

Predicate Abstraction for Dense Real-Time Systems

Oliver Möller¹, Harald Rueß², Maria Sorea²

¹  BRICS

Århus, Denmark

omoeller@brics.dk

² **SRI International**

Menlo Park, California, USA

{ruess,sorea}@cs1.sri.com

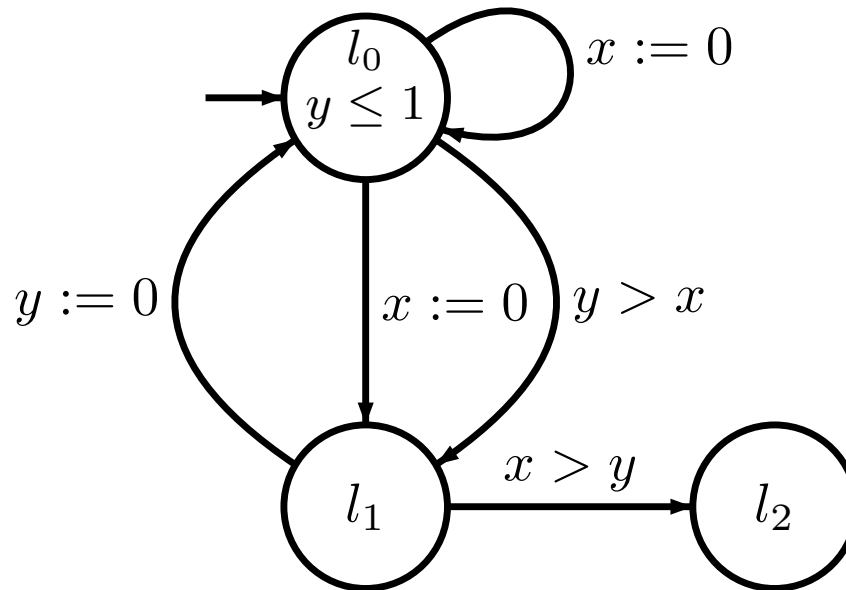
Outline

- 1 Framework
 - Timed systems
 - Propositional μ -calculus
- 2 Predicate abstraction of timed systems
- 3 Restricted delay steps
- 4 Completeness of Refinement Algorithm
- 5 Small Example

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 infinite, 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 $\chi \in \text{Constr}(c)$ and for any two $\nu, \nu' \in \mathcal{X}C$ it is the case that $\nu \models \chi$ if and only if $\nu' \models \chi$
- $\nu_1 \equiv_{\mathcal{S}} \nu_2$

Propositional Next-Free 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: $\llbracket \varphi \rrbracket_{\vartheta}^{\mathcal{M}}$... set of states for which φ holds

Intuitively, an existential (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.

$$\llbracket \exists (\varphi_1 U \varphi_2) \rrbracket_{\vartheta}^{\mathcal{M}} \stackrel{\text{def}}{=}$$

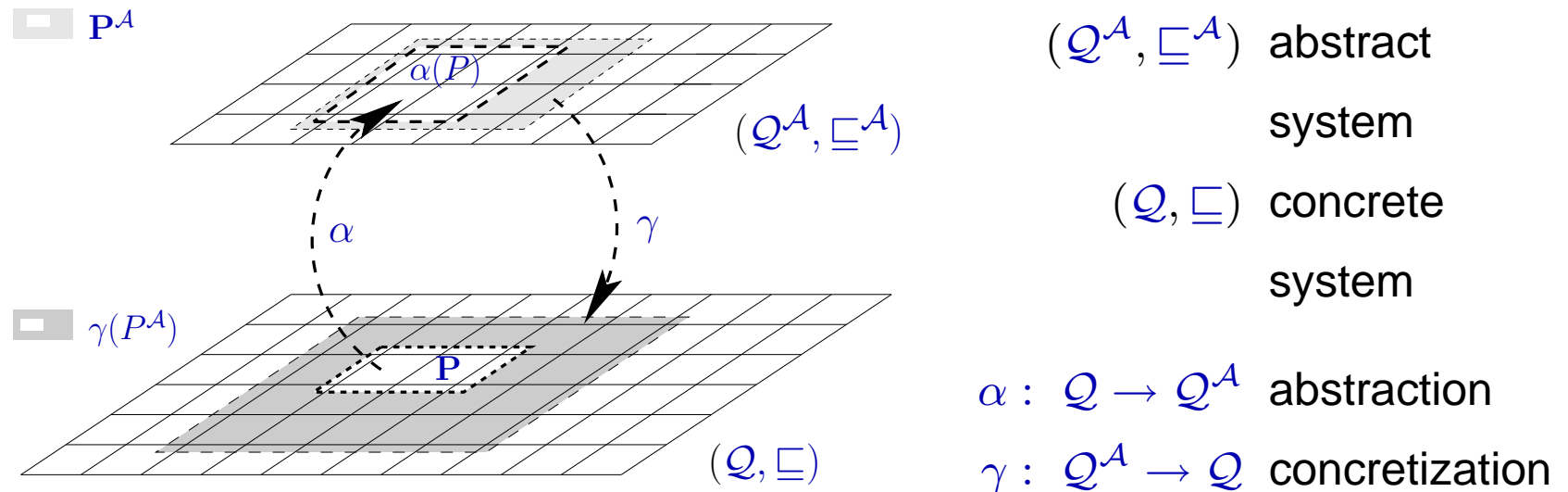
$\{s_0 \in S \mid \text{there exists a path } \tau = (s_0 \Rightarrow s_1 \Rightarrow \dots), \text{ s.t. } s_i \in \llbracket \varphi_2 \rrbracket_{\vartheta}^{\mathcal{M}}$

for some $i \geq 0$, and for all $0 \leq j < i$, $s_j \in \llbracket \varphi_1 \rrbracket_{\vartheta}^{\mathcal{M}}\}$

Model Checking

- Given: \mathcal{M}, φ
- Model checking problem: $l_0 \stackrel{?}{\in} \llbracket \varphi \rrbracket^{\mathcal{M}} \rightarrow \mathbf{Yes/No}$
- Finite quotient for timed systems: region construction
- Our approach: successive refinements of finite approximations

Abstract Interpretation: Galois Connections



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 $\Psi = \{\psi_0, \dots, \psi_{n-1}\}$

Abstraction function

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

Concretization function

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

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 $\exists \nu \in \gamma(b). \exists \nu' \in \gamma(b'). (l, \nu) \Rightarrow (l', \nu')$

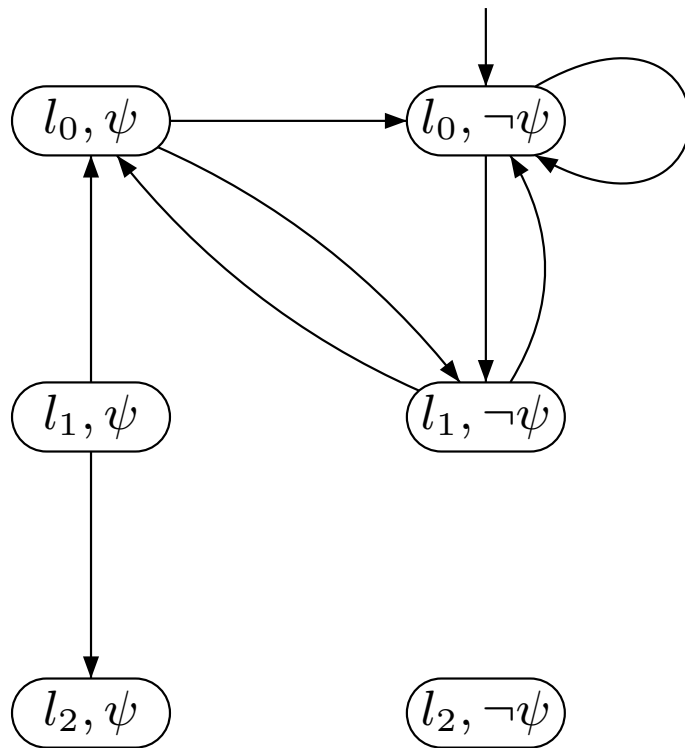
- $(l, b) \Rightarrow^{-} (l', b')$ iff $\forall \nu \in \gamma(b). \exists \nu' \in \gamma(b'). (l, \nu) \Rightarrow (l', \nu')$

- $s_0^A := (l_0, b_0)$, where $b_0(i) = 1$ if $\psi_i \nu_0$ and **0** otherwise.

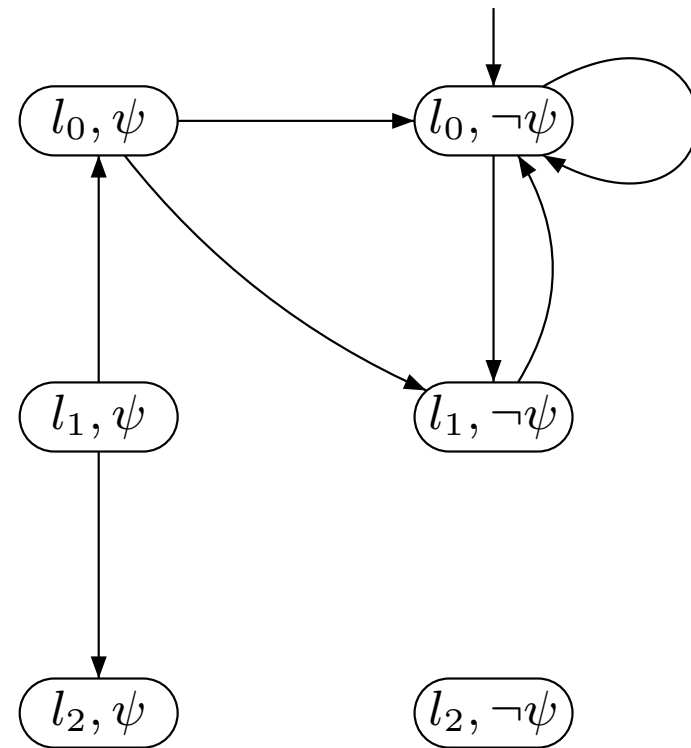
- $\Rightarrow^{-} \subseteq \Rightarrow^{+}$

Over-/Under-Approximation – Example

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

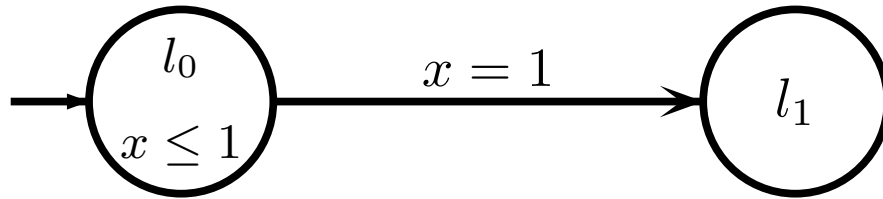


a: Over-Approximation



b: Under-Approximation

Example for Abstraction



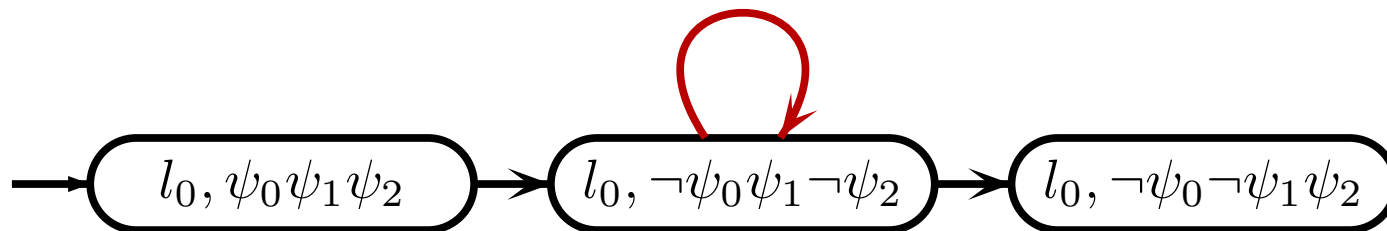
We want to verify: $\varphi = \forall (tt \ U \ at_l_1)$

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

Assume the following sequence in the concrete trace:

$(l_0, x = 0) \xrightarrow{1/2} (l_0, x = 1/2) \xrightarrow{1/4} (l_0, x = 3/4) \xrightarrow{1/4} (l_0, x = 1) \xrightarrow{\text{true}} (l_1, x = 1)$

Abstraction yields (only a fragment is illustrated):



Problem: spurious self-loop

Modified Semantics: 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

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

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

The second delay step in the previous trace is disallowed:

$$(l_0, x = 0) \Rightarrow (l_0, x = 1/2) \not\Rightarrow (l_0, x = 3/4) \Rightarrow (l_0, x = 1) \Rightarrow (l_1, x = 1)$$

Theorem:

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

Predicate Abstracted Semantics

$$\begin{aligned}
 \llbracket tt \rrbracket_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} &:= S^A \\
 \llbracket p \rrbracket_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} &:= \{(l, b) \in S^A \mid p \in P(l)\} \\
 \llbracket \varphi_1 \wedge \varphi_2 \rrbracket_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} &:= \llbracket \varphi_1 \rrbracket_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} \cap \llbracket \varphi_2 \rrbracket_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} \\
 \llbracket \neg \varphi \rrbracket_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} &:= S^A \setminus \llbracket \varphi \rrbracket_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} \\
 \llbracket \exists (\varphi_1 U \varphi_2) \rrbracket_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} &:= \{s_0 \in S^A \mid \text{there exists a path } \tau = (s_0 \Rightarrow^{\sigma} s_1 \Rightarrow^{\sigma} s_2 \dots), \\
 &\quad \text{s.t. } s_i \in \llbracket \varphi_2 \rrbracket_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} \text{ for some } i \geq 0, \text{ and} \\
 &\quad \text{for all } 0 \leq j < i, s_j \in \llbracket \varphi_1 \rrbracket_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}}\} \\
 \llbracket \forall (\varphi_1 U \varphi_2) \rrbracket_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} &:= \{s_0 \in S^A \mid \text{for every path } \tau = (s_0 \Rightarrow^{\bar{\sigma}} s_1 \Rightarrow^{\bar{\sigma}} \dots), \\
 &\quad \text{there exists } i \geq 0 \text{ s.t. } s_i \in \llbracket \varphi_2 \rrbracket_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}}, \text{ and} \\
 &\quad \text{for all } 0 \leq j < i, s_j \in \llbracket \varphi_1 \rrbracket_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}}\} \\
 \llbracket Z \rrbracket_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} &:= \vartheta(Z) \\
 \llbracket \mu Z. \varphi \rrbracket_{\vartheta}^{\mathcal{M}_{\Psi}^{\sigma}} &:= \bigcap \{S' \in S^A \mid \llbracket \varphi \rrbracket_{\vartheta[Z:=S']}^{\mathcal{M}_{\Psi}^{\sigma}} \subseteq S'\}
 \end{aligned}$$

Soundness & Completeness

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

Ψ a set of predicates

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

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

Soundness & Completeness

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

Ψ a set of predicates

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

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

$$(\forall \psi \in \Psi. \psi \nu_1 \Leftrightarrow \psi \nu_2) \Rightarrow \nu_1 \equiv_S \nu_2$$

Soundness & Completeness

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

Ψ a set of predicates

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

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

Theorem:

If $(\forall \psi \in \Psi. \psi \nu_1 \Leftrightarrow \psi \nu_2) \Rightarrow \nu_1 \equiv_S \nu_2$

Then $\llbracket \varphi \rrbracket_\nu^{\mathcal{M}_\Psi^-} = \llbracket \varphi \rrbracket_\nu^{\mathcal{M}_\Psi^+}$

Refinement of the Abstraction

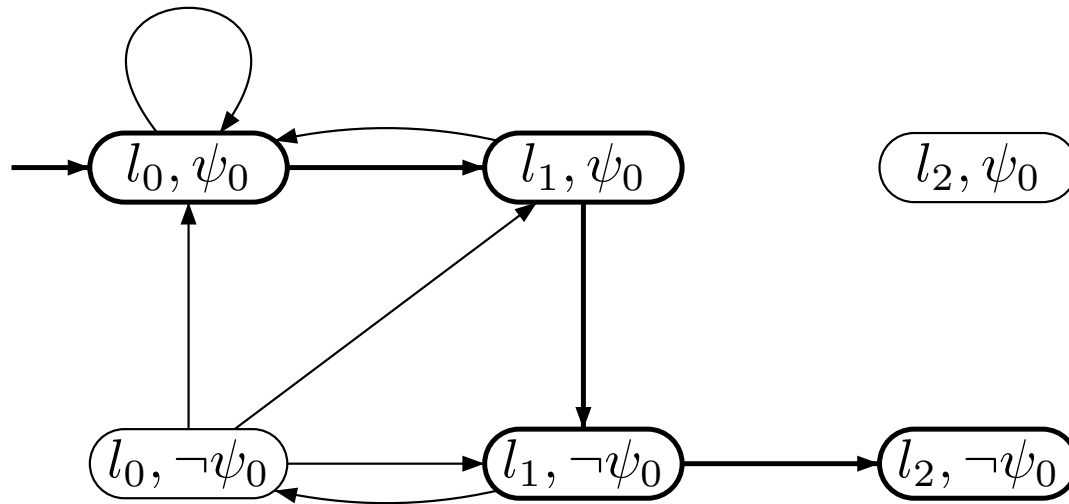
- Basis: the "exact" abstract transition system can be computed
Not practicable
- Successive approximation of the abstract transition relation
- Counterexamples
- Given: $\mathcal{M}, \Psi, \varphi$
- Algorithm for computing \mathcal{M}_ψ^+ stepwise s.t. $(\psi \subseteq \Psi)$
 $\mathcal{M} \models \varphi$ 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. $\psi_0 \equiv x = 0$



$$\mathcal{M}_{\{x=0\}}^+ \stackrel{?}{\models} \varphi$$

NO

$$\tau = \left((l_0, \psi_0) \Rightarrow^+ (l_1, \psi_0) \Rightarrow^+ (l_1, \neg\psi_0) \Rightarrow^+ (l_2, \neg\psi_0) \right)$$

Example – Continuation I.

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

Is there a corresponding counterexample on the concrete transition system?

$$\exists \tau^c = (y_0 \Rightarrow y_1 \Rightarrow y_2 \Rightarrow y_3) \text{ s.t.}$$

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

$$F := \exists y_0, y_1, y_2, y_3 \in S^C.$$

$$y_0 \in \gamma(s_0) \wedge y_1 \in \gamma(s_1) \wedge y_2 \in \gamma(s_2) \wedge y_3 \in \gamma(s_3) \wedge$$

$$y_1 \Rightarrow y_2 \wedge y_2 \Rightarrow y_3 \wedge y_0 = s_0^c$$

Is F valid?

Example – Continuation II.

Here F is unsatisfiable!

$$\begin{array}{l} y_0 \in (l_0, x = y = 0) \in \gamma(s_0) \\ \Downarrow \\ y_1 \in (l_1, x = 0 \wedge 0 \leq y \leq 1) \in \gamma(s_1) \\ \Downarrow \\ y_2 \in (l_1, x > 0 \wedge y > x) \in \gamma(s_2) \\ \Downarrow \\ y_3 \in (l_1, x > 0 \wedge y \geq 0) = \gamma(s_3) \end{array}$$

Example – Continuation III.

Let k s.t.

1. $\exists (y_0 \Rightarrow \dots \Rightarrow y_k)$

2. $y_i \in \gamma(s_i)$ for all $0 \leq i \leq k$

$k = 2$

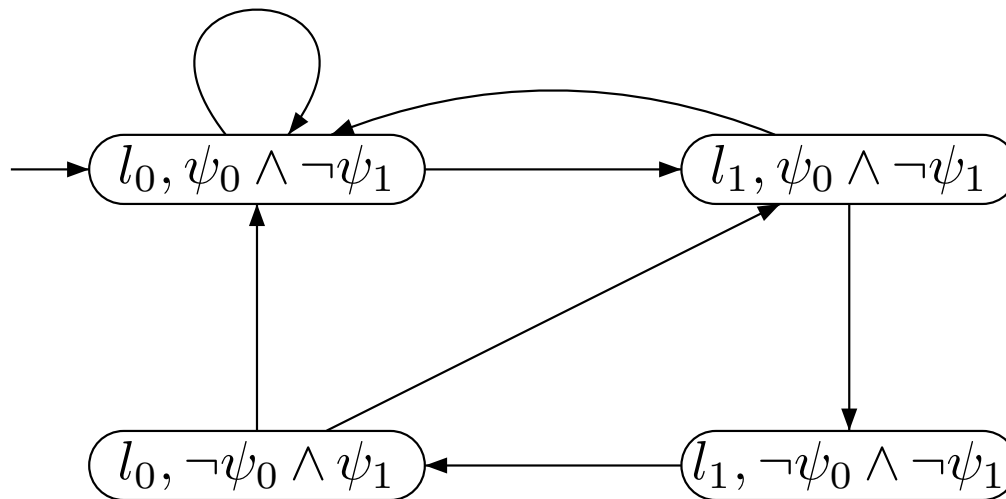
3. $\forall y_{k+1} \in \gamma(s_{k+1}). y_k \not\Rightarrow y_{k+1}$

Choose $\psi_1 \in \Psi$ s.t. $\forall y \in \gamma(s_k), y' \in \gamma(s_{k+1}). y \not\Rightarrow y'$

In our case: $\psi_1 \equiv x > y$

Example – Continuation IV.

New approximation $\mathcal{M}_{\{x=0, x>y\}}^+$
Satisfies formula $\varphi = \neg\exists (tt \text{ U } at_l_2)$



Algorithm terminates with **true**

$(l_0, x = y = 0) \in \llbracket \neg\exists (tt \text{ U } at_l_2) \rrbracket^{\mathcal{M}}$

What can be verified ?

Safety

Liveness

Observations:

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

Bibliography

- [Möl02] M. Oliver Möller. *Structure and Hierarchy in Real-Time Systems*. PhD thesis, BRICS PhD school, University of Aarhus, February 2002. see <http://www.brics.dk/~omoeller/papers/>.
- [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>.