Real-Time Systems

Lecture 17: Automatic Verification of DC Properties for TA

2013-07-09

Dr. Bernd Westphal

Albert-Ludwigs-Universität Freiburg, Germany
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
You Are Here
Content

Introduction

- First-order Logic
- Duration Calculus (DC)
- Semantical Correctness
  Proofs with DC
- DC Decidability
- DC Implementables

PLC-Automata

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

Timed Automata (TA), Uppaal

- Networks of Timed Automata
- Region/Zone-Abstraction
- Extended Timed Automata
- Undecidability Results

Automatic Verification...

...whether TA satisfies DC formula, observer-based

Recap
Observer-based Automatic Verification of DC Properties for TA
Model-Checking DC Properties with Uppaal

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

\[ \xi = \langle \text{off} \rangle, 0 \xrightarrow{2.5} \langle \text{off} \rangle, 2.5 \xrightarrow{\tau} \langle \text{light} \rangle, 2.5 \xrightarrow{2.0} \langle \text{light} \rangle, 4.5 \xrightarrow{\tau} \langle \text{bright} \rangle, 4.5 \ldots \]

Construct interpretation \( L_I(\xi) : \text{Time} \rightarrow \{\text{off}, \text{light}, \text{bright}\} : \)
Example 2: Another Single Run

\[ \xi = \langle \text{off}, 0 \rangle, 0 \xrightarrow{2.5} \langle \text{off}, 2.5 \rangle, 2.5 \xrightarrow{\tau} \langle \text{light}, 0 \rangle, 2.5 \xrightarrow{\tau} \langle \text{bright}, 0 \rangle, 2.5 \xrightarrow{\tau} \langle \text{off}, 0 \rangle, 2.5 \xrightarrow{1.0} \ldots \]

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 $\mathcal{I}_\xi$ 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 $\forall \xi \in \text{CompPaths}(\mathcal{N}) : \mathcal{I}_\xi \models F$. 

---

![Diagram of timed automata states and transitions](image-url)
Observables of TA Network

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

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

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).

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

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

with

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

Current location of $A_{e,i}$

(should be less confusing if we used $\{0, \ldots, \Theta_n\}$)
$$\mathcal{A}_{e,i} = (L_i, C_i, B_i, U_i, X_i, V_i, I_i, E_i, \ell_{ini,i}).$$

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

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

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

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

$$\mathcal{D}(\ell_2) = \{\ell_0\}$$

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