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**

$obs : \mathsf{Time} \to \mathscr{D}(obs)$

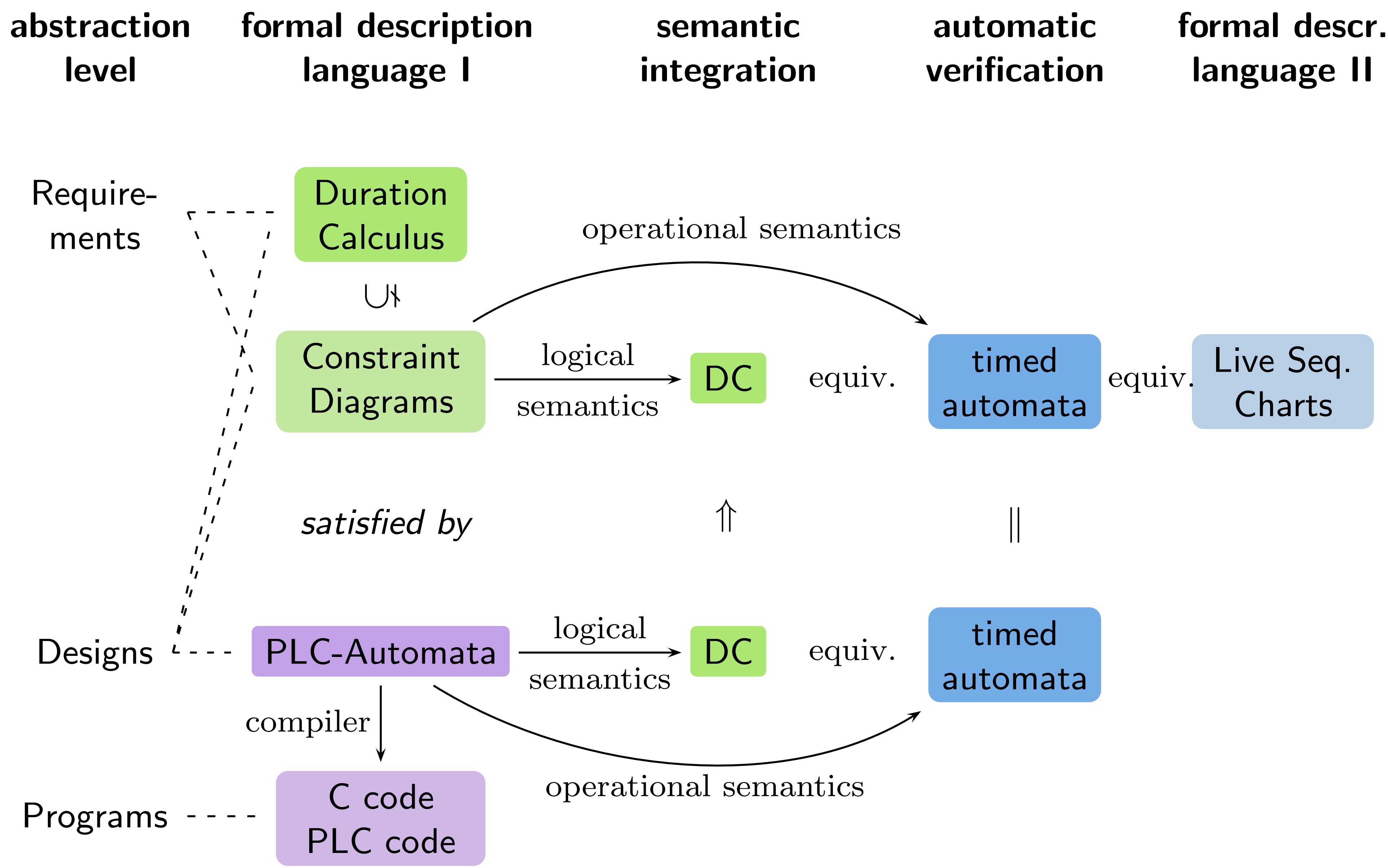
- **Timed Automata** (TA), Uppaal
- Networks of Timed Automata
- Region/Zone-Abstraction
- Extended Timed Automata
- Undecidability Results

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

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

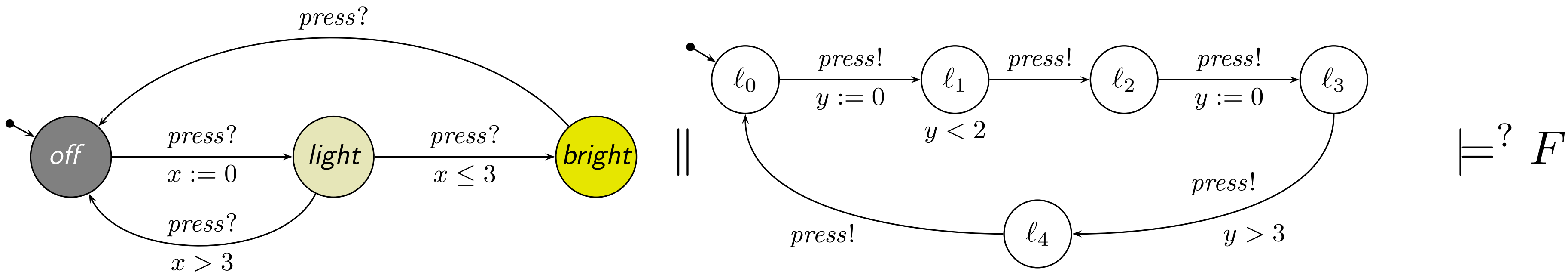
Recap

Tying It All Together



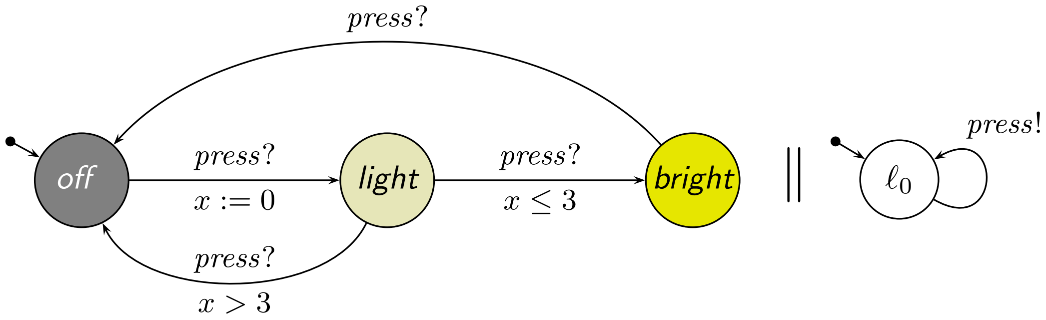
Observer-based Automatic Verification of DC Properties for TA

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**: $F = \Box\lceil \mathsf{off} \rceil$ or $F = \neg\Diamond\lceil \mathsf{light} \rceil$
    (Use Uppaal's fragment of TCTL, something like $\forall\Box\,\mathsf{off}$,
    but not exactly (see later).)
  - **Maybe**: $F = \ell > 5 \implies \Diamond\lceil \mathsf{off} \rceil^5$
  - **Not so clear**: $F = \neg\Diamond(\lceil \mathsf{bright} \rceil \,;\, \lceil \mathsf{light} \rceil)$

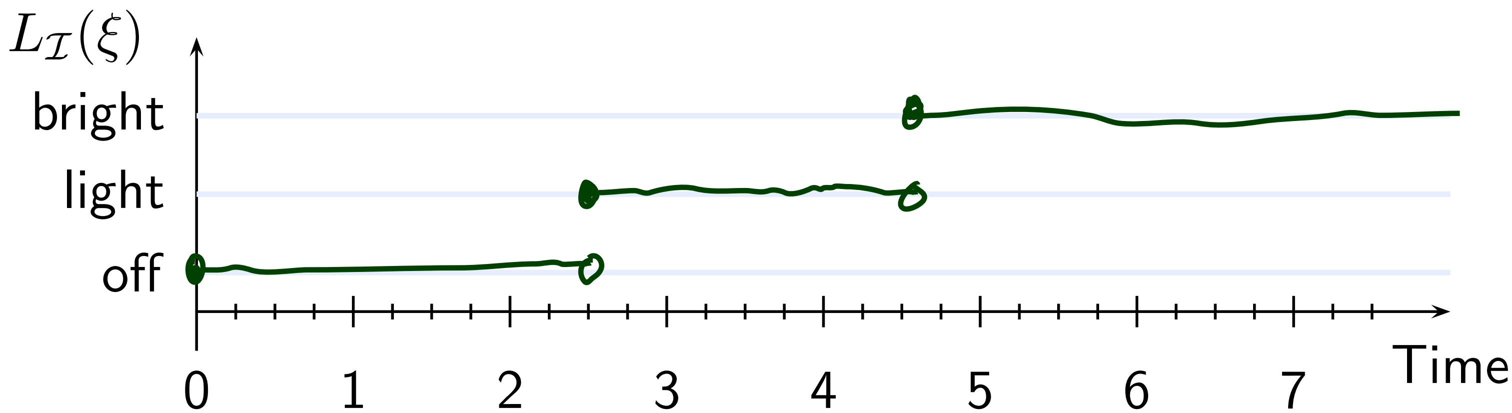
Example: Let's Start With Single Runs



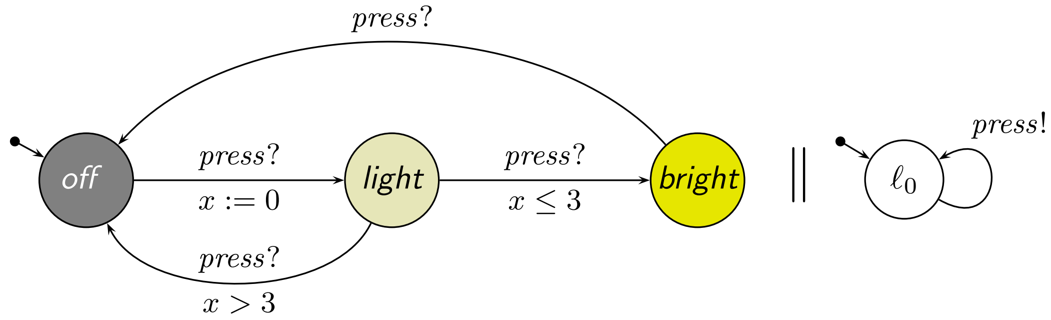
$\models^? \neg\Diamond\lceil \mathsf{light} \rceil$

$$\xi = \langle {\mathsf{off} \atop 0} \rangle, 0 \xrightarrow{2.5} \langle {\mathsf{off} \atop 2.5} \rangle, 2.5 \xrightarrow{\tau} \langle {\mathsf{light} \atop 0} \rangle, 2.5 \xrightarrow{2.0} \langle {\mathsf{light} \atop 2.0} \rangle, 4.5 \xrightarrow{\tau} \langle {\mathsf{bright} \atop 2.0} \rangle, 4.5 \ldots$$

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



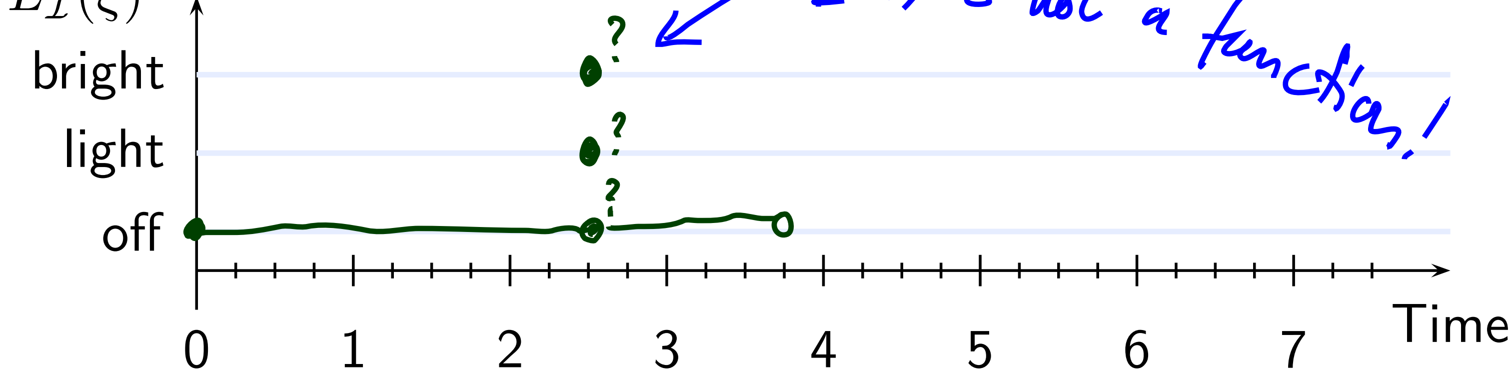
Example 2: Another Single Run



$\models^? \neg\Diamond\lceil\mathsf{light}\rceil$

$$\xi = \left\langle \begin{matrix}\mathsf{off}\\0\end{matrix}\right\rangle, 0 \xrightarrow{2.5} \left\langle \begin{matrix}\mathsf{off}\\2.5\end{matrix}\right\rangle, 2.5 \xrightarrow{\tau} \left\langle \begin{matrix}\mathsf{light}\\0\end{matrix}\right\rangle, 2.5 \xrightarrow{\tau} \left\langle \begin{matrix}\mathsf{bright}\\0\end{matrix}\right\rangle, 2.5 \xrightarrow{\tau} \left\langle \begin{matrix}\mathsf{off}\\0\end{matrix}\right\rangle, 2.5 \xrightarrow{1.0} \dots$$

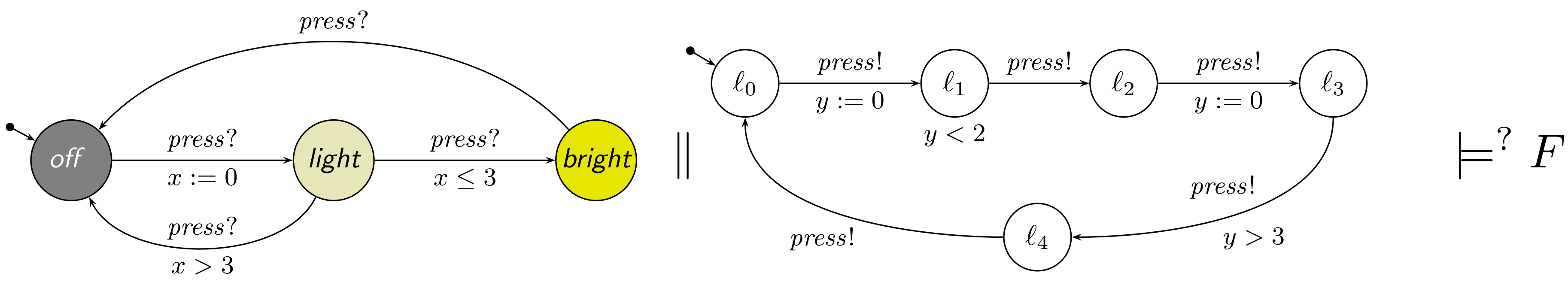
this $L_\mathcal{I}(\xi)$ is not a function!



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

Observables of TA Network

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

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

locations clocks

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

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

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

current location of $\mathcal{A}_{e,1}$
(would be less confusing if we used {☺$_1$, ..., ☺$_n$}

with

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

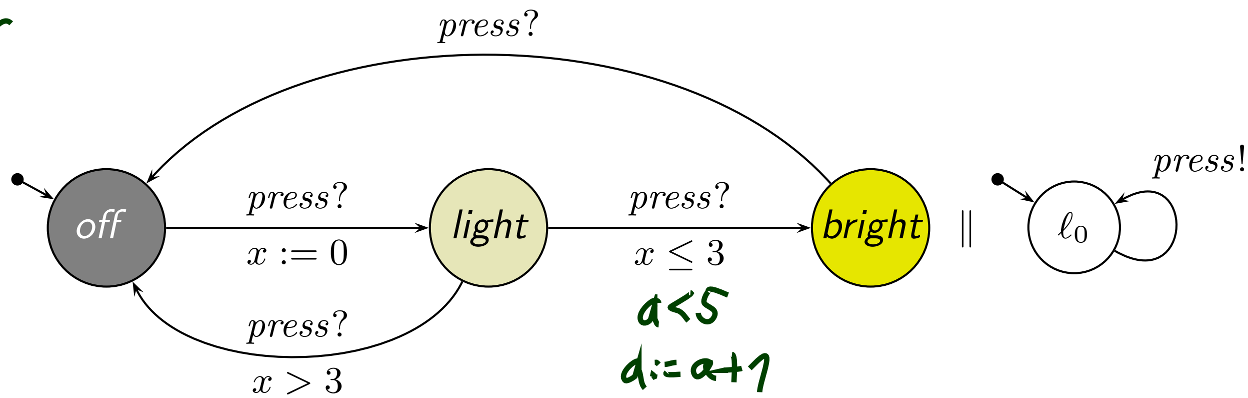
Observables of TA Network: Example

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

The observables 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, $v \in V_i$.

$\mathcal{N}$



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

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

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

References

References

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