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
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

PLC-Automata

\[ \text{obs} : \text{Time} \to \mathcal{P}(\text{obs}) \]

\[ \langle \text{obs}_0, \nu_0 \rangle, t_0 \xrightarrow{\lambda_0} \langle \text{obs}_1, \nu_1 \rangle, t_1 \ldots \]

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**: $F = \Box \langle \text{off} \rangle$ or $F = \neg \Diamond \langle \text{light} \rangle$
    (Use Uppaal’s fragment of TCTL, something like $\forall \Box \langle \text{off} \rangle$, but not exactly (see later).)
  - **Maybe**: $F = \tau > 5 \implies \Diamond \langle \text{off} \rangle$
  - **Not so clear**: $F = \neg \Diamond (\langle \text{bright} \rangle ; \langle \text{light} \rangle)$

**Example: Let’s Start With Single Runs**

$\xi = \langle \text{off}, 0 \rangle, 0 \overset{2.5}{\rightarrow} \langle \text{off}, 2.5 \rangle, 2.5 \overset{\tau}{\rightarrow} \langle \text{light}, 0 \rangle, 2.5 \overset{2.0}{\rightarrow} \langle \text{light}, 2.0 \rangle, 4.5 \overset{\tau}{\rightarrow} \langle \text{bright}, 2.0 \rangle, 4.5 \ldots$

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

- $L_\xi(\xi)(\text{off})$
- $L_\xi(\xi)(\text{light})$
- $L_\xi(\xi)(\text{bright})$

- $\tau$
Example 2: Another Single Run

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

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 \( \mathcal{A}_e \), \( i = (L_i, C_i, B_i, U_i, X_i, V_i, I_i, E_i, \ell_{\text{ini}}, i) \)
- Define observables \( \text{Obs}(\mathcal{N}) \) of \( \mathcal{N} \).
- Define evolution \( I_\xi \) 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 \( \forall \xi \in \text{CompPaths}(\mathcal{N}) : I_\xi \models F \).

**Observables of TA Network**

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

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

**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, \( v \in V_i \)

\( \text{current location of } \mathcal{A}_{e,i} \)

(\( \text{would be less confusing} \) if we used \( \{q_0, \ldots, q_n\} \))
Observables of TA Network: Example

\[ \mathcal{A}_{e,i} = (L_i, C_i, B_i, U_i, X_i, V_i, I_i, E_i, \ell_{0;i,i}). \]

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

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

\[ \text{Obs}(\mathcal{N}) = \{\ell_1, \ell_2, a\} \]

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

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

\( D(a) = \{0, \ldots, 5\} \)

References
References