \nu' \rangle \text{ and } \langle \ell', \nu' \rangle \xrightarrow{\lambda_2} \langle \ell_2, \nu_2 \rangle.$$

**Remark.** The following property of **time additivity** holds.

$$\forall t_1, t_2 \in \text{Time} : \xrightarrow{t_1} \circ \xrightarrow{t_2} = \xrightarrow{t_1+t_2}$$

## Time-abstract Transition System

**Definition 4.19.** [Time-abstract transition system]

Let  $\mathcal{A}$  be a timed automaton.

The **time-abstract transition system**  $\mathcal{U}(\mathcal{A})$  is obtained from  $\mathcal{T}(\mathcal{A})$  (Def. 4.4) by taking

$$\mathcal{U}(\mathcal{A}) = (\text{Conf}(\mathcal{A}), B_{?!}, \{\xrightarrow{\alpha} \mid \alpha \in B_{?!}\}, C_{ini})$$

where

$$\xrightarrow{\alpha} \subseteq \text{Conf}(\mathcal{A}) \times \text{Conf}(\mathcal{A})$$

is defined as follows: Let  $\langle l, \nu \rangle, \langle l', \nu' \rangle \in \text{Conf}(\mathcal{A})$  be configurations of  $\mathcal{A}$  and  $\alpha \in B_{?!}$  an action. Then

$$\langle l, \nu \rangle \xrightarrow{\alpha} \langle l', \nu' \rangle$$

if and only if there exists  $t \in \text{Time}$  such that

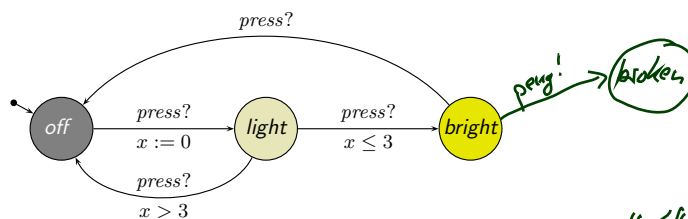
$$\langle l, \nu \rangle \xrightarrow{t} \circ \xrightarrow{\alpha} \langle l', \nu' \rangle.$$

- 12 - 2013-06-12 - 5dec -

9/33

### Example

$$\langle l, \nu \rangle \xrightarrow{\alpha} \langle l', \nu' \rangle \text{ iff } \exists t \in \text{Time} \bullet \langle l, \nu \rangle \xrightarrow{t} \circ \xrightarrow{\alpha} \langle l', \nu' \rangle$$



$\langle \text{off}, x=3 \rangle \stackrel{?}{\Rightarrow} \langle \text{off}, x=3.5 \rangle$  NO,  $t=0.5$  is a delay candidate, but no  $\alpha$  with  $\langle \text{off}, 3.5 \rangle \xrightarrow{\alpha} \langle \text{off}, 3.5 \rangle$   
 $\langle \text{off}, x=4 \rangle \stackrel{\text{press?}}{\Rightarrow} \langle \text{light}, x=0 \rangle$  YES, any  $t \in \mathbb{R}_0^+$  works,  $\alpha = \text{press?}$   
 $\langle \text{off}, x=4 \rangle \stackrel{?}{\Rightarrow} \langle \text{light}, x=5 \rangle$  NO,  $\langle \text{off}, x=4 \rangle \xrightarrow{t} \circ \xrightarrow{\alpha} \langle \text{light}, x=4 \rangle$  implies  $\alpha = \text{press?}$  and  $t=0$   
 $\langle \text{off}, x=7 \rangle \stackrel{!}{\Rightarrow} \langle \text{bright}, x=3 \rangle$  NO, cannot go from off to bright with one action transition

$\langle \text{bright}, x=13 \rangle \stackrel{\text{peng!}}{\Rightarrow} \langle \text{broken}, x=13 \rangle$  YES,  $t=0$  and  $\alpha = \text{peng!}$   
 $\langle \text{broken}, x=13 \rangle \stackrel{?}{\Rightarrow} \langle \text{broken}, x=27 \rangle$  NO, no outgoing edge from broken

- 12 - 2013-06-12 - 5dec -

10/33

## Location Reachability is preserved in $U(\mathcal{A})$

**Lemma 4.20.** For all locations  $l$  of a given timed automaton  $\mathcal{A}$  the following holds:

$l$  is reachable in  $\mathcal{T}(\mathcal{A})$  if and only if  $l$  is reachable in  $U(\mathcal{A})$ .

**Proof:**

" $\Leftarrow$ ": easy

" $\Rightarrow$ ":  $l$  reachable in  $\mathcal{T}(\mathcal{A})$   $n_0 > 0$ , i.e. sequence could be empty

$\Leftrightarrow$  there is  $\langle l_0, v_0 \rangle \xrightarrow{t_0} \langle l_1, v_1 \rangle \rightarrow \dots \xrightarrow{t_{n_0}} \langle l_{n_0}, v_{n_0} \rangle \xrightarrow{\alpha_1} \langle l_1, v_1 \rangle$

$\xrightarrow{t_1} \langle l_1, v_1 \rangle \rightarrow \dots \xrightarrow{t_{n_1}} \langle l_{n_1}, v_{n_1} \rangle \rightarrow \dots \xrightarrow{t_{n_2}} \langle l_{n_2}, v_{n_2} \rangle \rightarrow \dots \xrightarrow{\alpha_m} \langle l_m, v_m \rangle, l_m = l, n_i \in \mathbb{N}_0$

$\Rightarrow \langle l_0, v_0 \rangle \xRightarrow{\alpha_1} \langle l_1, v_1 \rangle \dots \xRightarrow{\alpha_m} \langle l_m, v_m \rangle, l_m = l$

$\uparrow$  by  $t_1 \rightarrow 0 \xrightarrow{\alpha_1}$

- 12 - 2013-06-12 - 5dec -

11/33

## Decidability of The Location Reachability Problem

**Claim:** (Theorem 4.33)

The location reachability problem is **decidable** for timed automata.

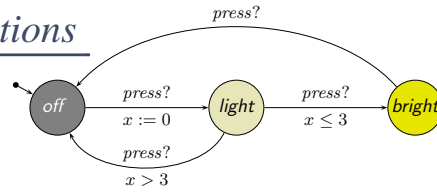
**Approach:** Constructive proof.

- ✓ Observe: clock constraints are **simple**  
— w.l.o.g. assume constants  $c \in \mathbb{N}_0$ .
- ✓ **Def. 4.19: time-abstract transition system**  $U(\mathcal{A})$  — abstracts from uncountably many delay transitions, still infinite-state.
- ✓ **Lem. 4.20:** location reachability of  $\mathcal{A}$  is **preserved** in  $U(\mathcal{A})$ .
- ✗ **Def. 4.29: region automaton**  $\mathcal{R}(\mathcal{A})$  — equivalent configurations collapse into regions
- ✗ **Lem. 4.32:** location reachability of  $U(\mathcal{A})$  is **preserved** in  $\mathcal{R}(\mathcal{A})$ .
- ✗ **Lem. 4.28:**  $\mathcal{R}(\mathcal{A})$  is **finite**.

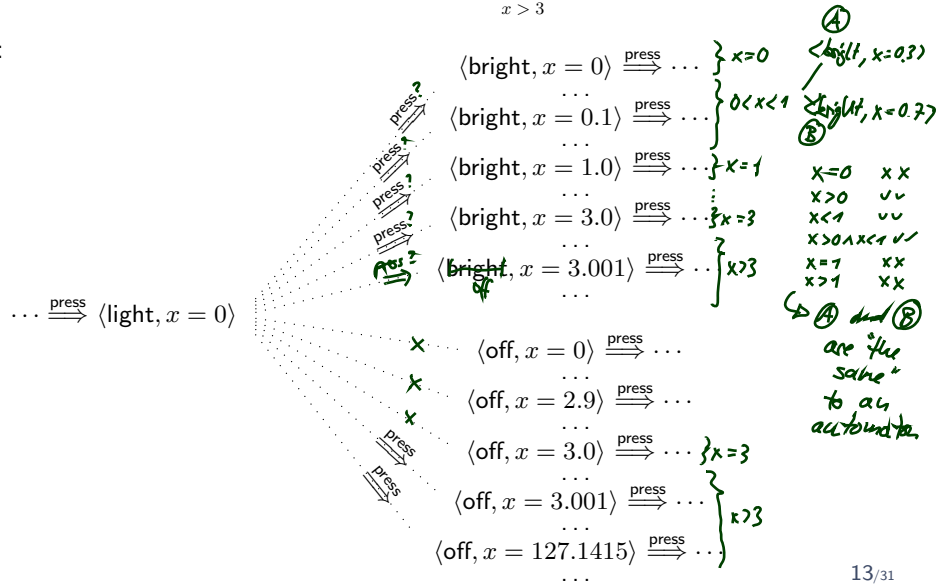
- 12 - 2013-06-12 - 5dec -

12/33

# Indistinguishable Configurations



$\mathcal{U}(\mathcal{A})$ :



- 12 - 2012-06-28 - Sdec -

# Distinguishing Clock Valuations: One Clock

- Assume  $\mathcal{A}$  with only a single clock, i.e.  $X = \{x\}$  (recall:  $C(\mathcal{A}) \subset \mathbb{N}$ .)

- $\mathcal{A}$  **could detect**, for a given  $\nu$ , whether  $\nu(x) \in \{0, \dots, c_x\}$ .  
e.g.  $0 \xrightarrow{x \leq 3 \wedge x \geq 3} 0$
- $\mathcal{A}$  **cannot distinguish**  $\nu_1$  and  $\nu_2$  if  $\nu_i(x) \in (k, k+1)$ ,  $i = 1, 2$ , and  $k \in \{0, \dots, c_x - 1\}$ .  
e.g.  $0 \xrightarrow{x > 1 \wedge k < 2} 0$
- $\mathcal{A}$  **cannot distinguish**  $\nu_1$  and  $\nu_2$  if  $\nu_i(x) > c_x$ ,  $i = 1, 2$ .  
e.g.  $0 \xrightarrow{x > c_x} 0$

- If  $c_x \geq 1$ , there are  $(2c_x + 2)$  **equivalence classes**:

$$\{\{0\}, (0, 1), \{1\}, (1, 2), \dots, \{c_x\}, (c_x, \infty)\}$$

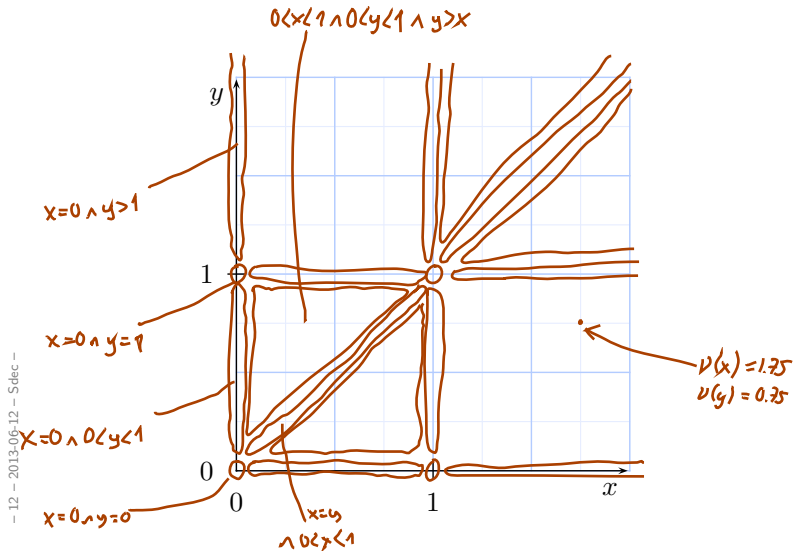
If  $\nu_1(x)$  and  $\nu_2(x)$  are in the **same** equivalence class, then  $\nu_1$  and  $\nu_2$  are **indistinguishable** by  $\mathcal{A}$ .

- 12 - 2013-06-12 - Sdec -



## Distinguishing Clock Valuations: Two Clocks

- $X = \{x, y\}$ ,  $c_x = 1$ ,  $c_y = 1$ .



15/33

## Helper: Floor and Fraction

- **Recall:**

Each  $q \in \mathbb{R}_0^+$  can be split into

- **floor**  $\lfloor q \rfloor \in \mathbb{N}_0$  and
- **fraction**  $frac(q) \in [0, 1)$

such that

$$q = \lfloor q \rfloor + frac(q).$$

## An Equivalence-Relation on Valuations

**Definition.** Let  $X$  be a set of clocks,  $c_x \in \mathbb{N}_0$  for each clock  $x \in X$ , and  $\nu_1, \nu_2$  clock valuations of  $X$ .

We set  $\nu_1 \cong \nu_2$  iff the following **four** conditions are satisfied.

(1) For all  $x \in X$ ,

$$\lfloor \nu_1(x) \rfloor = \lfloor \nu_2(x) \rfloor \text{ or both } \nu_1(x) > c_x \text{ and } \nu_2(x) > c_x.$$

(2) For all  $x \in X$  with  $\nu_1(x) \leq c_x$ ,

$$\text{frac}(\nu_1(x)) = 0 \text{ if and only if } \text{frac}(\nu_2(x)) = 0.$$

(3) For all  $x, y \in X$ ,

$$\lfloor \nu_1(x) - \nu_1(y) \rfloor = \lfloor \nu_2(x) - \nu_2(y) \rfloor$$

$$\text{or both } |\nu_1(x) - \nu_1(y)| > c \text{ and } |\nu_2(x) - \nu_2(y)| > c.$$

(4) For all  $x, y \in X$  with  $-c \leq \nu_1(x) - \nu_1(y) \leq c$ ,

$$\text{frac}(\nu_1(x) - \nu_1(y)) = 0 \text{ if and only if } \text{frac}(\nu_2(x) - \nu_2(y)) = 0.$$

Where  $c = \max\{c_x, c_y\}$ .

- 12 - 2013-06-12 - 5dec -

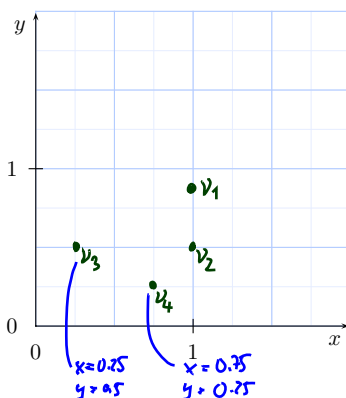
17/33

### Example: Regions

- (1)  $\forall x \in X : \lfloor \nu_1(x) \rfloor = \lfloor \nu_2(x) \rfloor \vee (\nu_1(x) > c_x \wedge \nu_2(x) > c_x)$
- (2)  $\forall x \in X : \nu_1(x) \leq c_x$   
 $\implies (\text{frac}(\nu_1(x)) = 0 \iff \text{frac}(\nu_2(x)) = 0)$
- (3)  $\forall x, y \in X : \lfloor \nu_1(x) - \nu_1(y) \rfloor = \lfloor \nu_2(x) - \nu_2(y) \rfloor$   
 $\vee (|\nu_1(x) - \nu_1(y)| > c \wedge |\nu_2(x) - \nu_2(y)| > c)$
- (4)  $\forall x, y \in X : -c \leq \nu_1(x) - \nu_1(y) \leq c \implies$   
 $(\text{frac}(\nu_1(x) - \nu_1(y)) = 0 \iff \text{frac}(\nu_2(x) - \nu_2(y)) = 0)$

$$c_x = 1$$

$$c_y = 1$$



•  $\nu_1 \cong \nu_2$ :

- (1) ✓✓
- (2) ✓✓
- (3) ✓
- (4) ✓

•  $\nu_3 \not\cong \nu_4$ :

- (1) ✓✓
- (2) ✓✓
- (3)  $\nu_3(x) - \nu_3(y) = -0.25 \lfloor -0.25 \rfloor = -1$
- $\nu_4(x) - \nu_4(y) = 0.5 \lfloor 0.5 \rfloor = 1 \neq -1$

- 12 - 2013-06-12 - 5dec -

18/33

## Regions

**Proposition.**  $\cong$  is an **equivalence relation**.

**Definition 4.27.** For a given valuation  $\nu$  we denote by  $[\nu]$  the equivalence class of  $\nu$ . We call equivalence classes of  $\cong$  **regions**.

$\{\nu' \mid \nu \cong \nu'\}$

## The Region Automaton

**Definition 4.29.** [Region Automaton] The **region automaton**  $\mathcal{R}(\mathcal{A})$  of the timed automaton  $\mathcal{A}$  is the labelled transition system

$$\mathcal{R}(\mathcal{A}) = (\text{Conf}(\mathcal{R}(\mathcal{A})), B_{?!}, \{\overset{\alpha}{\rightarrow}_{\mathcal{R}(\mathcal{A})} \mid \alpha \in B_{?!}\}, C_{ini})$$

where

- $\text{Conf}(\mathcal{R}(\mathcal{A})) = \{\langle \ell, [\nu] \rangle \mid \ell \in L, \nu : X \rightarrow \text{Time}, \nu \models I(\ell)\}$ ,
- for each  $\alpha \in B_{?!}$ ,

$$\langle \ell, [\nu] \rangle \overset{\alpha}{\rightarrow}_{\mathcal{R}(\mathcal{A})} \langle \ell', [\nu'] \rangle \text{ if and only if } \langle \ell, \nu \rangle \overset{\alpha}{\Rightarrow} \langle \ell', \nu' \rangle$$

in  $\mathcal{U}(\mathcal{A})$ , and

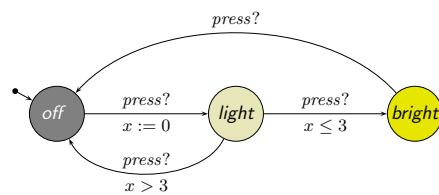
- $C_{ini} = \{\langle \ell_{ini}, [\nu_{ini}] \rangle\} \cap \text{Conf}(\mathcal{R}(\mathcal{A}))$  with  $\nu_{ini}(X) = \{0\}$ .

representative of region  $[\nu]$

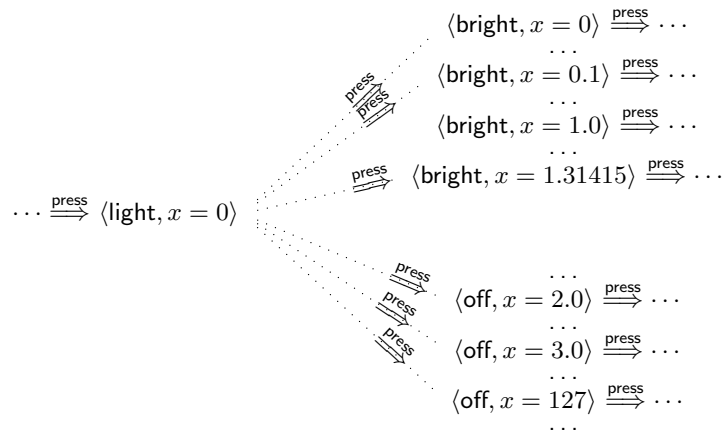
representative of region  $[\nu']$

**Proposition.** The transition relation of  $\mathcal{R}(\mathcal{A})$  is **well-defined**, that is, independent of the choice of the representative  $\nu$  of a region  $[\nu]$ .

## Example: Region Automaton



$\mathcal{U}(\mathcal{A})$ :



- 12 - 2013-06-12 - 5dec -

21/33

## Remark

**Remark 4.30.** That a configuration  $\langle \ell, [\nu] \rangle$  is reachable in  $\mathcal{R}(\mathcal{A})$  represents the fact, that all  $\langle \ell, \nu \rangle$  are reachable.

IAW: in  $\mathcal{A}$ , we can observe  $\nu$  when  
location  $\ell$  has **just been entered**.

The clock values reachable by staying/letting time pass in  $\ell$  are **not explicitly** represented by the regions of  $\mathcal{R}(\mathcal{A})$ .

- 12 - 2013-06-12 - 5dec -

22/33

## Decidability of The Location Reachability Problem

**Claim:** (Theorem 4.33)

The location reachability problem is **decidable** for timed automata.

**Approach:** Constructive proof.

- ✓ Observe: clock constraints are **simple**  
— w.l.o.g. assume constants  $c \in \mathbb{N}_0$ .
- ✓ **Def. 4.19: time-abstract transition system**  $\mathcal{U}(\mathcal{A})$  — abstracts from uncountably many delay transitions, still infinite-state.
- ✓ **Lem. 4.20:** location reachability of  $\mathcal{A}$  is **preserved** in  $\mathcal{U}(\mathcal{A})$ .
- ✓ **Def. 4.29: region automaton**  $\mathcal{R}(\mathcal{A})$  — equivalent configurations collapse into regions
- ✗ **Lem. 4.32:** location reachability of  $\mathcal{U}(\mathcal{A})$  is **preserved** in  $\mathcal{R}(\mathcal{A})$ .
- ✗ **Lem. 4.28:**  $\mathcal{R}(\mathcal{A})$  is **finite**.

– 12 – 2013-06-12 – 5dec –

23/33

## Region Automaton Properties

**Lemma 4.32.** [Correctness] For all locations  $\ell$  of a given timed automaton  $\mathcal{A}$  the following holds:

$\ell$  is reachable in  $\mathcal{U}(\mathcal{A})$  if and only if  $\ell$  is reachable in  $\mathcal{R}(\mathcal{A})$ .

For the **Proof:**

**Definition 4.21.** [Bisimulation] An equivalence relation  $\sim$  on valuations is a **(strong) bisimulation** if and only if, whenever

$$\nu_1 \sim \nu_2 \text{ and } \langle \ell, \nu_1 \rangle \xrightarrow{\alpha} \langle \ell', \nu'_1 \rangle$$

then there exists  $\nu'_2$  with  $\nu'_1 \sim \nu'_2$  and  $\langle \ell, \nu_2 \rangle \xrightarrow{\alpha} \langle \ell', \nu'_2 \rangle$ .

**Lemma 4.26.** [Bisimulation]  $\cong$  is a **strong bisimulation**.

– 12 – 2013-06-12 – 5dec –

24/33

## Decidability of The Location Reachability Problem

### Claim: (Theorem 4.33)

The location reachability problem is **decidable** for timed automata.

### Approach: Constructive proof.

- ✓ Observe: clock constraints are **simple**  
— w.l.o.g. assume constants  $c \in \mathbb{N}_0$ .
- ✓ **Def. 4.19: time-abstract transition system**  $\mathcal{U}(\mathcal{A})$  — abstracts from uncountably many delay transitions, still infinite-state.
- ✓ **Lem. 4.20:** location reachability of  $\mathcal{A}$  is **preserved** in  $\mathcal{U}(\mathcal{A})$ .
- ✓ **Def. 4.29: region automaton**  $\mathcal{R}(\mathcal{A})$  — equivalent configurations collapse into regions
- ✓ **Lem. 4.32:** location reachability of  $\mathcal{U}(\mathcal{A})$  is **preserved** in  $\mathcal{R}(\mathcal{A})$ .
- ✗ **Lem. 4.28:**  $\mathcal{R}(\mathcal{A})$  is **finite**.

– 12 – 2013-06-12 – 5dec –

25/33

## The Number of Regions

**Lemma 4.28.** Let  $X$  be a set of clocks,  $c_x \in \mathbb{N}_0$  the maximal constant for each  $x \in X$ , and  $c = \max\{c_x \mid x \in X\}$ . Then

$$(2c + 2)^{|X|} \cdot (4c + 3)^{\frac{1}{2}|X| \cdot (|X|-1)}$$

is an **upper bound** on the **number of regions**.

**Proof:** [Olderog and Dierks, 2008]

– 12 – 2013-06-12 – 5dec –

26/33

## Observations Regarding the Number of Regions

- Lemma 4.28 **in particular** tells us that each timed automaton (in our definition) has **finitely** many regions.
- Note: the upper bound is a **worst case**, not an **exact bound**.

## Decidability of The Location Reachability Problem

### **Claim:** (Theorem 4.33)

The location reachability problem is **decidable** for timed automata.

### **Approach:** Constructive proof.

- ✓ Observe: clock constraints are **simple**  
— w.l.o.g. assume constants  $c \in \mathbb{N}_0$ .
- ✓ **Def. 4.19:** **time-abstract transition system**  $\mathcal{U}(\mathcal{A})$  — abstracts from uncountably many delay transitions, still infinite-state.
- ✓ **Lem. 4.20:** location reachability of  $\mathcal{A}$  is **preserved** in  $\mathcal{U}(\mathcal{A})$ .
- ✓ **Def. 4.29:** **region automaton**  $\mathcal{R}(\mathcal{A})$  — equivalent configurations collapse into regions
- ✓ **Lem. 4.32:** location reachability of  $\mathcal{U}(\mathcal{A})$  is **preserved** in  $\mathcal{R}(\mathcal{A})$ .
- ✓ **Lem. 4.28:**  $\mathcal{R}(\mathcal{A})$  is **finite**.

## Putting It All Together

Let  $\mathcal{A} = (L, B, X, I, E, \ell_{ini})$  be a timed automaton,  $\ell \in L$  a location.

- $\mathcal{R}(\mathcal{A})$  can be constructed effectively.
- There are finitely many locations in  $L$  (by definition).
- There are finitely many regions by Lemma 4.28.
- So  $Conf(\mathcal{R}(\mathcal{A}))$  is finite (by construction).
- It is decidable whether ( $C_{init}$  of  $\mathcal{R}(\mathcal{A})$  is empty) or whether there exists a sequence

$$\langle \ell_{ini}, [\nu_{ini}] \rangle \xrightarrow{\alpha}_{R(\mathcal{A})} \langle \ell_1, [\nu_1] \rangle \xrightarrow{\alpha}_{R(\mathcal{A})} \dots \xrightarrow{\alpha}_{R(\mathcal{A})} \langle \ell_n, [\nu_n] \rangle$$

such that  $\ell_n = \ell$  (reachability in graphs).

## Putting It All Together

Let  $\mathcal{A} = (L, B, X, I, E, \ell_{ini})$  be a timed automaton,  $\ell \in L$  a location.

- $\mathcal{R}(\mathcal{A})$  can be constructed effectively.
- There are finitely many locations in  $L$  (by definition).
- There are finitely many regions by Lemma 4.28.
- So  $Conf(\mathcal{R}(\mathcal{A}))$  is finite (by construction).
- It is decidable whether ( $C_{init}$  of  $\mathcal{R}(\mathcal{A})$  is empty) or whether there exists a sequence

$$\langle \ell_{ini}, [\nu_{ini}] \rangle \xrightarrow{\alpha}_{R(\mathcal{A})} \langle \ell_1, [\nu_1] \rangle \xrightarrow{\alpha}_{R(\mathcal{A})} \dots \xrightarrow{\alpha}_{R(\mathcal{A})} \langle \ell_n, [\nu_n] \rangle$$

such that  $\ell_n = \ell$  (reachability in graphs).

So we have

**Theorem 4.33.** [*Decidability*]  
The location reachability problem for timed automata is **decidable**.



## The Constraint Reachability Problem

- **Given:** A timed automaton  $\mathcal{A}$ , one of its control locations  $\ell$ , and a clock constraint  $\varphi$ .
- **Question:** Is a configuration  $\langle \ell, \nu \rangle$  **reachable** where  $\nu \models \varphi$ , i.e. is there a transition sequence of the form

$$\langle \ell_{ini}, \nu_{ini} \rangle \xrightarrow{\lambda_1} \langle \ell_1, \nu_1 \rangle \xrightarrow{\lambda_2} \langle \ell_2, \nu_2 \rangle \xrightarrow{\lambda_3} \dots \xrightarrow{\lambda_n} \langle \ell_n, \nu_n \rangle = \langle \ell, \nu \rangle$$

in the labelled transition system  $\mathcal{T}(\mathcal{A})$  with  $\nu \models \varphi$ ?

- **Note:** we just observed that  $\mathcal{R}(\mathcal{A})$  loses some information about the clock valuations that are possible in/from a region.

## The Constraint Reachability Problem

- **Given:** A timed automaton  $\mathcal{A}$ , one of its control locations  $\ell$ , and a clock constraint  $\varphi$ .
- **Question:** Is a configuration  $\langle \ell, \nu \rangle$  **reachable** where  $\nu \models \varphi$ , i.e. is there a transition sequence of the form

$$\langle \ell_{ini}, \nu_{ini} \rangle \xrightarrow{\lambda_1} \langle \ell_1, \nu_1 \rangle \xrightarrow{\lambda_2} \langle \ell_2, \nu_2 \rangle \xrightarrow{\lambda_3} \dots \xrightarrow{\lambda_n} \langle \ell_n, \nu_n \rangle = \langle \ell, \nu \rangle$$

in the labelled transition system  $\mathcal{T}(\mathcal{A})$  with  $\nu \models \varphi$ ?

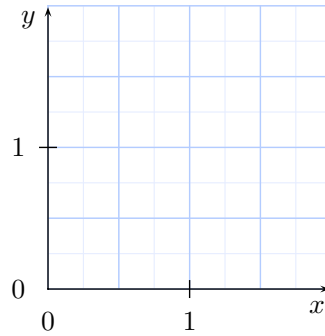
- **Note:** we just observed that  $\mathcal{R}(\mathcal{A})$  loses some information about the clock valuations that are possible in/from a region.

**Theorem 4.34.** The constraint reachability problem for timed automata is decidable.

## The Delay Operation

- Let  $[\nu]$  be a clock region.
- We set

$$\text{delay}[\nu] = \{\nu' + t \mid \nu' \cong \nu \text{ and } t \in \text{Time}\}.$$



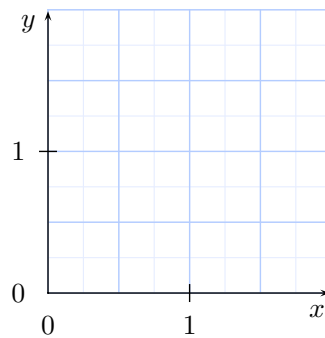
- 12 - 2013-06-12 - 5dec -

31/33

## The Delay Operation

- Let  $[\nu]$  be a clock region.
- We set

$$\text{delay}[\nu] = \{\nu' + t \mid \nu' \cong \nu \text{ and } t \in \text{Time}\}.$$



- 12 - 2013-06-12 - 5dec -

- **Note:**  $\text{delay}[\nu]$  can be represented as a **finite** union of regions.  
**For example,** with our two-clock example we have

$$\text{delay}[x = y = 0] = [x = y = 0] \cup [0 < x = y < 1] \cup [x = y = 1] \cup [1 < x = y]$$

31/33

## *References*

---

## References

[Olderog and Dierks, 2008] Olderog, E.-R. and Dierks, H. (2008). *Real-Time Systems - Formal Specification and Automatic Verification*. Cambridge University Press.