

Real-Time Systems

Lecture 17: Automatic Verification of DC Properties for TA

2013-07-09

Dr. Bernd Westphal

Albert-Ludwigs-Universität Freiburg, Germany

- 17 - 2013-07-09 - main -

Contents & Goals

Last Lecture:

- Undecidability Results for TBA

This Lecture:

- **Educational Objectives:** Capabilities for following tasks/questions.
 - How can we relate TA and DC formulae? What's a bit tricky about that?
 - Can we use Uppaal to check whether a TA satisfies a DC formula?
- **Content:**
 - An evolution-of-observables semantics of TA
 - A satisfaction relation between TA and DC
 - Model-checking DC properties with Uppaal

- 17 - 2013-07-09 - Spinelim -

You Are Here

Content

Introduction

- **First-order Logic**
- **Duration Calculus (DC)**
- Semantical Correctness Proofs with DC
- DC Decidability
- DC Implementables
- **PLC-Automata**
- **Timed Automata (TA)**, Uppaal
- Networks of Timed Automata
- Region/Zone-Abstraction
- Extended Timed Automata
- Undecidability Results

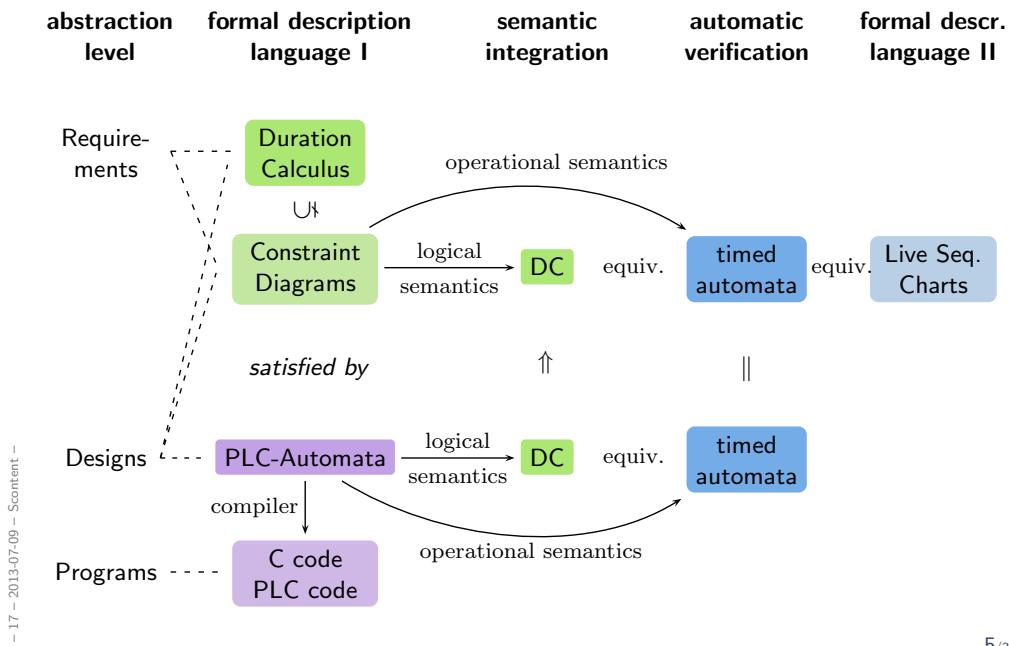
$obs : \text{Time} \rightarrow \mathcal{D}(obs)$

$\langle obs_0, \nu_0 \rangle, t_0 \xrightarrow{\lambda_0} \langle obs_1, \nu_1 \rangle, t_1 \dots$

- **Automatic Verification...**
- ...whether TA satisfies DC formula, observer-based

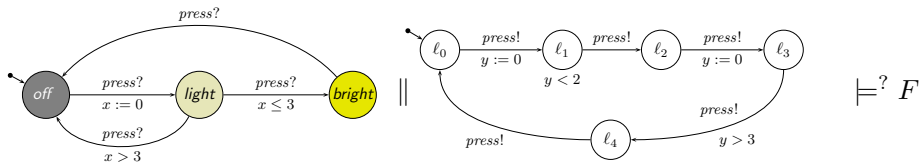
Recap

Tying It All Together



Observer-based Automatic Verification of DC Properties for TA

Model-Checking DC Properties with Uppaal

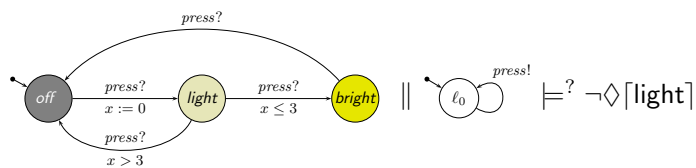


- **First Question:** what is the “ \models ” here?
- **Second Question:** what kinds of DC formulae can we check with Uppaal?
 - **Clear:** Not every DC formula. (Otherwise contradicting undecidability results.)
 - **Quite clear:** $F = \Box[\text{off}]$ or $F = \neg\Diamond[\text{light}]$
(Use Uppaal’s fragment of TCTL, something like $\forall\Box\text{off}$, but not exactly (see later).)
 - **Maybe:** $F = \ell > 5 \implies \Diamond[\text{off}]^5$
 - **Not so clear:** $F = \neg\Diamond([\text{bright}] ; [\text{light}])$

- 17 - 2013.07.09 - SdeVintro -

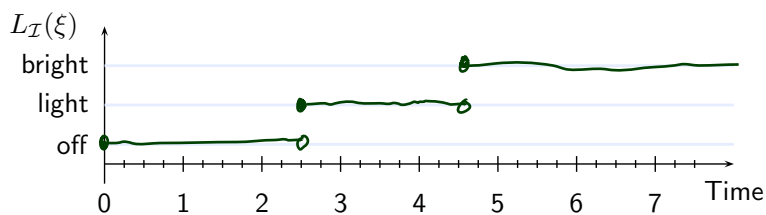
7/38

Example: Let’s Start With Single Runs



$$\xi = \langle \text{off} \rangle_0, 0 \xrightarrow{2.5} \langle \text{off} \rangle_{2.5}, 2.5 \xrightarrow{\tau} \langle \text{light} \rangle_0, 2.5 \xrightarrow{2.0} \langle \text{light} \rangle_{2.0}, 4.5 \xrightarrow{\tau} \langle \text{bright} \rangle_{2.0}, 4.5 \dots$$

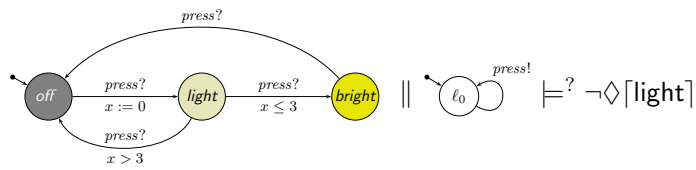
Construct interpretation $L_{\mathcal{I}}(\xi) : \text{Time} \rightarrow \{\text{off}, \text{light}, \text{bright}\}$:



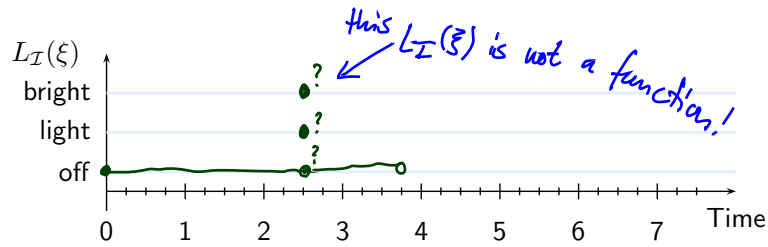
- 17 - 2013.07.09 - SdeVintro -

8/38

Example 2: Another Single Run



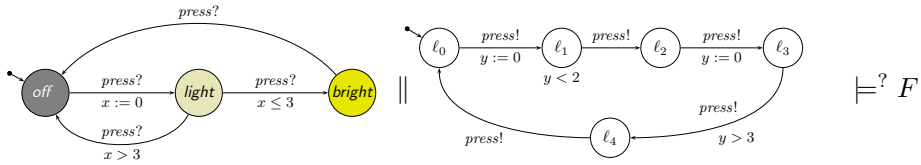
$$\xi = \langle \text{off} \rangle_0, 0 \xrightarrow{2.5} \langle \text{off} \rangle_{2.5}, 2.5 \xrightarrow{\tau} \langle \text{light} \rangle_0, 2.5 \xrightarrow{\tau} \langle \text{bright} \rangle_0, 2.5 \xrightarrow{\tau} \langle \text{off} \rangle_0, 2.5 \xrightarrow{1.0} \dots$$



We know this problem from the exercises...

Observing Timed Automata

DC Properties of Timed Automata



Wanted: A satisfaction relation between networks of timed automata and DC formulae, a notion of \mathcal{N} **satisfies** F , denoted by $\mathcal{N} \models F$.

Plan:

- Consider network \mathcal{N} consisting of TA

$$\mathcal{A}_{e,i} = (L_i, C_i, B_i, U_i, X_i, V_i, I_i, E_i, \ell_{ini,i})$$

- Define observables $\text{Obs}(\mathcal{N})$ of \mathcal{N} .
- Define evolution \mathcal{I}_ξ of $\text{Obs}(\mathcal{N})$ induced by computation path $\xi \in \text{CompPaths}(\mathcal{N})$ of \mathcal{N} ,
 $\text{CompPaths}(\mathcal{N}) = \{\xi \mid \xi \text{ is a computation path of } \mathcal{N}\}$
- Say $\mathcal{N} \models F$ if and only if $\forall \xi \in \text{CompPaths}(\mathcal{N}) : \mathcal{I}_\xi \models_0 F$.

11/38

- 17 - 2013-07-09 - Stobbs -

Observables of TA Network

Let \mathcal{N} be a network of n extended timed automata

$$\mathcal{A}_{e,i} = (L_i, C_i, B_i, U_i, X_i, V_i, I_i, E_i, \ell_{ini,i})$$

For simplicity: assume that the L_i and X_i are pairwise disjoint and that each V_i is pairwise disjoint to every L_i and X_i (otherwise rename).

← variables

locations clocks

- Definition:** The observables $\text{Obs}(\mathcal{N})$ of \mathcal{N} are

$$\{\ell_1, \dots, \ell_n\} \cup \bigcup_{1 \leq i \leq n} V_i$$

with

- $D(\ell_i) = L_i$,
- $D(v)$ as given, $v \in V_i$.

← current location of $\mathcal{A}_{e,1}$
 (would be less confusing if we used $\{\odot_1, \dots, \odot_n\}$)

- 17 - 2013-07-09 - Stobbs -

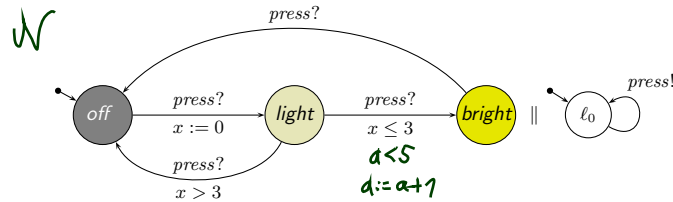
12/38

Observables of TA Network: Example

$\mathcal{A}_{e,i} = (L_i, C_i, B_i, U_i, X_i, V_i, I_i, E_i, l_{ini,i})$.

The observables $\text{Obs}(\mathcal{N})$ of \mathcal{N} are $\{\ell_1, \dots, \ell_n\} \cup \bigcup_{1 \leq i \leq n} V_i$ with

- $\mathcal{D}(\ell_i) = L_i$,
- $\mathcal{D}(v)$ as given, $v \in V_i$.



$$\text{Obs}(\mathcal{N}) = \{\ell_1, \ell_2, d\}$$

$$\mathcal{D}(\ell_1) = \{\text{off}, \text{light}, \text{bright}\} \quad \mathcal{D}(\ell_2) = \{\ell_0\}$$

$$\mathcal{D}(d) = \{0, \dots, 5\}$$

References

References

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