Predicate Abstraction for Dense Real-Time Systems

Oliver Möller, Harald Rueß, Maria Sorea

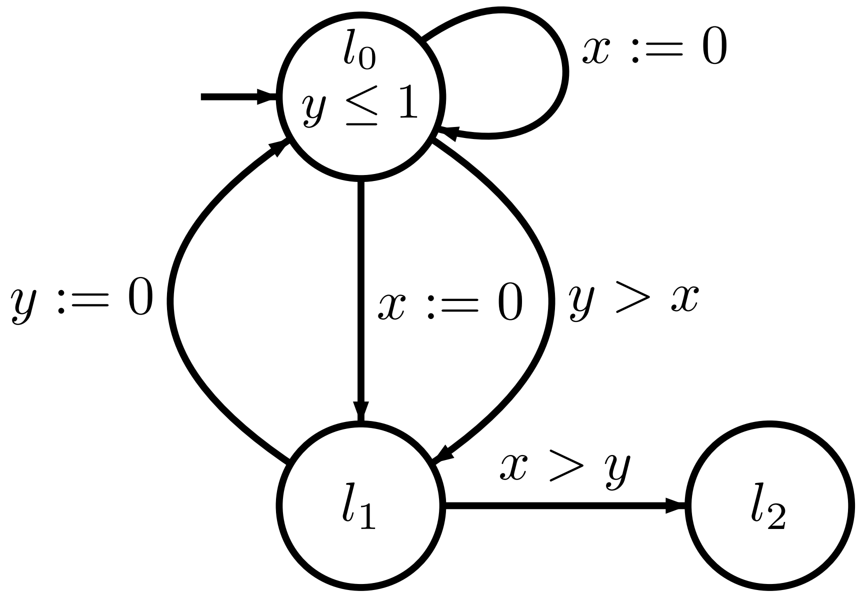
Outline

1. Framework
   - Timed systems
   - Propositional μ-calculus
2. Model Checking in infinite state systems
3. Predicate abstraction of timed systems
4. Restricted semantics of timed systems
5. Theorem: Soundness of abstraction
6. Basis: Completeness of abstraction
7. Refinement of the abstraction

Timed Systems

Timing constraints Γ, propositional Symbols A

Timed System $\mathcal{S} = \langle L, P, C, \rightarrow, l_0, I \rangle$



Semantics as transition system $\mathcal{M} = \langle L \times \mathcal{V}_C, P, \Rightarrow, (l_0, \nu_0) \rangle$ with non-zenoness assumption:

if trace in£nite, sum over all delays is ∞

Clock Regions

- Given: $\mathcal{S}$, C, $\tilde{c}$
- Finite partition of the infinite state space
- Clock region: $\mathcal{X}C \subseteq \mathcal{V}_C$ s.t. for all $\chi \in Constr(c)$ and for any two $\nu, \nu' \in \mathcal{X}C$ it is the case that $\nu \models\!\!\!\approx \chi$ if and only if $\nu' \models\!\!\!\approx \chi$
- $\nu_1 \equiv_{\mathcal{S}} \nu_2$

Propositional μ-Calculus

Syntax:

$$\varphi := p \mid \forall\,(\varphi_1 U \varphi_2) \mid \exists\,(\varphi_1 U \varphi_2) \mid Z \mid \mu Z.\varphi \mid \neg\varphi \mid \varphi \wedge \varphi \mid tt$$

Semantics: $[\![\varphi]\!]^{\mathcal{M}}_{\vartheta}$ . . . set of states for which φ holds

Intuitively, an existial (strong) until formula $\exists\,(\varphi_1 U \varphi_2)$ holds in some states s iff φ_1 holds on some path from s until φ_2 holds.

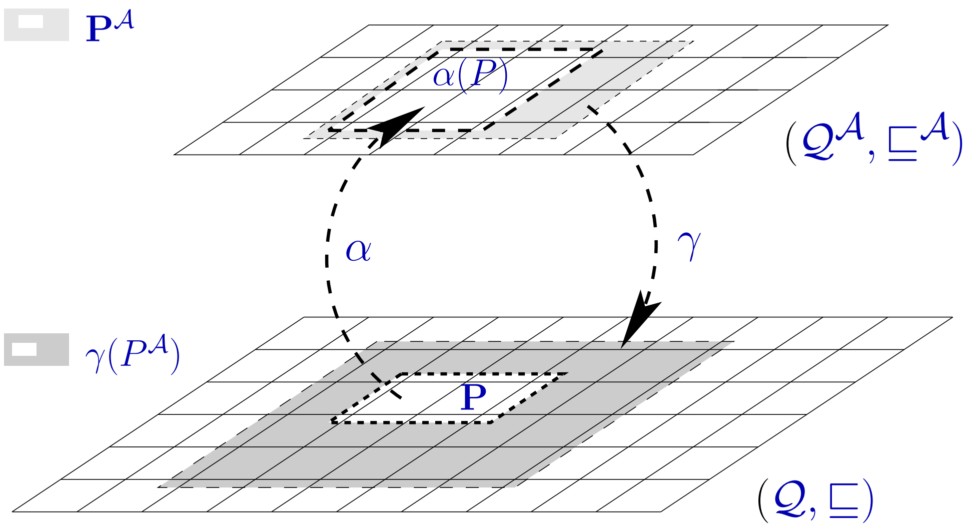
$$[\![\exists\,(\varphi_1 U \varphi_2)]\!]^{\mathcal{M}}_{\vartheta} \stackrel{\text{def}}{=}$$

$$\{s_0 \in S \mid \text{there exists a path } \tau = (s_0 \Rightarrow s_1 \Rightarrow \ldots), \text{ s.t. } s_i \in [\![\varphi_2]\!]^{\mathcal{M}}_{\vartheta} \text{ for some } i \geq 0, \text{ and for all } 0 \leq j < i,\ s_j \in [\![\varphi_1]\!]^{\mathcal{M}}_{\vartheta}\}$$

Model Checking

- Given: $\mathcal{M}$, φ
- Model checking problem: $\mathcal{M} \models \varphi$
- Model checking timed systems: region construction
- Our approach: verify safety and liveness properties of timed systems based on successive re£nements of £nite approximations

Abstract Interpretation: Galois Connections



$(\mathcal{Q}^{\mathcal{A}}, \sqsubseteq^{\mathcal{A}})$ abstract system

$(\mathcal{Q}, \sqsubseteq)$ concrete system

$\alpha : \mathcal{Q} \longrightarrow \mathcal{Q}^{\mathcal{A}}$ abstraction

$\gamma : \mathcal{Q}^{\mathcal{A}} \longrightarrow \mathcal{Q}$ concretization

Essence: connection of 2 lattice structures

Problems: stability and self-loops

Predicate Abstraction of Timed Systems

Abstraction Predicates

- with respect to a given clock set C
- formula with the set of free variables in C
- set of abstractions predicates $\Psi = \{\psi_0, \ldots, \psi_{n-1}\}$

Abstraction function

- $\alpha : \mathcal{V}_C \to B_n$
- $\alpha(\nu)(i) := \psi_i \nu$

Concretization function

- $\gamma : B_n \to \wp(\mathcal{V}_C)$
- $\gamma(b) := \{\nu \in \mathcal{V}_C \mid \bigwedge_{i=0}^{n-1} \psi_i \nu \equiv b(i)\}$

Over-/Under-approximation

Given: $\mathcal{M}$, Ψ

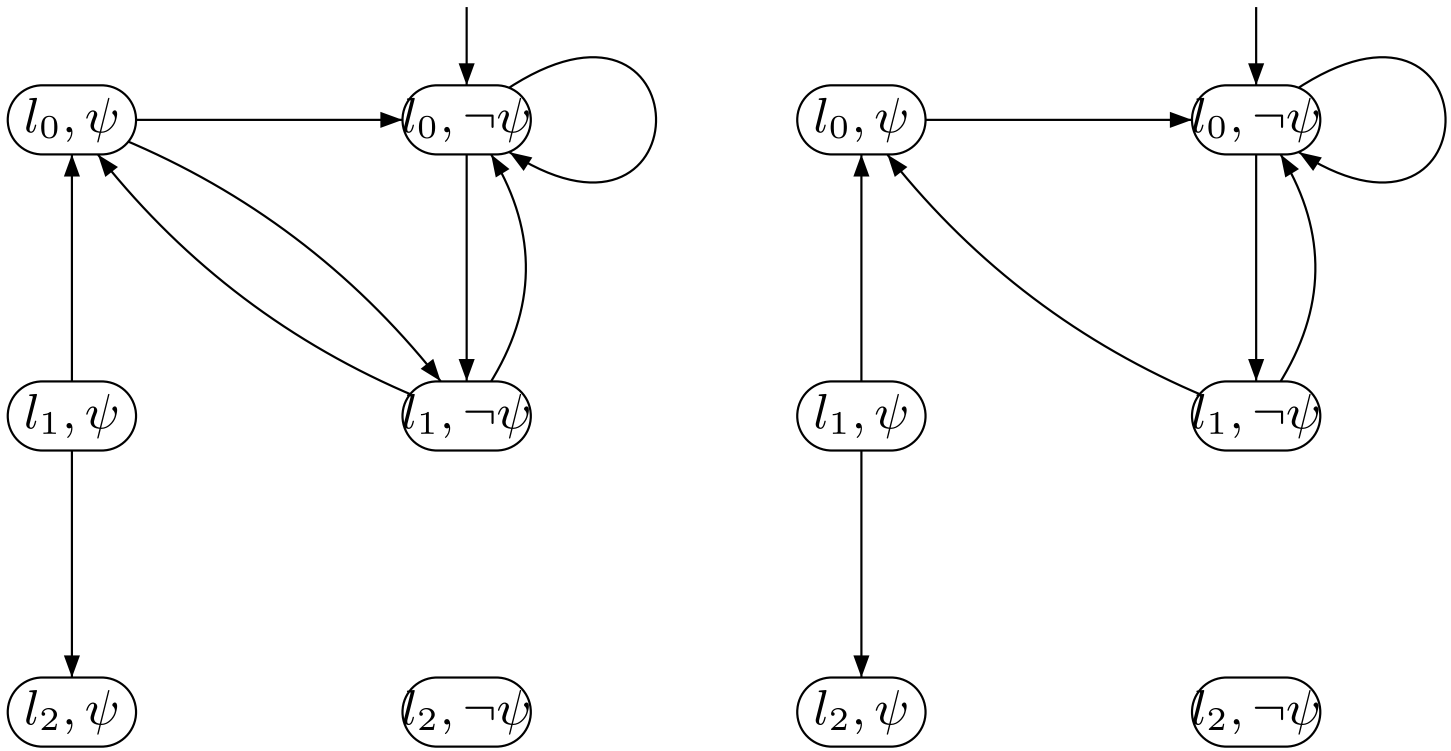
Over-approximation of $\mathcal{M}$: $\mathcal{M}_\Psi^+ = \langle S^A, P, \Rightarrow^+, s_0^A \rangle$

Under-approximation of $\mathcal{M}$: $\mathcal{M}_\Psi^- = \langle S^A, P, \Rightarrow^-, s_0^A \rangle$

- $S^A := L \times B_n$
- $(l, b) \Rightarrow^+ (l', b')$ iff $\exists \nu \in \gamma(b).\ \exists \nu' \in \gamma(b').\ \ (l, \nu) \Rightarrow (l', \nu')$
- $(l, b) \Rightarrow^- (l', b')$ iff $\forall \nu \in \gamma(b).\ \exists \nu' \in \gamma(b').\ \ (l, \nu) \Rightarrow (l', \nu')$
- $s_0^A := (l_0, b_0)$, where $b_0(i) = 1$ if $\psi_i \nu_0$ and 0 otherwise.
- $\Rightarrow^- \subseteq \Rightarrow^+$

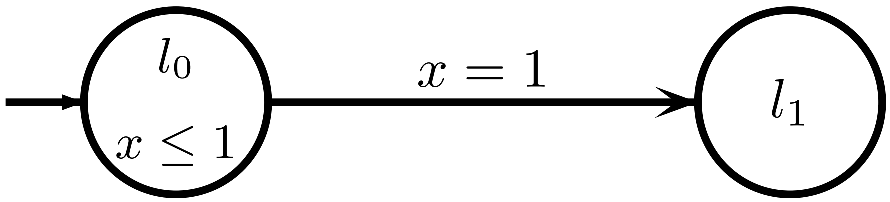
Over-/Under-approximation – Example

$\Psi = \{\psi\}$, where $\psi \equiv x > y$



a: Over-approximation　　　　b: Under-approximation

Example to Abstraction

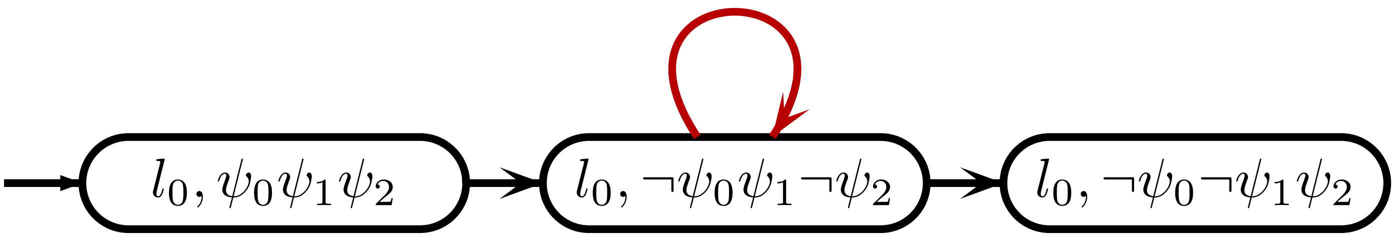


We want to verify: $\varphi = \forall\,(tt\; U\; at\_l_1)$

Abstraction predicates: $\{x = 0, x < 1, x = 1\}$

Assume the following sequence in the concrete system: $(l_0, x = 0) \overset{1/2}{\Rightarrow} (l_0, x = 1/2) \overset{1/2}{\Rightarrow} (l_0, x = 3/4) \overset{3/4}{\Rightarrow} (l_0, x = 1) \overset{\mathbf{true}}{\Rightarrow} (l_1, x = 1)$

Abstraction yields (only a fragment is illustrated):



Problem: spurious self-loop

Restricted Semantics of Timed Systems

Restricted Delay Step

Given: $\mathcal{S}$,C, $\tilde{c}$

A delay step $(l,\nu)\xrightarrow{\delta}(l,(\nu+\delta))$ is a restricted delay step iff

$$\exists x \in C. \exists k \in \{0,\ldots,c\}.\ \nu(x)=k \ \vee\ (\nu(x)<k \wedge \nu(x)+\delta \geq k)$$

Restricted transition relation: $\Rightarrow_R \subseteq (L,\mathcal{V}_C)\times(L,\mathcal{V}_C)$

The second delay step is disallowed:

$$(l_0, x=0) \Rightarrow (l_0, x=1/2) \ \not\Rightarrow (l_0, x=1/4) \Rightarrow (l_0, x=1) \Rightarrow (l_1, x=1)$$

Theorem:

$$[\![\varphi]\!]^{\mathcal{M}}_{\vartheta} \ = \ [\![\varphi]\!]^{\mathcal{M}_{\mathcal{R}}}_{\vartheta}$$

Predicate Abstracted Semantics

$$
\begin{array}{rcl}
[\![tt]\!]_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} & := & S^A \\
[\![p]\!]_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} & := & \{(l,b) \in S^A \mid p \in P(l)\} \\
[\![\varphi_1 \wedge \varphi_2]\!]_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} & := & [\![\varphi_1]\!]_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} \cap [\![\varphi_2]\!]_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} \\
[\![\neg\varphi]\!]_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} & := & S^A \setminus [\![\varphi]\!]_{\vartheta}^{\mathcal{M}_{\Psi}^{\bar{\sigma}}} \\
[\![\exists\,(\varphi_1 U \varphi_2)]\!]_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} & := & \{s_0 \in S^A \mid \text{there exists a path } \tau = (s_0 \Rightarrow^{\sigma} s_1 \Rightarrow^{\sigma} s_1 \ldots), \\
 & & \text{s.t. } s_i \in [\![\varphi_2]\!]_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} \text{ for some } i \geq 0, \text{ and} \\
 & & \text{for all } 0 \leq j < i,\ s_j \in [\![\varphi_1]\!]_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} \\
[\![\forall\,(\varphi_1 U \varphi_2)]\!]_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} & := & \{s_0 \in S^A \mid \text{for every path } \tau = (s_0 \Rightarrow^{\bar{\sigma}} s_1 \Rightarrow^{\bar{\sigma}} \ldots), \\
 & & \text{there exists } i \geq 0 \text{ s.t. } s_i \in [\![\varphi_2]\!]_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}}, \text{ and} \\
 & & \text{for all } 0 \leq j < i,\ s_j \in [\![\varphi_1]\!]_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}}\} \\
[\![Z]\!]_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} & := & \vartheta(Z) \\
[\![\mu Z.\varphi]\!]_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} & := & \cap\{S' \in S^A \mid [\![\varphi]\!]_{\vartheta[Z:=S']}^{\mathcal{M}_{\Psi}^{\sigma}} \subseteq S'\}
\end{array}
$$

Soundness of Abstraction

Theorem:

Given:

$\mathcal{M} = \langle S^C, P, \Rightarrow, s_0^C \rangle$ transition system

Ψ set of predicates

$\mathcal{M}_\Psi^+, \mathcal{M}_\Psi^-$ over-/under-approximations

Then:

$$\gamma(\llbracket\varphi\rrbracket^{\mathcal{M}_\Psi^-}) \subseteq \llbracket\varphi\rrbracket^{\mathcal{M}} \subseteq \gamma(\llbracket\varphi\rrbracket^{\mathcal{M}_\Psi^+})$$

Example

Safety: Location l_2 is never reached $\varphi := \neg\exists\,(\mathit{tt}\,U\,at\_l_2)$

Abstraction predicate: $\psi \equiv x > y$

$$\begin{aligned}
[\![\neg\exists\,(\mathit{tt}\,U\,at_l_2)]\!]^{\mathcal{M}^{-}_{\{\psi\}}} &= S^A \setminus [\![\neg\exists\,(\mathit{tt}\,U\,at_l_2)]\!]^{\mathcal{M}^{+}_{\{\psi\}}} \\
&= S^A \setminus \{(l_1,\psi),(l_2,\psi),(l_2,\neg\psi)\} \\
&= \{(l_0,\psi),(l_0,\neg\psi),(l_1,\neg\psi)\}
\end{aligned}$$

Note: $\mathcal{M}^{+}_{\{\psi\}} = \mathcal{M}^{-}_{\{\psi\}}$

$$\gamma([\![\varphi]\!]^{\mathcal{M}^{-}_{\{\psi\}}}) = [\![\varphi]\!]^{\mathcal{M}} = \gamma([\![\varphi]\!]^{\mathcal{M}^{+}_{\{\psi\}}})$$

Basis

For a given timed automaton, a *basis* is a set Ψ of predicates such that for all clock evaluations ν_1, ν_2:

$$(\forall \psi \in \Psi.\ \psi\nu_1 \Leftrightarrow \psi\nu_2) \quad \Rightarrow \quad \nu_1 \equiv_{\mathcal{S}} \nu_2$$

One basis for our example:

$$\Psi := \{x = 0, y = 0, x \leq 1, x \geq 1, y \leq 1, y \geq 1, x > y, x < y\}$$

Completeness

Theorem

Let Ψ be a basis.

Then our abstraction is strongly preserving with respect to the μ-calculus without next-operator

$$[\![\varphi]\!]_{\vartheta}^{\mathcal{M}_{\Psi}^{-}} = [\![\varphi]\!]_{\vartheta}^{\mathcal{M}_{\Psi}^{+}}$$

Refinement of the Abstraction

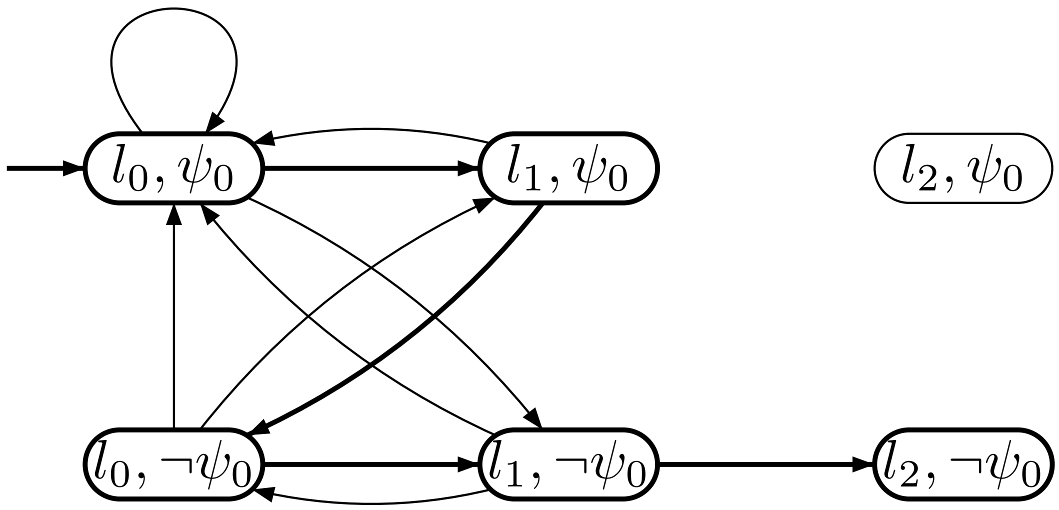
- Basis: the "exact" abstract transition system can be computed Not practicable
- Successive approximation of the abstract transition relation
- Counterexamples
- Given: $\mathcal{M}$, Ψ, φ
- Algorithm for computing $\mathcal{M}_{\psi}^{+}$ stepwise s.t. ($\psi \subseteq \Psi$)
  $\mathcal{M} \models \varphi$ iff $\mathcal{M}_{\psi}^{+} \models \varphi$

Example (Refinement)

$$\varphi := \neg\exists\,(tt\,U\,at\_l_2)$$

$$\Psi := \{x = 0, y = 0, x \leq 1, x \geq 1, y \leq 1, y \geq 1, x > y, x < y\}$$

I. $\psi_0 \equiv x = 0$



$\mathcal{M}^{+}_{\{x=0\}} \overset{?}{\models} \varphi$ NO

$$\tau = ((l_0, \psi_0) \Rightarrow^{+} (l_1, \psi_0) \Rightarrow^{+} (l_0, \neg\psi_0) \Rightarrow^{+} (l_1, \neg\psi_0) \Rightarrow^{+} (l_2, \neg\psi_0))$$

Example – Continuation I.

$$\tau = (\underbrace{(l_0, \psi_0)}_{s_0} \Rightarrow^+ \underbrace{(l_1, \psi_0)}_{s_1} \Rightarrow^+ \underbrace{(l_0, \neg\psi_0)}_{s_2} \Rightarrow^+ \underbrace{(l_1, \neg\psi_0)}_{s_3} \Rightarrow^+ \underbrace{(l_2, \neg\psi_0)}_{s_4})$$

Is there a corresponding counterexample on the concrete transition system?

$\exists\, \tau^c = (y_0 \Rightarrow y_1 \Rightarrow y_2 \Rightarrow y_3 \Rightarrow y_4)$ s.t.

$y_0 \in \gamma(s_0),\ y_1 \in \gamma(s_1),\ y_2 \in \gamma(s_2),\ y_3 \in \gamma(s_3),\ y_4 \in \gamma(s_4),\ y_0 = s_0^c$

$$\begin{aligned} F \ := \ \exists\, y_0, y_1, y_2, y_3, y_4 \in S^C.\ & y_0 \in \gamma(s_0) \ \wedge\ y_1 \in \gamma(s_1) \ \wedge \\ & y_2 \in \gamma(s_2) \ \wedge\ y_3 \in \gamma(s_3) \ \wedge\ y_4 \in \gamma(s_4) \ \wedge \\ & y_1 \Rightarrow y_2 \ \wedge\ y_2 \Rightarrow y_3 \ \wedge\ y_3 \Rightarrow y_4 \ \wedge\ y_0 = s_0^c \end{aligned}$$

Is F valid?

Example – Continuation II.

Here F is unsatisfiable!

$$
\begin{array}{lcr}
y_0 \in & (l_0, x = y = 0) & \in \gamma(s_0) \\
 & \Downarrow & \\
y_1 \in & (l_1, x = 0 \land 0 \leq y \leq 1) & \in \gamma(s_1) \\
 & \Downarrow & \\
y_2 \in & (l_0, x > 0 \land y \leq 1 \land x \geq y) & \in \gamma(s_2) \\
 & \Downarrow & \\
y_3 \in & (l_1, x > 0 \land y > x) & \in \gamma(s_3) \\
 & \not\Downarrow & \\
y_4 \in & (l_1, x > 0 \land y \geq 0) & = \gamma(s_4)
\end{array}
$$

Example – Continuation III.

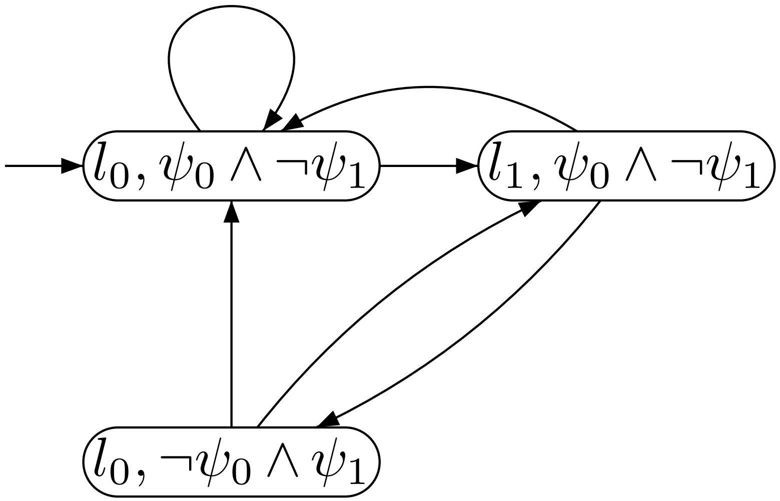
Let k s.t.

1. $\exists\,(y_0 \Rightarrow \cdots \Rightarrow y_k)$
2. $y_i \in \gamma(s_i)$ forall $0 \leq i \leq k$ $\quad$ $k = 3$
3. $\forall\, y_{k+1} \in \gamma(s_{k+1}).\, y_k \not\Rightarrow y_{k+1}$

Choose $\psi_1 \in \Psi$ s.t. $\forall\, y_1 \in \gamma(s_k),\ y_2 \in \gamma(s_{k+1}).\, y_1 \not\Rightarrow y_2$
In our case: $\psi_1 \equiv x > y$

Example – Continuation IV.

New approximation $\mathcal{M}^{+}_{\{x=0,x>y\}}$
Satisfies formula $\varphi = \neg\exists\,(tt\,U\,at\_l_2)$



Algorithm terminates with **true**

$\mathcal{M} \models \neg\exists\,(tt\,U\,at\_l_2)$

What can be verified ?

Safety

Liveness

Observations:

- self-loops problem:
  solved by resticing the delay steps in *concrete* system
- logic does it un-timed and *without next*
- a weaker assumption than non-zenoness suffices
  (only restict infinite sequences of delay steps)

Bibliography

[MRS01] M. Oliver Möller, Harald Rueß, and Maria Sorea. Predicate abstraction for dense real-time systems. Research Series RS-01-44, BRICS, Department of Computer Science, University of Aarhus, November 2001. available at http://www.brics.dk/RS/01/44.