Control of Timed Systems

Habilitation à Diriger les Recherches

Franck Cassez
CNRS/IRCCyN

Nantes, France

September 21st, 2007

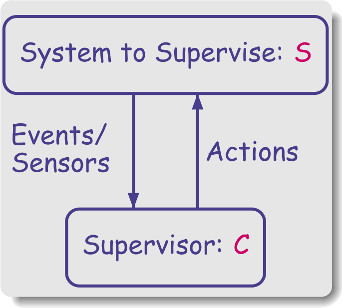
Rapporteurs:

Ahmed Bouajjani	Professor, University of Paris 7, France
Oded Maler	Research Director, CNRS, VERIMAG, Grenoble, France
Jean-François Raskin	Professor, Université Libre de Bruxelles, Belgium

Examinateurs:

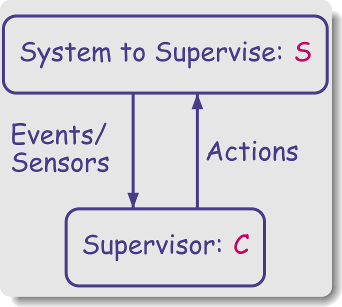
Jean Bézivin	Professor, University of Nantes, France
Claude Jard	Professor, ENS Cachan, Antenne de Bretagne, Rennes, France
Kim G. Larsen	Professor, Aalborg University, Denmark
Jean-Jacques Loiseau	Research Director, CNRS, IRCCyN, Nantes, France
Olivier H. Roux	Assistant Professor (HDR), University of Nantes, France

Research Domain: Design of Real-Time Systems



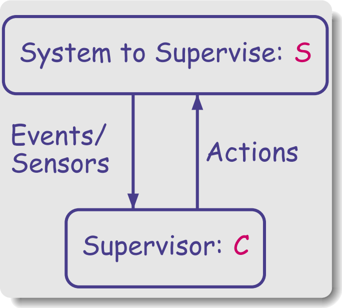
Research Domain: Design of Real-Time Systems

Build Safe Systems



Research Domain: Design of Real-Time Systems

Build Safe Systems

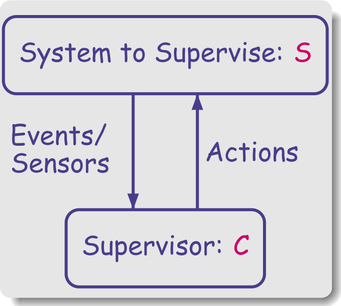


Property φ

Research Domain: Design of Real-Time Systems

Build Safe Systems

Modeling
- Timed Automata
- Time Petri Nets
- Timed Logics

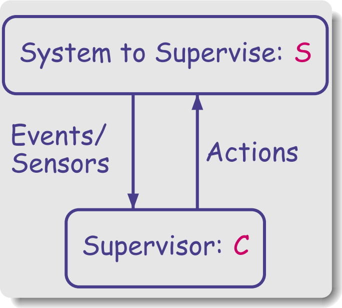


Property φ

Research Domain: Design of Real-Time Systems

Build Safe Systems

Modeling
- Timed Automata
- Time Petri Nets
- Timed Logics



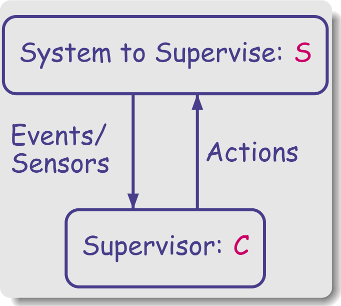
Verification
- Test
- Theorem Proving
- Model-Checking

Property φ

Research Domain: Design of Real-Time Systems

Build Safe Systems

Modeling
- Timed Automata
- Time Petri Nets
- Timed Logics



Diagnosis & Control
- Diagnosis
- Control
- Optimal Control

Verification
- Test
- Theorem Proving
- Model-Checking

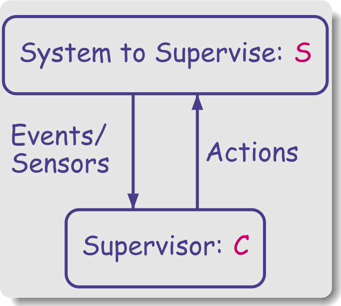
Property φ

Research Domain: Design of Real-Time Systems

Build Safe Systems

Modeling
- Timed Automata
- Time Petri Nets
- Timed Logics

Diagnosis & Control
- Diagnosis
- Control
- Optimal Control



Verification
- Test
- Theorem Proving
- Model-Checking

Property φ

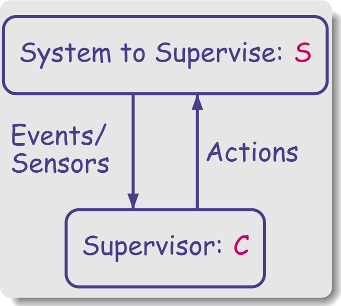
Implementation
- Digital Supervisors
- Continuous Systems

Research Domain: Design of Real-Time Systems

Build Safe Systems

Modeling
- Timed Automata
- Time Petri Nets
- Timed Logics

Diagnosis & Control
- Diagnosis
- Control
- Optimal Control



Verification
- Test
- Theorem Proving
- Model-Checking

Property φ

Implementation
- Digital Supervisors
- Continuous Systems

Outline of the Talk

- Control of Timed Systems: Basics
  - Verification and Control
  - Timed Automata
  - Timed Game Automata
  - Symbolic Algorithms for Timed Game Automata
- Selected Contributions
  - Implementable Controllers
  - Optimal Controllers
- Conclusion & Perspectives

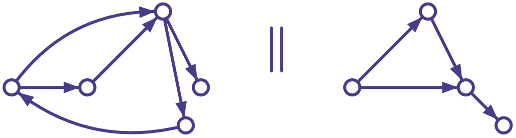
Next:

- Control of Timed Systems: Basics
  - Verification and Control
  - Timed Automata
  - Timed Game Automata
  - Symbolic Algorithms for Timed Game Automata
- Selected Contributions
- Conclusion & Perspectives

Verification and Control

Verification and Control

Modelling



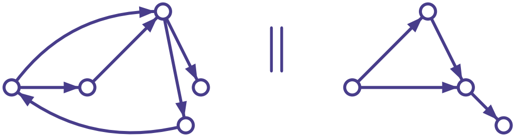
Always (not bad)

$S \quad \| \quad C \quad \models \quad \varphi$

Verification and Control

Does the system meet the specification?

Modelling



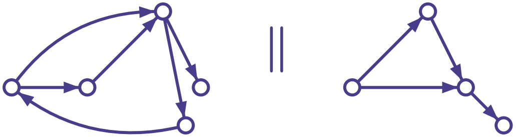
Always (not bad)

$$S \parallel C \models \varphi$$

Verification and Control

Does the system meet the specification?

Modelling



Always (not bad)

$S \parallel C \models \varphi$

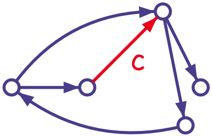
Model Checking Problem

Does the closed system $(S \parallel C)$ satisfy φ ?

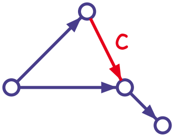
Verification and **Control**

Can we enforce the system to meet the specification?

Modelling



||



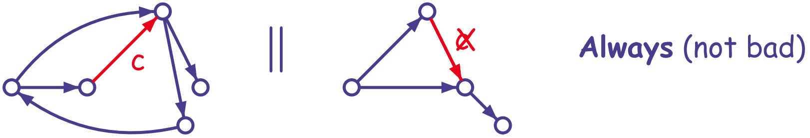
Always (not bad)

$S \quad || \quad C \quad \models \quad \varphi$

Verification and Control

Can we enforce the system to meet the specification?

Modelling

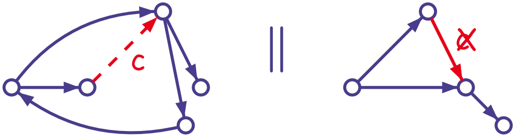


$S \quad \| \quad C \quad \models \quad \varphi$

Verification and Control

Can we enforce the system to meet the specification?

Modelling



$S \;\|\; C \models \varphi$

Control Problem

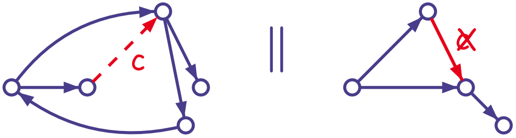
Can the open system S be restricted to satisfy φ ?

Is there a Controller C such that $(S \| C) \models \varphi$?

Verification and **Control**

Can we enforce the system to meet the specification?

Modelling



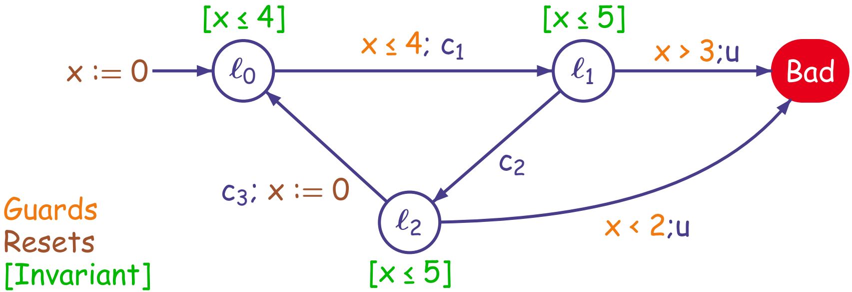
Always (not bad)

$S \;\|\; ?? \;\models\; \varphi$

Control Problem

Can the open system S be restricted to satisfy φ ?
Is there a Controller C such that $(S \,\|\, C) \models \varphi$?

Timed Automaton [Alur & Dill'94]



Timed Automaton = Finite Automaton + clock variables

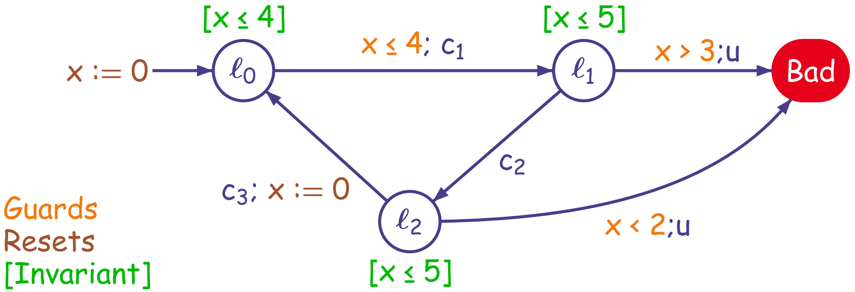
Run = sequence of discrete and time steps

$\rho_1 : \quad (\ell_0, 0) \xrightarrow{1.55} (\ell_0, 1.55) \xrightarrow{c_1} (\ell_1, 1.55) \xrightarrow{1.67} (\ell_1, 3.22) \xrightarrow{u} (Bad, 3.22)$

$\rho_3 : \quad (\ell_0, 0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{2}} (\ell_0, 0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{4}} (\ell_0, 0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{8}} \cdots$

Zeno behaviour

Timed Automaton [Alur & Dill'94]



Timed Automaton = Finite Automaton + clock variables

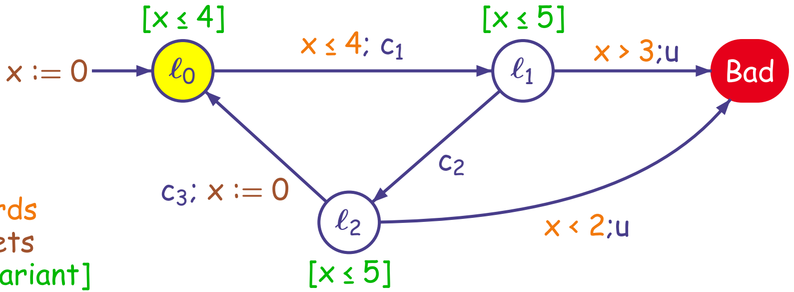
Run = sequence of discrete and time steps

$$\rho_1 : \quad (\ell_0,0) \xrightarrow{1.55} (\ell_0,1.55) \xrightarrow{c_1} (\ell_1,1.55) \xrightarrow{1.67} (\ell_1,3.22) \xrightarrow{u} (Bad,3.22)$$

$$\rho_3 : \quad (\ell_0,0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{2}} (\ell_0,0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{4}} (\ell_0,0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{8}} \cdots$$

Zeno behaviour

Timed Automaton [Alur & Dill'94]



Guards
Resets
[Invariant]

Timed Automaton = Finite Automaton + clock variables

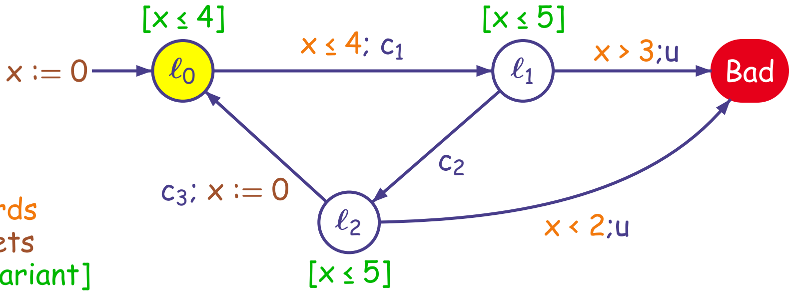
Run = sequence of discrete and time steps

$\rho_1: \quad (\ell_0, 0) \xrightarrow{1.55} (\ell_0, 1.55) \xrightarrow{c_1} (\ell_1, 1.55) \xrightarrow{1.67} (\ell_1, 3.22) \xrightarrow{u} (Bad, 3.22)$

$\rho_3: \quad (\ell_0, 0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{2}} (\ell_0, 0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{4}} (\ell_0, 0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{8}} \cdots$

Zeno behaviour

Timed Automaton [Alur & Dill'94]



Guards
Resets
[Invariant]

Timed Automaton = Finite Automaton + clock variables

Run = sequence of discrete and time steps

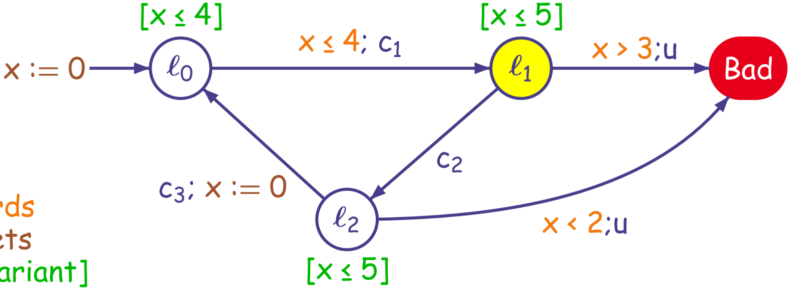
$\rho_1 : \quad (\ell_0, 0) \xrightarrow{1.55} (\ell_0, 1.55) \xrightarrow{c_1} (\ell_1, 1.55) \xrightarrow{1.67} (\ell_1, 3.22) \xrightarrow{u} (Bad, 3.22)$

$\rho_3 : \quad (\ell_0, 0) \xrightarrow{c_1 c_2 c_3 \text{ in } \frac{1}{2}} (\ell_0, 0) \xrightarrow{c_1 c_2 c_3 \text{ in } \frac{1}{4}} (\ell_0, 0) \xrightarrow{c_1 c_2 c_3 \text{ in } \frac{1}{8}} \cdots$

Zeno behaviour

Timed Automaton

[Alur & Dill'94]



Guards
Resets
[Invariant]

Timed Automaton = Finite Automaton + clock variables

Run = sequence of discrete and time steps

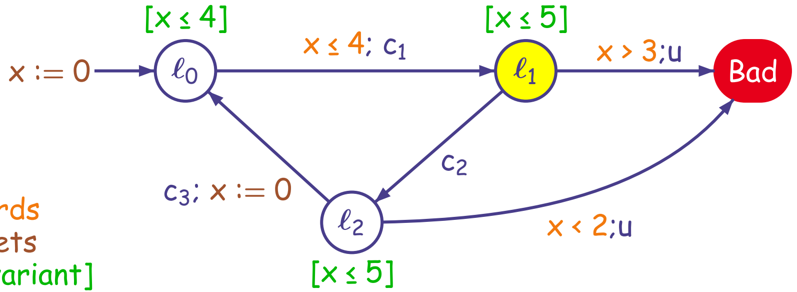
$\rho_1 : \quad (\ell_0, 0) \xrightarrow{1.55} (\ell_0, 1.55) \xrightarrow{c_1} (\ell_1, 1.55) \xrightarrow{1.67} (\ell_1, 3.22) \xrightarrow{u} (Bad, 3.22)$

$\rho_3 : \quad (\ell_0, 0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{2}} (\ell_0, 0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{4}} (\ell_0, 0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{8}} \cdots$

Zeno behaviour

Timed Automaton

[Alur & Dill'94]



Guards
Resets
[Invariant]

Timed Automaton = Finite Automaton + clock variables

Run = sequence of discrete and time steps

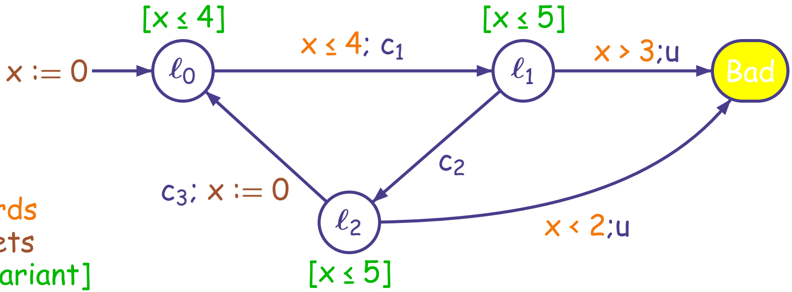
$\rho_1 : \quad (\ell_0, 0) \xrightarrow{1.55} (\ell_0, 1.55) \xrightarrow{c_1} (\ell_1, 1.55) \xrightarrow{1.67} (\ell_1, 3.22) \xrightarrow{u} (\text{Bad}, 3.22)$

$\rho_3 : \quad (\ell_0, 0) \xrightarrow{c_1 c_2 c_3 \text{ in } \frac{1}{2}} (\ell_0, 0) \xrightarrow{c_1 c_2 c_3 \text{ in } \frac{1}{4}} (\ell_0, 0) \xrightarrow{c_1 c_2 c_3 \text{ in } \frac{1}{8}} \cdots$

Zeno behaviour

Timed Automaton

[Alur & Dill'94]



Guards
Resets
[Invariant]

Timed Automaton = Finite Automaton + clock variables

Run = sequence of discrete and time steps

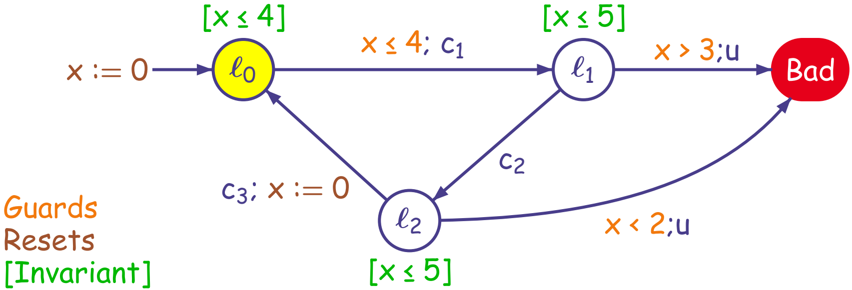
$\rho_1 : \quad (\ell_0, 0) \xrightarrow{1.55} (\ell_0, 1.55) \xrightarrow{c_1} (\ell_1, 1.55) \xrightarrow{1.67} (\ell_1, 3.22) \xrightarrow{u} (\text{Bad}, 3.22)$

$\rho_3 : \quad (\ell_0, 0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{2}} (\ell_0, 0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{4}} (\ell_0, 0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{8}} \cdots$

Zeno behaviour

Timed Automaton

[Alur & Dill'94]



Timed Automaton = Finite Automaton + clock variables

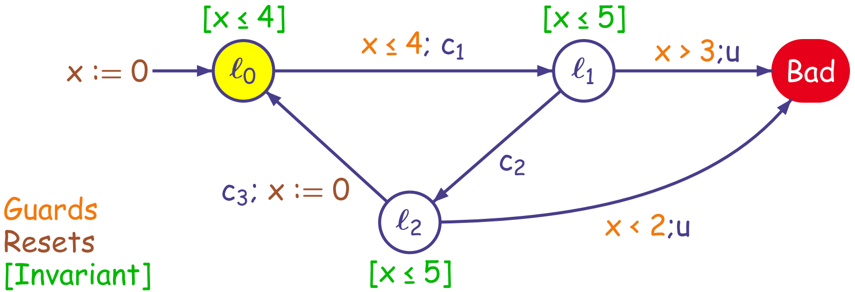
Run = sequence of discrete and time steps

$\rho_1: \quad (\ell_0, 0) \xrightarrow{1.55} (\ell_0, 1.55) \xrightarrow{c_1} (\ell_1, 1.55) \xrightarrow{1.67} (\ell_1, 3.22) \xrightarrow{u} (\mathrm{Bad}, 3.22)$

$\rho_3: \quad (\ell_0, 0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{2}} (\ell_0, 0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{4}} (\ell_0, 0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{8}} \cdots$

Zeno behaviour

Timed Automaton [Alur & Dill'94]



Timed Automaton = Finite Automaton + clock variables

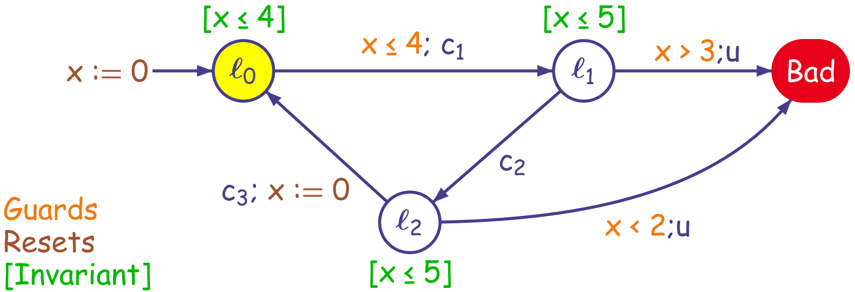
Run = sequence of discrete and time steps

$\rho_1: \quad (\ell_0, 0) \xrightarrow{1.55} (\ell_0, 1.55) \xrightarrow{c_1} (\ell_1, 1.55) \xrightarrow{1.67} (\ell_1, 3.22) \xrightarrow{u} (\mathrm{Bad}, 3.22)$

$\rho_3: \quad (\ell_0, 0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{2}} (\ell_0, 0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{4}} (\ell_0, 0) \xrightarrow{c_1c_2c_3 \text{ in } \frac{1}{8}} \cdots$

Zeno behaviour

Timed Automaton [Alur & Dill'94]



Timed Automaton = Finite Automaton + clock variables

Run = sequence of discrete and time steps

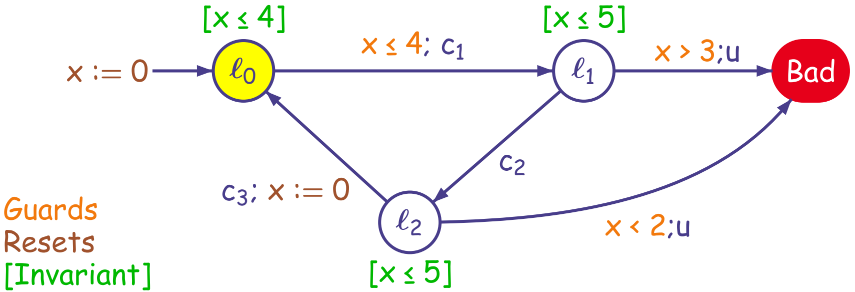
$\rho_1 : \quad (\ell_0, 0) \xrightarrow{1.55} (\ell_0, 1.55) \xrightarrow{c_1} (\ell_1, 1.55) \xrightarrow{1.67} (\ell_1, 3.22) \xrightarrow{u} (\text{Bad}, 3.22)$

$\rho_3 : \quad (\ell_0, 0) \xrightarrow{c_1 c_2 c_3 \text{ in } \frac{1}{2}} (\ell_0, 0) \xrightarrow{c_1 c_2 c_3 \text{ in } \frac{1}{4}} (\ell_0, 0) \xrightarrow{c_1 c_2 c_3 \text{ in } \frac{1}{8}} \cdots$

Zeno behaviour

Timed Automaton

[Alur & Dill'94]



Timed Automaton = Finite Automaton + clock variables

Run = sequence of discrete and time steps

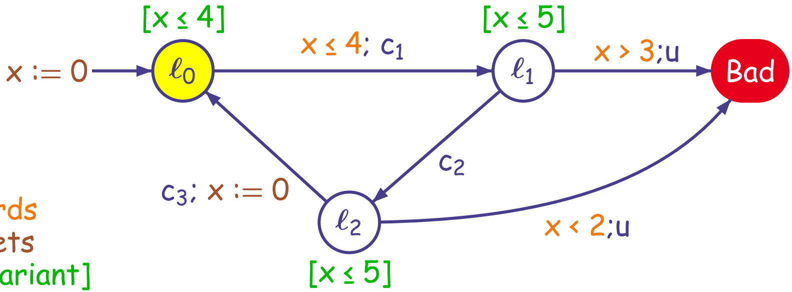
$$\rho_1 : \quad (\ell_0, 0) \xrightarrow{1.55} (\ell_0, 1.55) \xrightarrow{c_1} (\ell_1, 1.55) \xrightarrow{1.67} (\ell_1, 3.22) \xrightarrow{u} (\mathrm{Bad}, 3.22)$$

$$\rho_3 : \quad (\ell_0, 0) \xrightarrow{c_1 c_2 c_3 \text{ in } \frac{1}{2}} (\ell_0, 0) \xrightarrow{c_1 c_2 c_3 \text{ in } \frac{1}{4}} (\ell_0, 0) \xrightarrow{c_1 c_2 c_3 \text{ in } \frac{1}{8}} \cdots$$

Zeno behaviour

Timed Automaton

[Alur & Dill'94]



Guards
Resets
[Invariant]

Timed Automaton = Finite Automaton + clock variables

Run = sequence of discrete and time steps

$\rho_1: \quad (\ell_0, 0) \xrightarrow{1.55} (\ell_0, 1.55) \xrightarrow{c_1} (\ell_1, 1.55) \xrightarrow{1.67} (\ell_1, 3.22) \xrightarrow{u} (\text{Bad}, 3.22)$

$\rho_3: \quad (\ell_0, 0) \xrightarrow{c_1 c_2 c_3 \text{ in } \frac{1}{2}} (\ell_0, 0) \xrightarrow{c_1 c_2 c_3 \text{ in } \frac{1}{4}} (\ell_0, 0) \xrightarrow{c_1 c_2 c_3 \text{ in } \frac{1}{8}} \cdots$

Zeno behaviour

States & Symbolic States

- $Q = L \times \mathbb{R}_{\geq 0}^{Clock}$ is the set of states of the TGA
  $q = (\ell, v) \in Q$
- Discrete Successors of $X \subseteq Q$ by an action a:
  $$Post^a(X) = \{q' \in Q \mid q \xrightarrow{a} q' \text{ and } q \in X\}$$
- Time Successors of $X \subseteq Q$:
  $$Post^\delta(X) = \{q' \in Q \mid \exists t \geq 0 \mid q \xrightarrow{t} q' \text{ and } q \in X\}$$
- Zone = conjunction of triangular constraints
  $x - y < 3, x \geq 2 \wedge 1 < y - x < 2$
- Symbolic State is defined by a State predicate (SP)
  $P = \cup_{i \in [1..n]}(\ell_{j_i}, Z_i)$, $\ell_{j_i} \in L$, Z_i is a zone
  $(\ell_1, 2 \leq x < 4)$ or $(\ell_0, x < 1 \wedge y - x \geq 2)$ or $(\ell_0, x \leq 2) \cup (\ell_2, x > 0)$

States & Symbolic States

- $Q = L \times \mathbb{R}_{\geq 0}^{Clock}$ is the set of states of the TGA
  $q = (\ell, v) \in Q$
- Discrete Successors of $X \subseteq Q$ by an action a:
  $$Post^a(X) = \{q' \in Q \mid q \xrightarrow{a} q' \text{ and } q \in X\}$$
- Time Successors of $X \subseteq Q$:
  $$Post^\delta(X) = \{q' \in Q \mid \exists t \geq 0 \mid q \xrightarrow{t} q' \text{ and } q \in X\}$$
- Zone = conjunction of triangular constraints
  $x - y < 3, x \geq 2 \wedge 1 < y - x < 2$
- Symbolic State is defined by a State predicate (SP)
  $P = \cup_{i \in [1..n]}(\ell_{j_i}, Z_i), \ell_{j_i} \in L, Z_i$ is a zone
  $(\ell_1, 2 \leq x < 4)$ or $(\ell_0, x < 1 \wedge y - x \geq 2)$ or $(\ell_0, x \leq 2) \cup (\ell_2, x > 0)$

States & Symbolic States

- $Q = L \times \mathbb{R}_{\geq 0}^{Clock}$ is the set of states of the TGA
  $q = (\ell, v) \in Q$
- Discrete Successors of $X \subseteq Q$ by an action a:
  $$Post^a(X) = \{q' \in Q \mid q \xrightarrow{a} q' \text{ and } q \in X\}$$
- Time Successors of $X \subseteq Q$:
  $$Post^\delta(X) = \{q' \in Q \mid \exists t \geq 0 \mid q \xrightarrow{t} q' \text{ and } q \in X\}$$
- Zone = conjunction of triangular constraints
  $x - y < 3, x \geq 2 \wedge 1 < y - x < 2$
- Symbolic State is defined by a State predicate (SP)
  $P = \cup_{i \in [1..n]}(\ell_{j_i}, Z_i)$, $\ell_{j_i} \in L$, Z_i is a zone
  $(\ell_1, 2 \leq x < 4)$ or $(\ell_0, x < 1 \wedge y - x \geq 2)$ or $(\ell_0, x \leq 2) \cup (\ell_2, x > 0)$

States & Symbolic States

- $Q = L \times \mathbb{R}_{\geq 0}^{Clock}$ is the set of states of the TGA
  $q = (\ell, v) \in Q$
- Discrete Successors of $X \subseteq Q$ by an action a:
  $$Post^a(X) = \{q' \in Q \mid q \xrightarrow{a} q' \text{ and } q \in X\}$$
- Time Successors of $X \subseteq Q$:
  $$Post^\delta(X) = \{q' \in Q \mid \exists t \geq 0 \mid q \xrightarrow{t} q' \text{ and } q \in X\}$$
- Zone = conjunction of triangular constraints
  $x - y < 3, x \geq 2 \wedge 1 < y - x < 2$
- Symbolic State is defined by a State predicate (SP)
  $P = \cup_{i \in [1..n]}(\ell_{j_i}, Z_i)$, $\ell_{j_i} \in L$, Z_i is a zone
  $(\ell_1, 2 \leq x < 4)$ or $(\ell_0, x < 1 \wedge y - x \geq 2)$ or $(\ell_0, x \leq 2) \cup (\ell_2, x > 0)$

Effectiveness of *$Post^a$* and *$Post^\delta$*

If P is a SP then $Post^a(P), Post^\delta(P)$ are SP and can be computed effectively. (There is a symbolic version for $Post^a$ and $Post^\delta$.)

States & Symbolic States

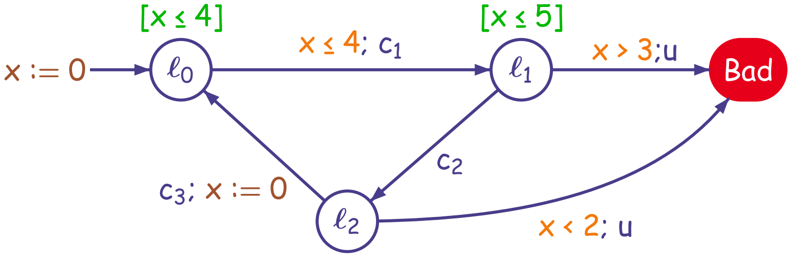
- $Q = L \times \mathbb{R}_{\geq 0}^{Clock}$ is the set of states of the TGA
  $q = (\ell, v) \in Q$
- Discrete Successors of $X \subseteq Q$ by an action a:
  $$Post^a(X) = \{q' \in Q \mid q \xrightarrow{a} q' \text{ and } q \in X\}$$
- Time Successors of $X \subseteq Q$:
  $$Post^\delta(X) = \{q' \in Q \mid \exists t \geq 0 \mid q \xrightarrow{t} q' \text{ and } q \in X\}$$
- Zone = conjunction of triangular constraints
  $x - y < 3, x \geq 2 \wedge 1 < y - x < 2$
- Symbolic State is defined by a State predicate (SP)
  $P = \cup_{i \in [1..n]}(\ell_{j_i}, Z_i), \ell_{j_i} \in L, Z_i$ is a zone
  $(\ell_1, 2 \leq x < 4)$ or $(\ell_0, x < 1 \wedge y - x \geq 2)$ or $(\ell_0, x \leq 2) \cup (\ell_2, x > 0)$

Decidability Result for TA

▸ Region Graph

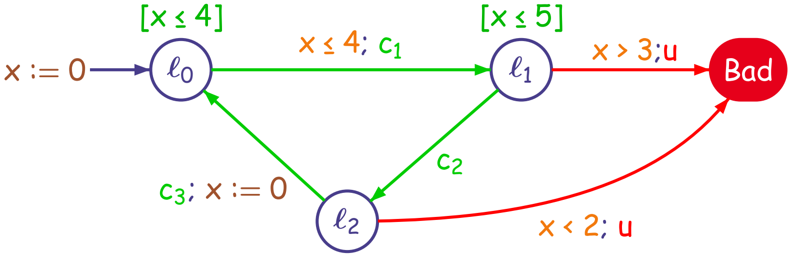
The Reachability Problem for TA is PSPACE-Complete.
Build a finite abstraction: region automaton

Timed Game Automata



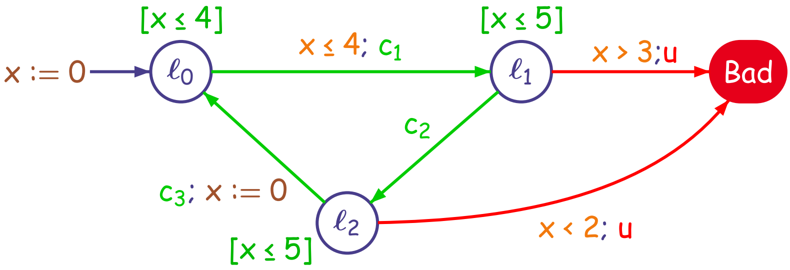
- Introduced by Maler, Pnueli, Sifakis [Maler et al.'95]
- The controller continuously observes the system
  time elapsing and discrete moves are observable
- The controller has the choice between two types of moves:
  - "do nothing" (delay action)
  - "do a controllable action" (among the ones that are possible)
- It can prevent time elapsing by taking a controllable move

Timed Game Automata

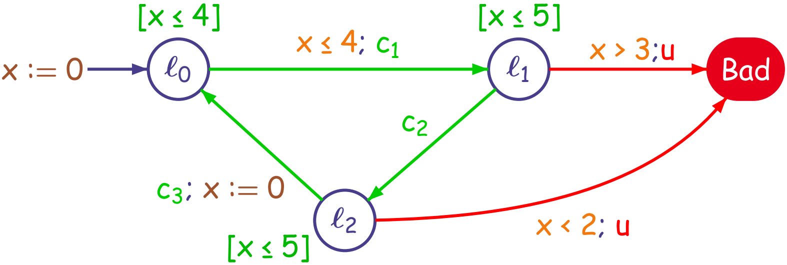


- Introduced by Maler, Pnueli, Sifakis [Maler et al.'95]
- The controller continuously observes the system
  time elapsing and discrete moves are observable
- The controller has the choice between two types of moves:
  - "do nothing" (delay action)
  - "do a controllable action" (among the ones that are possible)
- It can prevent time elapsing by taking a controllable move

Strategies and Winning States



Strategies and Winning States

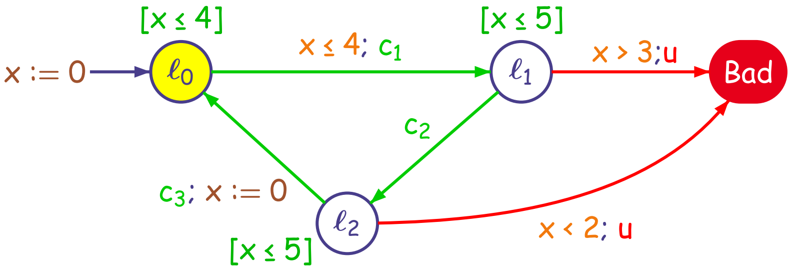


The strategy f: "Wait as long as the system permits"

$\rho_1 : \quad (\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{0.5} (\ell_1, 4.5) \xrightarrow{u} (Bad, 4.5)$

$\rho_2 : \quad (\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{1.0} (\ell_1, 5) \xrightarrow{c_2} (\ell_2, 5) \xrightarrow{c_3} (\ell_0, 0) \cdots$

Strategies and Winning States

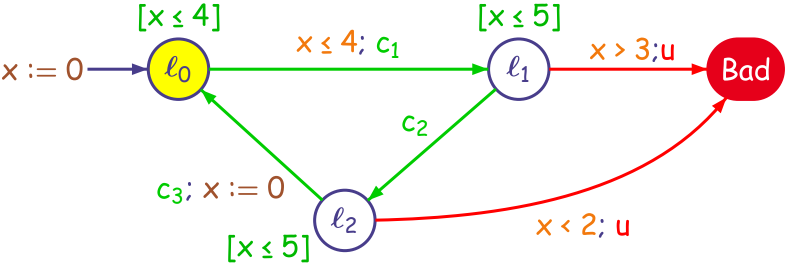


The strategy f: "Wait as long as the system permits"

$\rho_1 :\quad (\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{0.5} (\ell_1, 4.5) \xrightarrow{u} (Bad, 4.5)$

$\rho_2 :\quad (\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{1.0} (\ell_1, 5) \xrightarrow{c_2} (\ell_2, 5) \xrightarrow{c_3} (\ell_0, 0) \cdots$

Strategies and Winning States

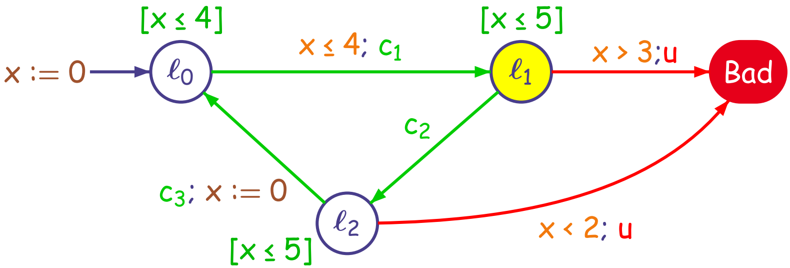


The strategy f: "Wait as long as the system permits"

$\rho_1: \quad (\ell_0,0) \xrightarrow{4} (\ell_0,4) \xrightarrow{c_1} (\ell_1,4) \xrightarrow{0.5} (\ell_1,4.5) \xrightarrow{u} (Bad,4.5)$

$\rho_2: \quad (\ell_0,0) \xrightarrow{4} (\ell_0,4) \xrightarrow{c_1} (\ell_1,4) \xrightarrow{1.0} (\ell_1,5) \xrightarrow{c_2} (\ell_2,5) \xrightarrow{c_3} (\ell_0,0) \cdots$

Strategies and Winning States

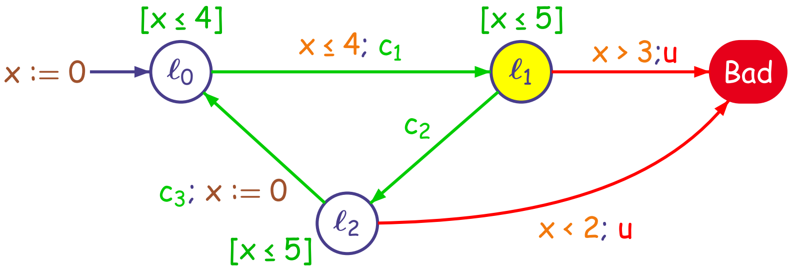


The strategy f: "Wait as long as the system permits"

$\rho_1 : \quad (\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{0.5} (\ell_1, 4.5) \xrightarrow{u} (Bad, 4.5)$

$\rho_2 : \quad (\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{1.0} (\ell_1, 5) \xrightarrow{c_2} (\ell_2, 5) \xrightarrow{c_3} (\ell_0, 0) \cdots$

Strategies and Winning States

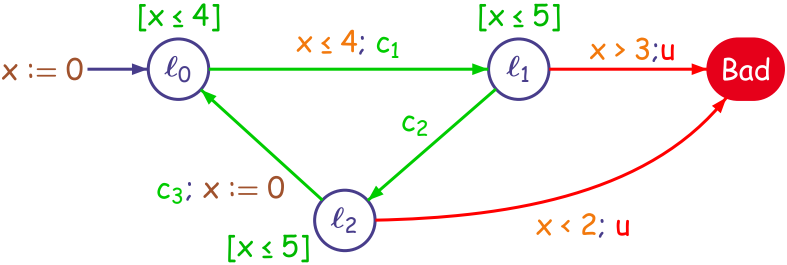


The strategy f: "Wait as long as the system permits"

$\rho_1 : \quad (\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{0.5} (\ell_1, 4.5) \xrightarrow{u} (Bad, 4.5)$

$\rho_2 : \quad (\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{1.0} (\ell_1, 5) \xrightarrow{c_2} (\ell_2, 5) \xrightarrow{c_3} (\ell_0, 0) \cdots$

Strategies and Winning States

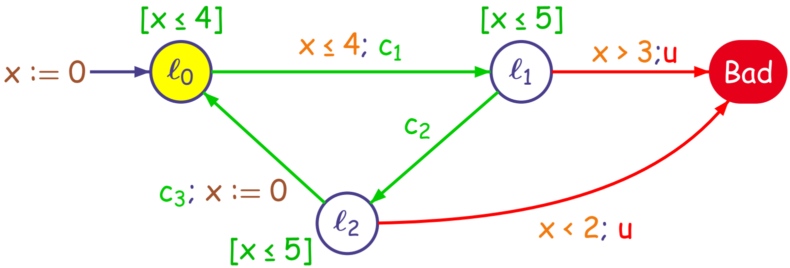


The strategy f: "Wait as long as the system permits"

$\rho_1: \quad (\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{0.5} (\ell_1, 4.5) \xrightarrow{u} (Bad, 4.5)$

$\rho_2: \quad (\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{1.0} (\ell_1, 5) \xrightarrow{c_2} (\ell_2, 5) \xrightarrow{c_3} (\ell_0, 0) \cdots$

Strategies and Winning States

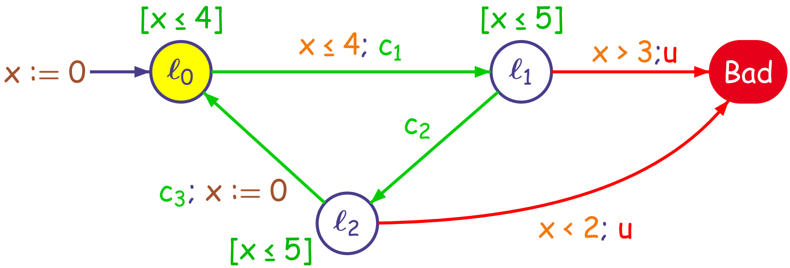


The strategy f: "Wait as long as the system permits"

$\rho_1 : \quad (\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{0.5} (\ell_1, 4.5) \xrightarrow{u} (Bad, 4.5)$

$\rho_2 : \quad (\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{1.0} (\ell_1, 5) \xrightarrow{c_2} (\ell_2, 5) \xrightarrow{c_3} (\ell_0, 0) \cdots$

Strategies and Winning States

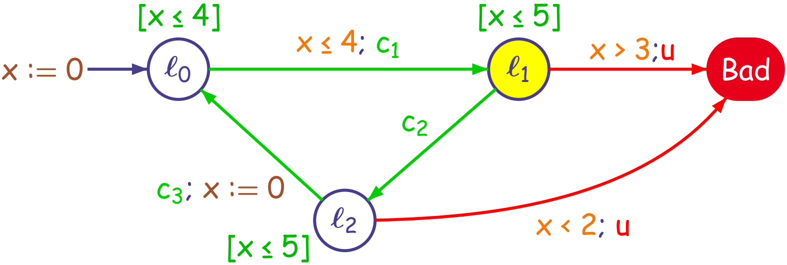


The strategy f: "Wait as long as the system permits"

$\rho_1 : \quad (\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{0.5} (\ell_1, 4.5) \xrightarrow{u} (Bad, 4.5)$

$\rho_2 : \quad (\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{1.0} (\ell_1, 5) \xrightarrow{c_2} (\ell_2, 5) \xrightarrow{c_3} (\ell_0, 0) \cdots$

Strategies and Winning States

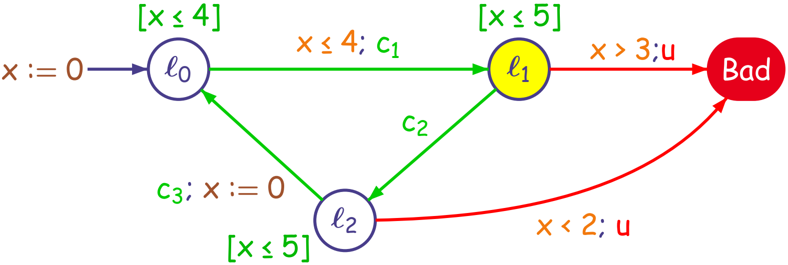


The strategy f: “Wait as long as the system permits”

$\rho_1: \quad (\ell_0,0) \xrightarrow{4} (\ell_0,4) \xrightarrow{c_1} (\ell_1,4) \xrightarrow{0.5} (\ell_1,4.5) \xrightarrow{u} (Bad,4.5)$

$\rho_2: \quad (\ell_0,0) \xrightarrow{4} (\ell_0,4) \xrightarrow{c_1} (\ell_1,4) \xrightarrow{1.0} (\ell_1,5) \xrightarrow{c_2} (\ell_2,5) \xrightarrow{c_3} (\ell_0,0) \cdots$

Strategies and Winning States

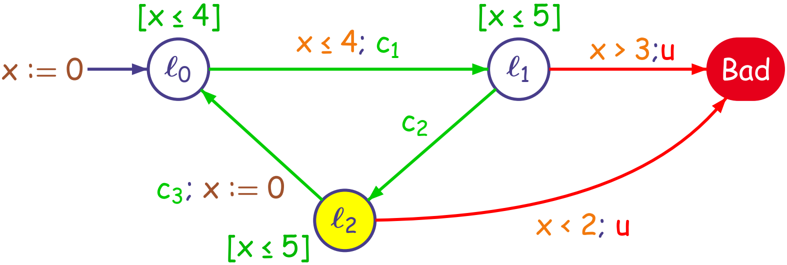


The strategy f: "Wait as long as the system permits"

$\rho_1: \quad (\ell_0,0) \xrightarrow{4} (\ell_0,4) \xrightarrow{c_1} (\ell_1,4) \xrightarrow{0.5} (\ell_1,4.5) \xrightarrow{u} (\text{Bad},4.5)$

$\rho_2: \quad (\ell_0,0) \xrightarrow{4} (\ell_0,4) \xrightarrow{c_1} (\ell_1,4) \xrightarrow{1.0} (\ell_1,5) \xrightarrow{c_2} (\ell_2,5) \xrightarrow{c_3} (\ell_0,0) \cdots$

Strategies and Winning States

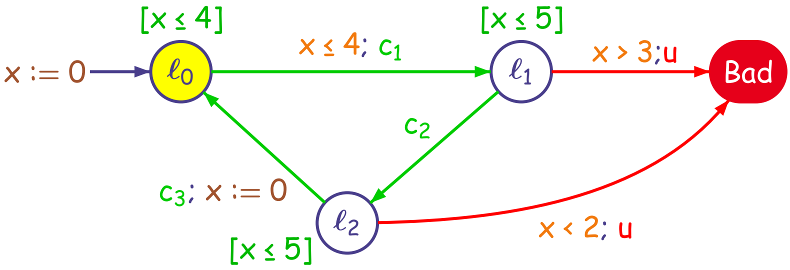


The strategy f: "Wait as long as the system permits"

ρ_1 : $(\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{0.5} (\ell_1, 4.5) \xrightarrow{u} (Bad, 4.5)$

ρ_2 : $(\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{1.0} (\ell_1, 5) \xrightarrow{c_2} (\ell_2, 5) \xrightarrow{c_3} (\ell_0, 0) \cdots$

Strategies and Winning States

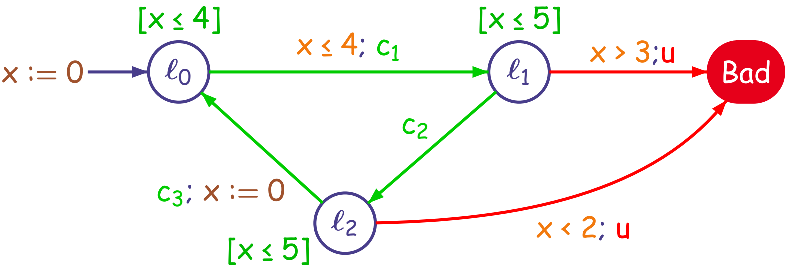


The strategy f: "Wait as long as the system permits"

$\rho_1: \quad (\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{0.5} (\ell_1, 4.5) \xrightarrow{u} (Bad, 4.5)$

$\rho_2: \quad (\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{1.0} (\ell_1, 5) \xrightarrow{c_2} (\ell_2, 5) \xrightarrow{c_3} (\ell_0, 0) \cdots$

Strategies and Winning States

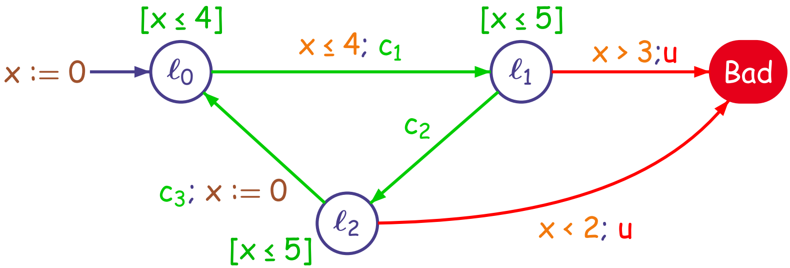


The strategy f: "Wait as long as the system permits"

$$\rho_1 : \quad (\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{0.5} (\ell_1, 4.5) \xrightarrow{u} (\text{Bad}, 4.5)$$

$$\rho_2 : \quad (\ell_0, 0) \xrightarrow{4} (\ell_0, 4) \xrightarrow{c_1} (\ell_1, 4) \xrightarrow{1.0} (\ell_1, 5) \xrightarrow{c_2} (\ell_2, 5) \xrightarrow{c_3} (\ell_0, 0) \cdots$$

Strategies and Winning States

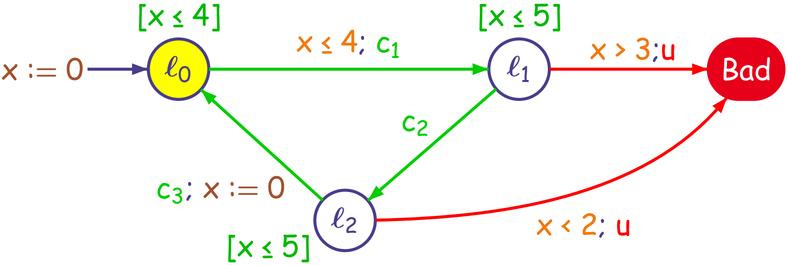


A winning strategy f'

in ℓ_0 at $x = 2$ do c_1; in ℓ_1 at $x = 2.5$ do c_2; in ℓ_2 at $x = 4$ do c_3

$\rho: \quad (\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2)$

Strategies and Winning States

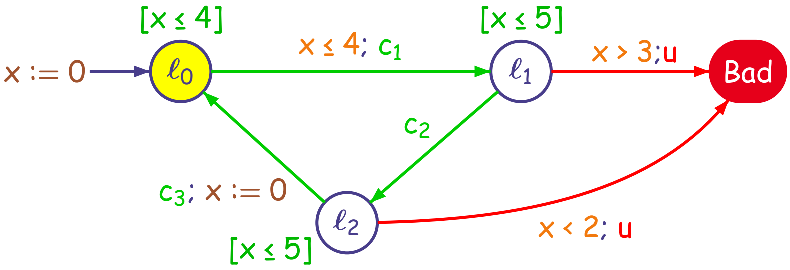


A winning strategy f'

in ℓ_0 at $x = 2$ do c_1; in ℓ_1 at $x = 2.5$ do c_2; in ℓ_2 at $x = 4$ do c_3

$\rho : \quad (\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2)$

Strategies and Winning States

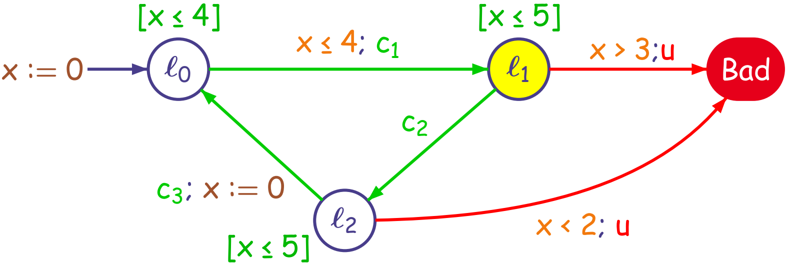


A winning strategy f'

in ℓ_0 at $x = 2$ do c_1; in ℓ_1 at $x = 2.5$ do c_2; in ℓ_2 at $x = 4$ do c_3

$\rho: \quad (\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2)$

Strategies and Winning States

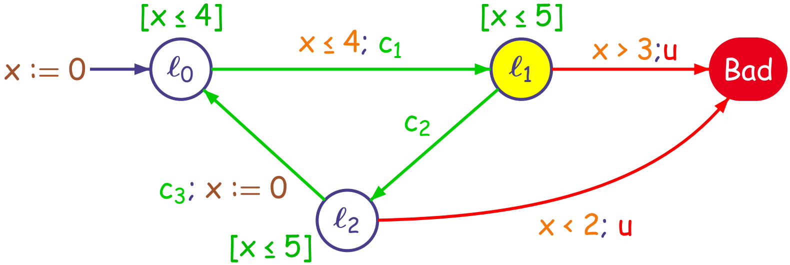


A winning strategy f'

in ℓ_0 at $x = 2$ do c_1; in ℓ_1 at $x = 2.5$ do c_2; in ℓ_2 at $x = 4$ do c_3

$\rho : \quad (\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2)$

Strategies and Winning States

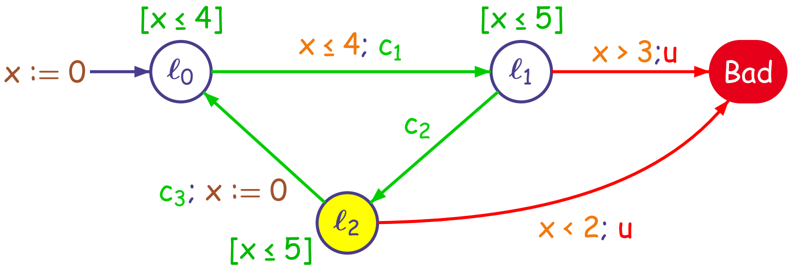


A winning strategy f'

in ℓ_0 at $x = 2$ do c_1; in ℓ_1 at $x = 2.5$ do c_2; in ℓ_2 at $x = 4$ do c_3

$$\rho : \quad (\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2) \xrightarrow{0.5} (\ell_1, 2.5)$$

Strategies and Winning States

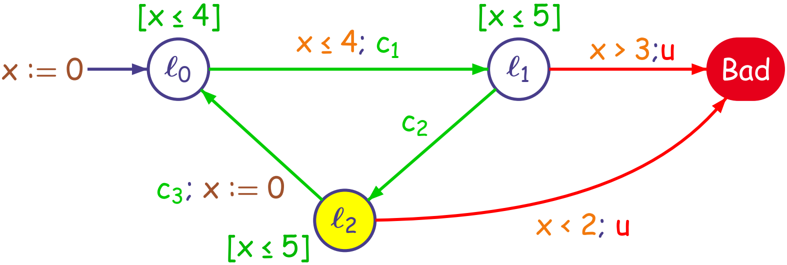


A winning strategy f'

in ℓ_0 at $x = 2$ do c_1; in ℓ_1 at $x = 2.5$ do c_2; in ℓ_2 at $x = 4$ do c_3

$$\rho: \quad (\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2) \xrightarrow{0.5} (\ell_1, 2.5) \xrightarrow{c_2} (\ell_2, 2.5)$$

Strategies and Winning States

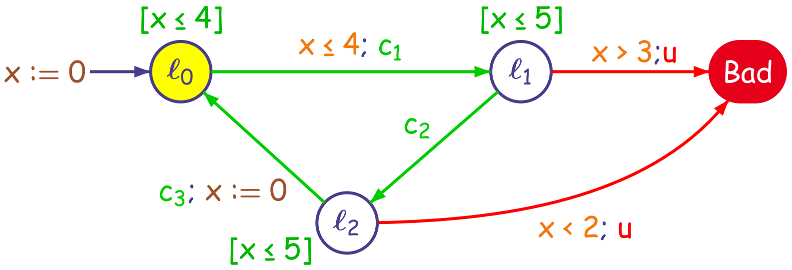


A winning strategy f'

in ℓ_0 at $x = 2$ do c_1; in ℓ_1 at $x = 2.5$ do c_2; in ℓ_2 at $x = 4$ do c_3

$$\rho : \quad (\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2) \xrightarrow{0.5} (\ell_1, 2.5) \xrightarrow{c_2} (\ell_2, 2.5) \xrightarrow{1.5} (\ell_2, 4)$$

Strategies and Winning States

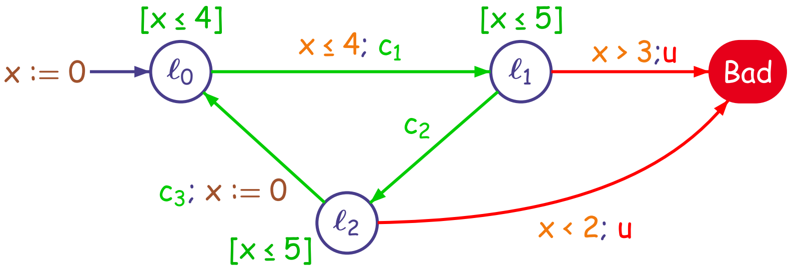


A winning strategy f'

in ℓ_0 at $x = 2$ do c_1; in ℓ_1 at $x = 2.5$ do c_2; in ℓ_2 at $x = 4$ do c_3

$$\rho : \quad (\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2) \xrightarrow{0.5} (\ell_1, 2.5) \xrightarrow{c_2} (\ell_2, 2.5) \xrightarrow{1.5} (\ell_2, 4) \xrightarrow{c_3} (\ell_0, 0)$$

Strategies and Winning States

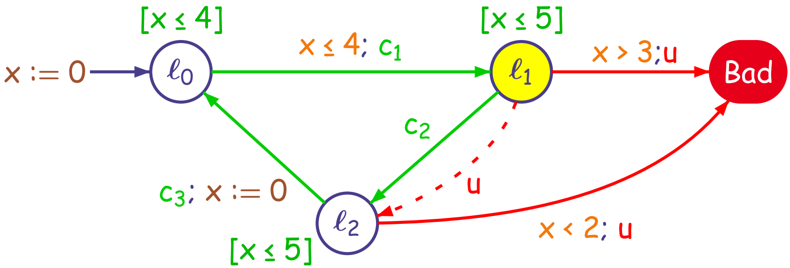


A winning strategy f'

in ℓ_0 at $x = 2$ do c_1; in ℓ_1 at $x = 2.5$ do c_2; in ℓ_2 at $x = 4$ do c_3

$$\rho : \quad (\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2) \xrightarrow{0.5} (\ell_1, 2.5) \xrightarrow{c_2} (\ell_2, 2.5) \xrightarrow{1.5} (\ell_2, 4) \xrightarrow{c_3} (\ell_0, 0) \cdots$$

Strategies and Winning States

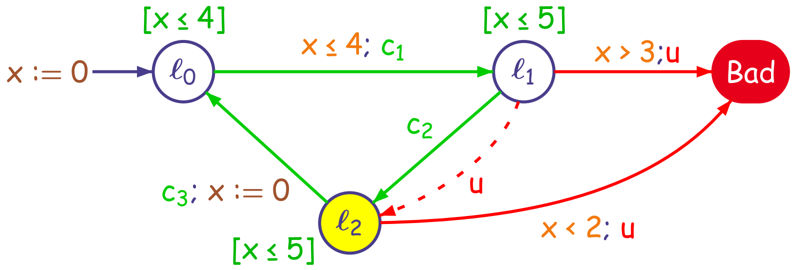


A winning strategy f'

in ℓ_0 at $x = 2$ do c_1; in ℓ_1 at $x = 2.5$ do c_2; in ℓ_2 at $x = 4$ do c_3

$\rho: \quad (\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2)$

Strategies and Winning States

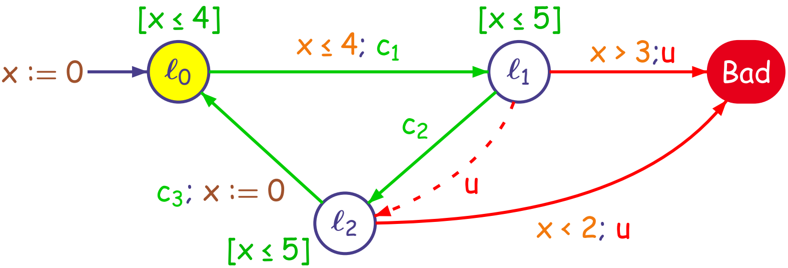


A winning strategy f'

in ℓ_0 at $x = 2$ do c_1; in ℓ_1 at $x = 2.5$ do c_2; in ℓ_2 at $x = 4$ do c_3

$\rho : \quad (\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2) \xrightarrow{u \text{ at } \delta \leq 0.5} (\ell_2, 2 + \delta)$

Strategies and Winning States

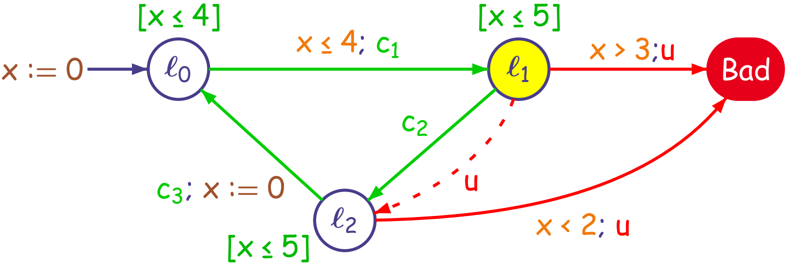


A winning strategy f'

in ℓ_0 at $x = 2$ do c_1; in ℓ_1 at $x = 2.5$ do c_2; in ℓ_2 at $x = 4$ do c_3

$$\rho : \quad (\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2) \xrightarrow{u \text{ at } \delta \leq 0.5} (\ell_2, 2 + \delta) \xrightarrow{c_3 \text{ at } 2-\delta} (\ell_0, 0)$$

Strategies and Winning States



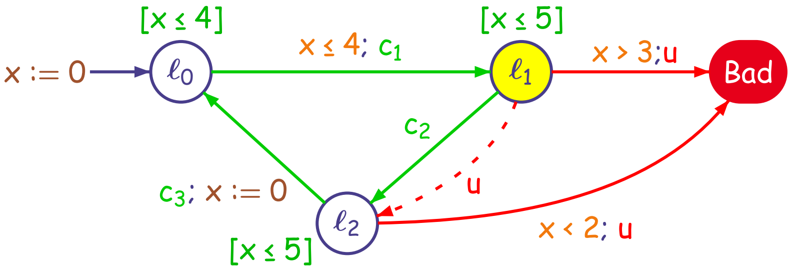
A winning strategy f'

in ℓ_0 at $x = 2$ do c_1; in ℓ_1 at $x = 2.5$ do c_2; in ℓ_2 at $x = 4$ do c_3

ρ : $(\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2) \xrightarrow{u \text{ at } \delta \leq 0.5} (\ell_2, 2+\delta) \xrightarrow{c_3 \text{ at } 2-\delta} (\ell_0, 0)$

ρ' : $(\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2)$

Strategies and Winning States



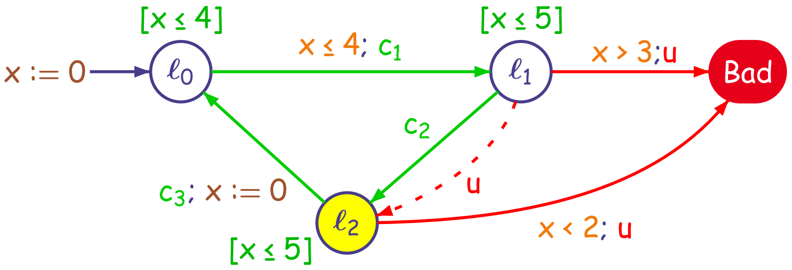
A winning strategy f'

in ℓ_0 at $x = 2$ do c_1; in ℓ_1 at $x = 2.5$ do c_2; in ℓ_2 at $x = 4$ do c_3

ρ : $(\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2) \xrightarrow{u \text{ at } \delta \leq 0.5} (\ell_2, 2 + \delta) \xrightarrow{c_3 \text{ at } 2-\delta} (\ell_0, 0)$

ρ' : $(\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2) \xrightarrow{0.5} (\ell_1, 2.5)$

Strategies and Winning States



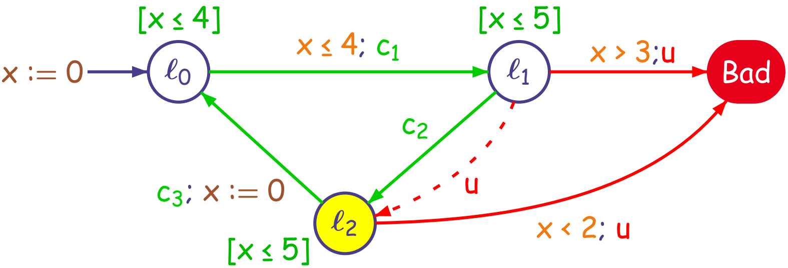
A winning strategy f'

in ℓ_0 at $x = 2$ do c_1; in ℓ_1 at $x = 2.5$ do c_2; in ℓ_2 at $x = 4$ do c_3

$\rho: \quad (\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2) \xrightarrow{u \text{ at } \delta \leq 0.5} (\ell_2, 2+\delta) \xrightarrow{c_3 \text{ at } 2-\delta} (\ell_0, 0)$

$\rho': \quad (\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2) \xrightarrow{0.5} (\ell_1, 2.5) \xrightarrow{c_2} (\ell_2, 2.5)$

Strategies and Winning States



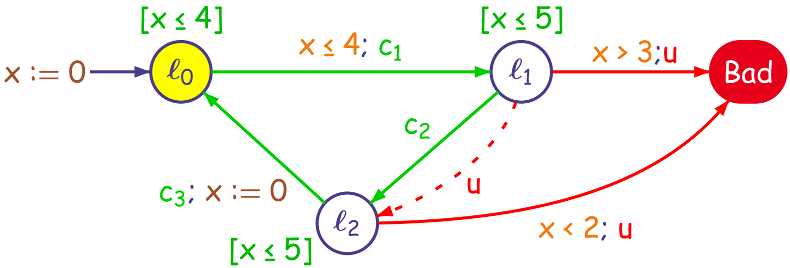
A winning strategy f'

in ℓ_0 at $x = 2$ do c_1; in ℓ_1 at $x = 2.5$ do c_2; in ℓ_2 at $x = 4$ do c_3

$\rho : \quad (\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2) \xrightarrow{u \text{ at } \delta \leq 0.5} (\ell_2, 2+\delta) \xrightarrow{c_3 \text{ at } 2-\delta} (\ell_0, 0)$

$\rho' : \quad (\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2) \xrightarrow{0.5} (\ell_1, 2.5) \xrightarrow{c_2} (\ell_2, 2.5) \xrightarrow{1.5} (\ell_2, 4)$

Strategies and Winning States



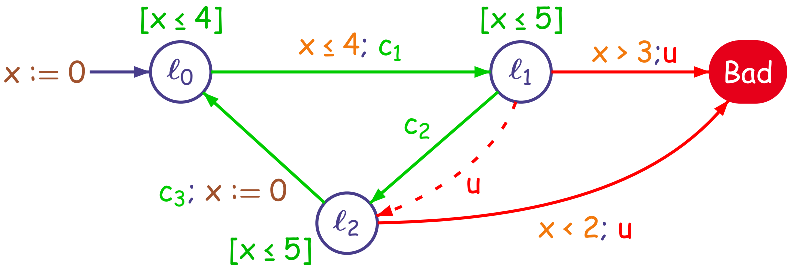
A winning strategy f'

in ℓ_0 at $x = 2$ do c_1; in ℓ_1 at $x = 2.5$ do c_2; in ℓ_2 at $x = 4$ do c_3

ρ : $(\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2) \xrightarrow{u \text{ at } \delta \leq 0.5} (\ell_2, 2+\delta) \xrightarrow{c_3 \text{ at } 2-\delta} (\ell_0, 0)$

ρ' : $(\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2) \xrightarrow{0.5} (\ell_1, 2.5) \xrightarrow{c_2} (\ell_2, 2.5) \xrightarrow{1.5} (\ell_2, 4) \xrightarrow{c_3} (\ell_0, 0) \cdots$

Strategies and Winning States



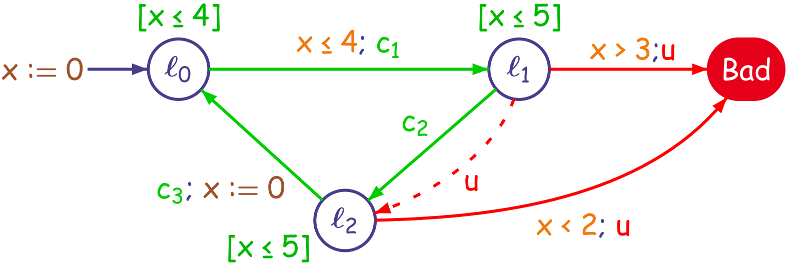
A winning strategy f'

in ℓ_0 at $x = 2$ do c_1; in ℓ_1 at $x = 2.5$ do c_2; in ℓ_2 at $x = 4$ do c_3

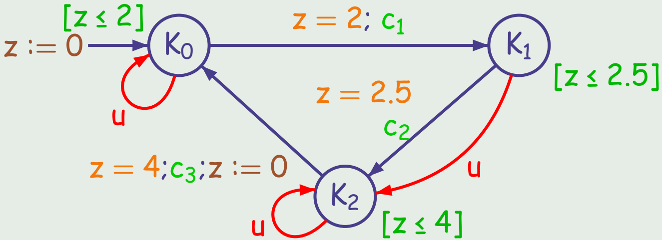
$\rho : \quad (\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2) \xrightarrow{u \text{ at } \delta \leq 0.5} (\ell_2, 2 + \delta) \xrightarrow{c_3 \text{ at } 2-\delta} (\ell_0, 0)$

$\rho' : \quad (\ell_0, 0) \xrightarrow{2} (\ell_0, 2) \xrightarrow{c_1} (\ell_1, 2) \xrightarrow{0.5} (\ell_1, 2.5) \xrightarrow{c_2} (\ell_2, 2.5) \xrightarrow{1.5} (\ell_2, 4) \xrightarrow{c_3} (\ell_0, 0) \cdots$

Strategies and Winning States

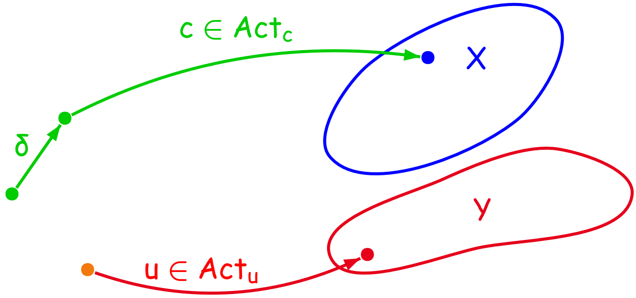


The Strategy f′ as a Timed Automaton



Controllable Predecessors

$\pi(X, Y) =$ states from which one can enforce X and avoid Y by: time elapsing followed by a controllable action

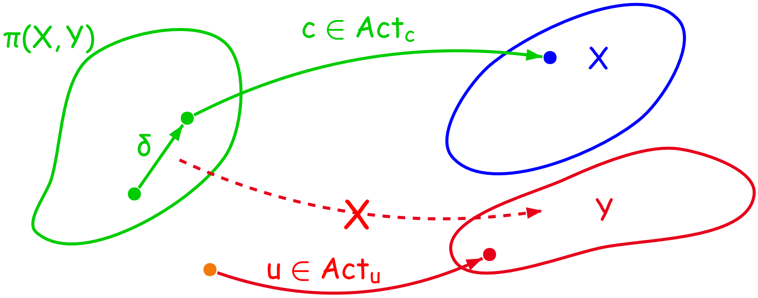


Fixpoint Characterization of Winning States for Safety Games:

1. Let φ be a set of safe (good) states and G a game
2. Let W^* be the greatest fixpoint of $h(X) = \varphi \cap \pi(X, \overline{X})$
3. W^* is the set of winning states for (G, φ)

Controllable Predecessors

$\pi(X,Y)$ = states from which one can enforce X and avoid Y by:
time elapsing followed by a controllable action

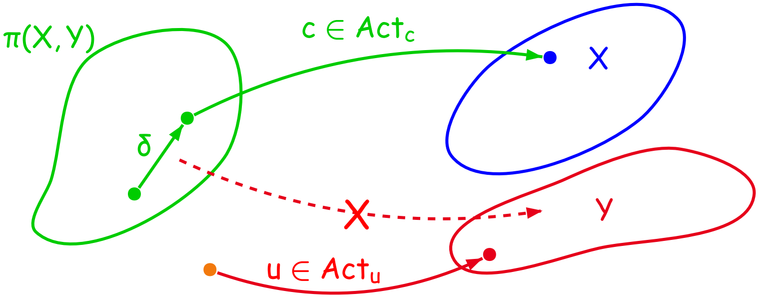


Fixpoint Characterization of Winning States for Safety Games:

1. Let φ be a set of safe (good) states and G a game
2. Let W^* be the greatest fixpoint of $h(X) = \varphi \cap \pi(X, \overline{X})$
3. W^* is the set of winning states for (G, φ)

Controllable Predecessors

$\pi(X, Y) =$ states from which one can enforce X and avoid Y by:
time elapsing followed by a controllable action



Fixpoint Characterization of Winning States for Safety Games:

1. Let φ be a set of safe (good) states and G a game
2. Let W^* be the greatest fixpoint of $h(X) = \varphi \cap \pi(X, \overline{X})$
3. W^* is the set of winning states for (G, φ)

Symbolic Algorithms for Safety Control

[Maler et al.'95, De Alfaro et al.'01]

Details & Example

1. There is a symbolic version for $\pi(X, Y)$
2. $\Longrightarrow$ there is a symbolic version for $h(X)$

Symbolic Algorithms for Safety Control

[Maler et al.'95, De Alfaro et al.'01]

▸ Details & Example

1. There is a symbolic version for $\pi(X, Y)$
2. $\Longrightarrow$ there is a symbolic version for $h(X)$

- Control Problem (CP): check that $(\ell_0, 0) \in W^*$
- Control Synthesis Problem (CSP): by definition of π there is a strategy

Symbolic Algorithms for Safety Control

[Maler et al.'95, De Alfaro et al.'01]

Details & Example

1. There is a symbolic version for $\pi(X, Y)$
2. $\Longrightarrow$ there is a symbolic version for $h(X)$

Theorem (Termination)

The iterative computation of W^* terminates for (G, φ) with G a timed game automaton φ a ω-regular winning condition.

Symbolic Algorithms for Safety Control

[Maler et al.'95, De Alfaro et al.'01]

Details & Example

1. There is a symbolic version for $\pi(X, Y)$
2. $\Longrightarrow$ there is a symbolic version for $h(X)$

Theorem (Termination)

The iterative computation of W^* terminates for (G, φ) with G a timed game automaton φ a ω-regular winning condition.

Theorem (Decidability of CP for Timed Game Automata)

The (Safety) Control Problem is decidable.

Symbolic Algorithms for Safety Control

[Maler et al.'95, De Alfaro et al.'01]

Details & Example

1. There is a symbolic version for $\pi(X, Y)$
2. $\Longrightarrow$ there is a symbolic version for $h(X)$

Theorem (Termination)

The iterative computation of W^* terminates for (G, φ) with G a timed game automaton φ a ω-regular winning condition.

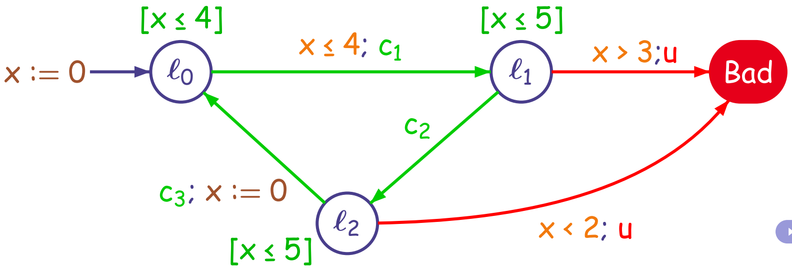
Theorem (Decidability of CP for Timed Game Automata)

The (Safety) Control Problem is decidable.

Theorem (Effectiveness of CSP)

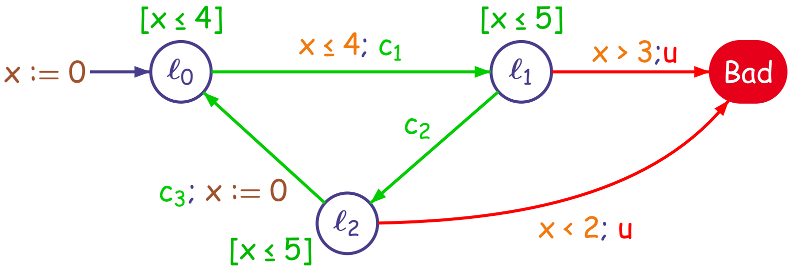
If $(\ell_0, 0) \in W^*$ we can compute the most permissive positional winning strategy.

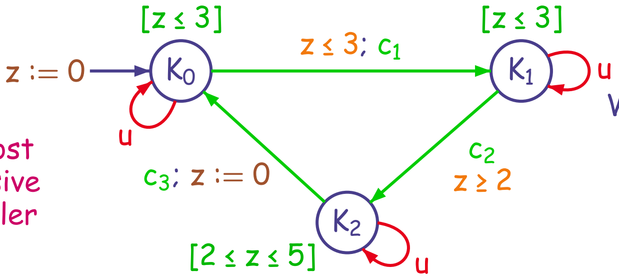
Result of the Computation for the Example



Skip

Result of the Computation for the Example





The Most Permissive Controller

Winning States

$(\ell_0, 0 \leq x \leq 3)$
$(\ell_1, 0 \leq x \leq 3)$
$(\ell_2, 2 \leq x \leq 5)$

Next:

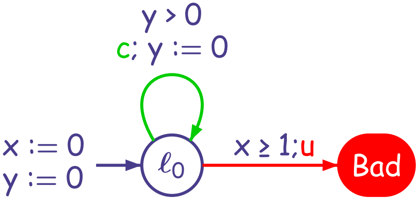
- Control of Timed Systems: Basics
- Selected Contributions
  - Implementable Controllers
  - Optimal Controllers
- Conclusion & Perspectives

Selection 1
Implementable Controllers

Joint work with Tom Henzinger and Jean-François Raskin

[HSCC'02]

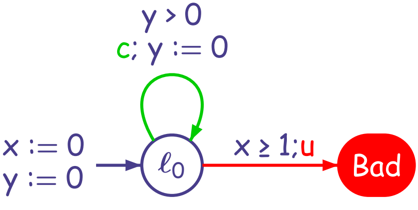
Problems with Dense-Time Control (1)



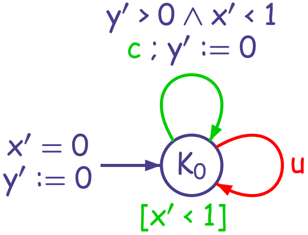
The System

The Controller is Zeno !!!

Problems with Dense-Time Control (1)



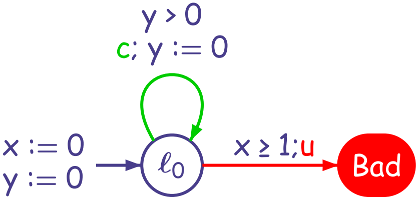
The System



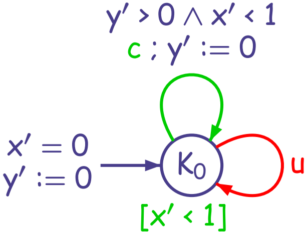
The Controller

The Controller is Zeno !!!

Problems with Dense-Time Control (1)



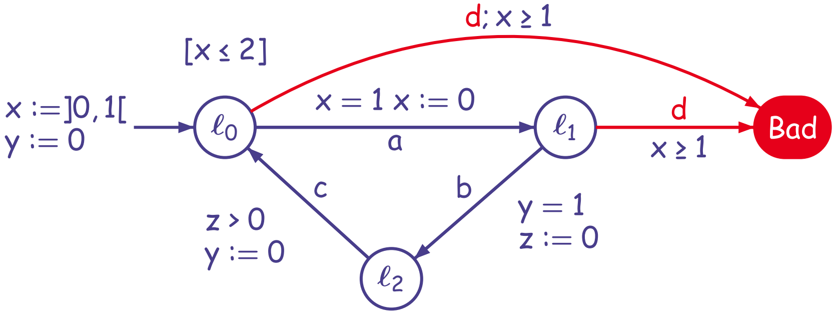
The System



The Controller

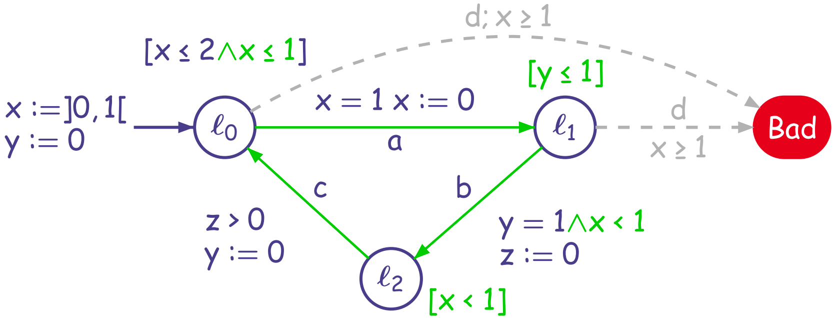
The Controller is Zeno !!!

Problems with Dense-Time Control (2)



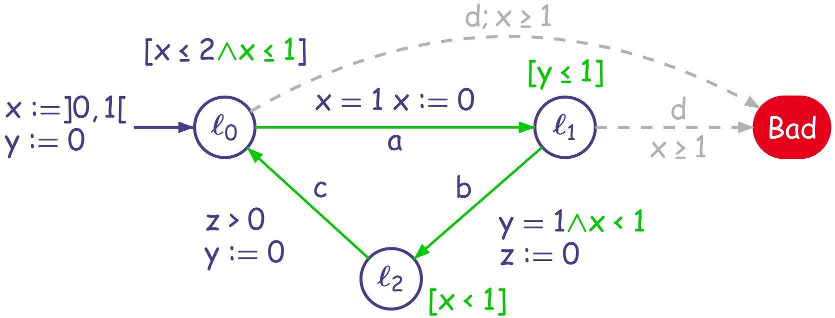
- The controller is Non-Zeno; One untimed behavior: $(\ell_0\ell_1\ell_2)^\omega$
- Let Δ_k = time spent in ℓ_2 in the k-th loop from ℓ_0 to ℓ_0
- It implies: $\forall k, \sum_{i=1}^{k} \Delta_i < 1 - x_0$, with $\forall i, \Delta_i > 0$

Problems with Dense-Time Control (2)



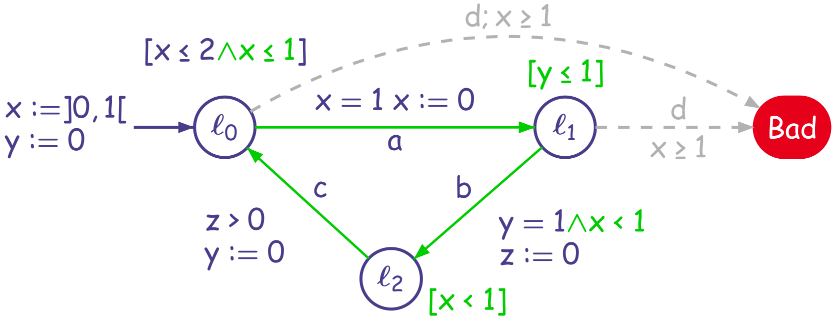
- The controller is Non-Zeno; One untimed behavior: $(\ell_0 \ell_1 \ell_2)^\omega$
- Let Δ_k = time spent in ℓ_2 in the k-th loop from ℓ_0 to ℓ_0
- It implies: $\forall k, \sum_{i=1}^{k} \Delta_i < 1 - x_0$, with $\forall i, \Delta_i > 0$

Problems with Dense-Time Control (2)



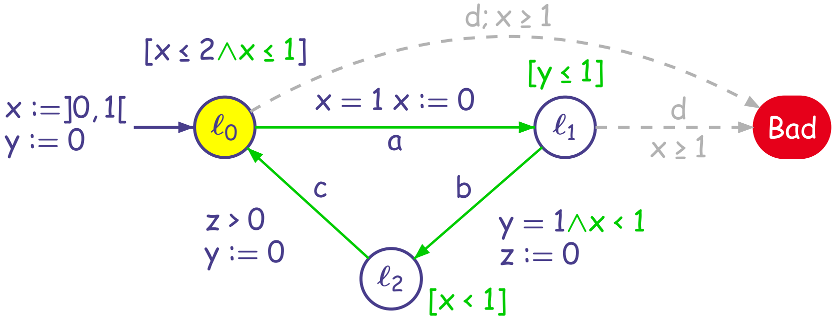
- The controller is Non-Zeno; One untimed behavior: $(\ell_0\ell_1\ell_2)^\omega$
- Let Δ_k = time spent in ℓ_2 in the k-th loop from ℓ_0 to ℓ_0
- It implies: $\forall k, \sum_{i=1}^{k} \Delta_i < 1 - x_0$, with $\forall i, \Delta_i > 0$

Problems with Dense-Time Control (2)



- The controller is Non-Zeno; One untimed behavior: $(\ell_0 \ell_1 \ell_2)^\omega$
- Let Δ_k = time spent in ℓ_2 in the k-th loop from ℓ_0 to ℓ_0
- It implies: $\forall k, \sum_{i=1}^{k} \Delta_i < 1 - x_0$, with $\forall i, \Delta_i > 0$

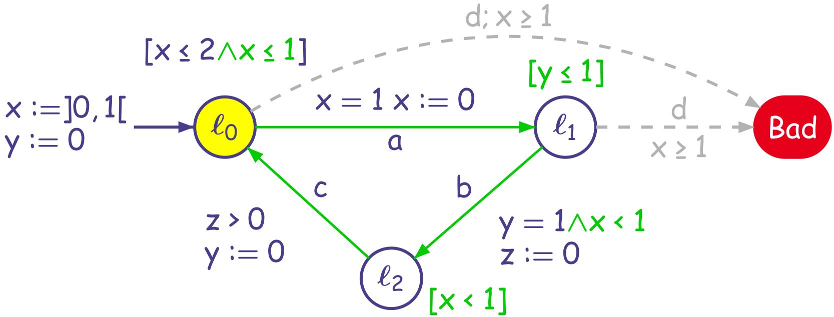
Problems with Dense-Time Control (2)



- The controller is Non-Zeno; One untimed behavior: $(\ell_0\ell_1\ell_2)^\omega$
- Let Δ_k = time spent in ℓ_2 in the k-th loop from ℓ_0 to ℓ_0
- It implies: $\forall k, \sum_{i=1}^{k} \Delta_i < 1 - x_0$, with $\forall i, \Delta_i > 0$

	ℓ_0
x:	x_0
y:	0

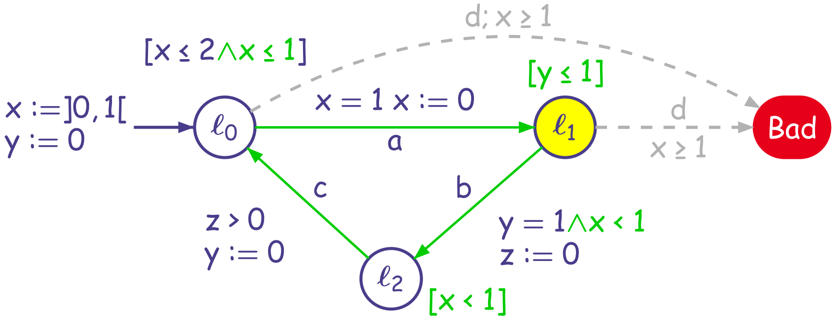
Problems with Dense-Time Control (2)



- The controller is Non-Zeno; One untimed behavior: $(\ell_0 \ell_1 \ell_2)^\omega$
- Let Δ_k = time spent in ℓ_2 in the k-th loop from ℓ_0 to ℓ_0
- It implies: $\forall k, \sum_{i=1}^{k} \Delta_i < 1 - x_0$, with $\forall i, \Delta_i > 0$

	ℓ_0		
x:	x_0	$\rightsquigarrow$	1
y:	0		$1 - x_0$

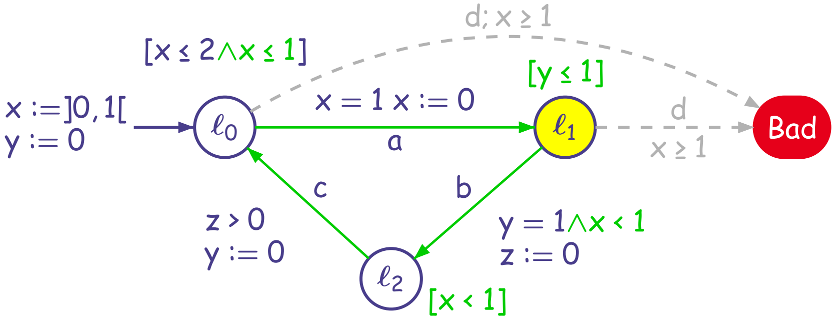
Problems with Dense-Time Control (2)



- The controller is Non-Zeno; One untimed behavior: $(\ell_0\ell_1\ell_2)^\omega$
- Let $\Delta_k =$ time spent in ℓ_2 in the k-th loop from ℓ_0 to ℓ_0
- It implies: $\forall k, \sum_{i=1}^{k} \Delta_i < 1 - x_0$, with $\forall i, \Delta_i > 0$

	ℓ_0				ℓ_1
x:	x_0	$\rightsquigarrow$	1	$\xrightarrow{a}$	0
y:	0		$1 - x_0$		$1 - x_0$

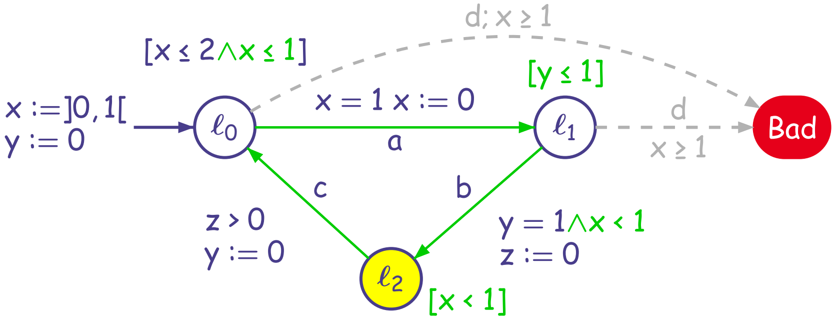
Problems with Dense-Time Control (2)



- The controller is Non-Zeno; One untimed behavior: $(\ell_0\ell_1\ell_2)^\omega$
- Let Δ_k = time spent in ℓ_2 in the k-th loop from ℓ_0 to ℓ_0
- It implies: $\forall k, \sum_{i=1}^{k} \Delta_i < 1 - x_0$, with $\forall i, \Delta_i > 0$

	ℓ_0				ℓ_1		
x:	x_0	$\rightsquigarrow$	1	$\xrightarrow{a}$	0	$\rightsquigarrow$	x_0
y:	0		$1 - x_0$		$1 - x_0$		1

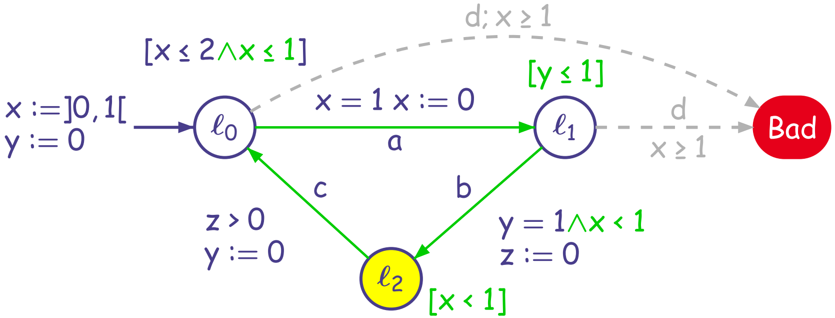
Problems with Dense-Time Control (2)



- The controller is Non-Zeno; One untimed behavior: $(\ell_0\ell_1\ell_2)^\omega$
- Let Δ_k = time spent in ℓ_2 in the k-th loop from ℓ_0 to ℓ_0
- It implies: $\forall k, \sum_{i=1}^{k} \Delta_i < 1 - x_0$, with $\forall i, \Delta_i > 0$

$$\begin{array}{lccccccc} & \ell_0 & & & \ell_1 & & & \ell_2 \\ x: & x_0 & \rightsquigarrow & 1 & \xrightarrow{a} 0 & \rightsquigarrow & x_0 & \xrightarrow{b} x_0 \\ y: & 0 & & 1 - x_0 & 1 - x_0 & & 1 & 1 \end{array}$$

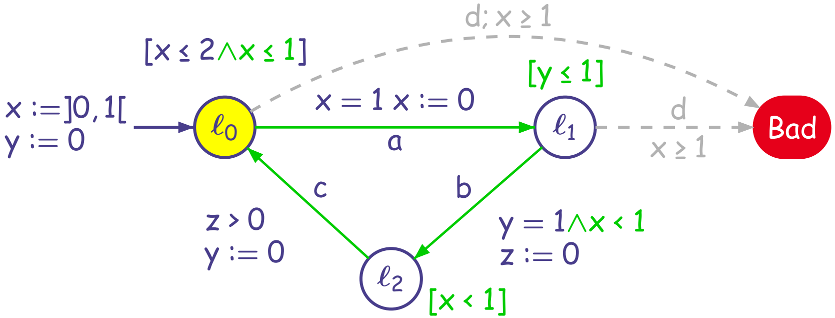
Problems with Dense-Time Control (2)



- The controller is Non-Zeno; One untimed behavior: $(\ell_0\ell_1\ell_2)^\omega$
- Let Δ_k = time spent in ℓ_2 in the k-th loop from ℓ_0 to ℓ_0
- It implies: $\forall k, \sum_{i=1}^{k} \Delta_i < 1 - x_0$, with $\forall i, \Delta_i > 0$

$$\begin{array}{lcccccccccc} & \ell_0 & & & & \ell_1 & & & & \ell_2 & & \\ x: & x_0 & \rightsquigarrow & 1 & \xrightarrow{a} & 0 & \rightsquigarrow & x_0 & \xrightarrow{b} & x_0 & \overset{\Delta_1}{\rightsquigarrow} & x_0 + \Delta_1 \\ y: & 0 & & 1 - x_0 & & 1 - x_0 & & 1 & & 1 & & 1 + \Delta_1 \end{array}$$

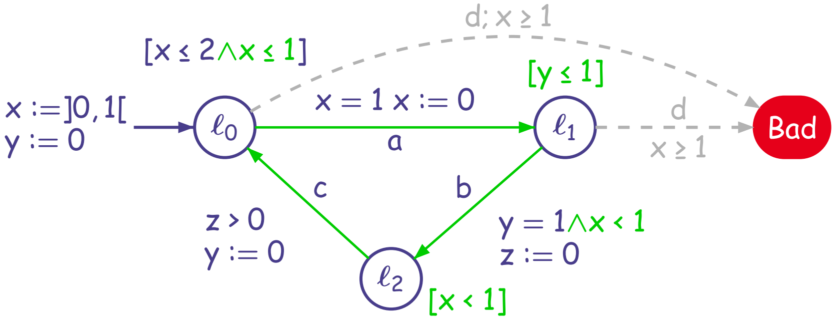
Problems with Dense-Time Control (2)



- The controller is Non-Zeno; One untimed behavior: $(\ell_0\ell_1\ell_2)^\omega$
- Let Δ_k = time spent in ℓ_2 in the k-th loop from ℓ_0 to ℓ_0
- It implies: $\forall k, \sum_{i=1}^{k} \Delta_i < 1 - x_0$, with $\forall i, \Delta_i > 0$

$$\begin{array}{lccccccccccc} & \ell_0 & & & \ell_1 & & & & \ell_2 & & & \ell_0 \\ x: & x_0 & \rightsquigarrow & 1 & \xrightarrow{a} 0 & \rightsquigarrow & x_0 & \xrightarrow{b} & x_0 & \overset{\Delta_1}{\rightsquigarrow} & x_0 + \Delta_1 & \xrightarrow{c} x_0 + \Delta_1 \\ y: & 0 & & 1 - x_0 & 1 - x_0 & & 1 & & 1 & & 1 + \Delta_1 & 0 \end{array}$$

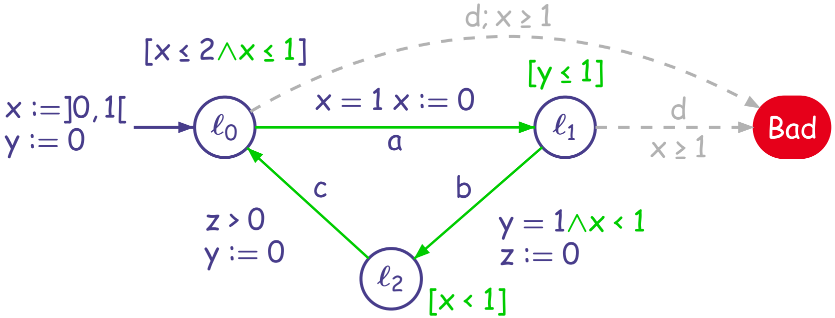
Problems with Dense-Time Control (2)



- The controller is Non-Zeno; One untimed behavior: $(\ell_0 \ell_1 \ell_2)^\omega$
- Let Δ_k = time spent in ℓ_2 in the k-th loop from ℓ_0 to ℓ_0
- It implies: $\forall k, \sum_{i=1}^{k} \Delta_i < 1 - x_0$, with $\forall i, \Delta_i > 0$

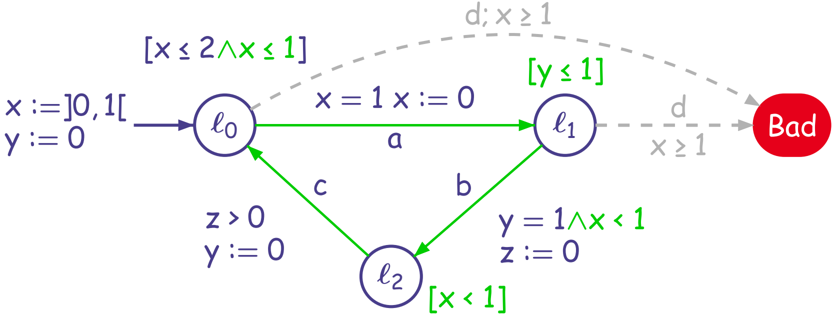
$$
\begin{array}{lccccccccccc}
 & \ell_0 & & & & \ell_1 & & & & \ell_2 & & & & \ell_0 \\
x: & x_0 & \rightsquigarrow & 1 & \xrightarrow{a} & 0 & \rightsquigarrow & x_0 & \xrightarrow{b} & x_0 & \overset{\Delta_1}{\rightsquigarrow} & x_0 + \Delta_1 & \xrightarrow{c} & x_0 + \Delta_1 \\
y: & 0 & & 1 - x_0 & & 1 - x_0 & & 1 & & 1 & & 1 + \Delta_1 & & 0
\end{array}
$$

Problems with Dense-Time Control (2)



- The controller is Non-Zeno; One untimed behavior: $(\ell_0\ell_1\ell_2)^\omega$
- Let Δ_k = time spent in ℓ_2 in the k-th loop from ℓ_0 to ℓ_0
- It implies: $\forall k, \sum_{i=1}^{k} \Delta_i < 1 - x_0$, with $\forall i, \Delta_i > 0$
- Must hold for ever: $\sum_{k=1}^{k=+\infty} \Delta_k < 1 - x_0$ with $\forall k, \Delta_k > 0$

Problems with Dense-Time Control (2)



- The controller is Non-Zeno; One untimed behavior: $(\ell_0\ell_1\ell_2)^\omega$
- Let Δ_k = time spent in ℓ_2 in the k-th loop from ℓ_0 to ℓ_0
- It implies: $\forall k, \sum_{i=1}^{k} \Delta_i < 1 - x_0$, with $\forall i, \Delta_i > 0$
- Must hold for ever: $\sum_{k=1}^{k=+\infty} \Delta_k < 1 - x_0$ with $\forall k, \Delta_k > 0$

The Controller is Non-Zeno but not Implementable !!!

Sampling Control

- Let $a \in \mathbb{Q}^*$ be a sampling rate
- An a-controller is a controller that can do actions only at $k \cdot a, k \geq 1$ and $k \in \mathbb{N}$

Sampling Control

- Let $a \in \mathbb{Q}^*$ be a sampling rate
- An a-controller is a controller that can do actions only at $k \cdot a, k \geq 1$ and $k \in \mathbb{N}$

Known Sampling Rate Control Problem (KSR)

Input: $a \in \mathbb{Q}^*$, Bad (states), G a TGA
Problem: Is there a a-controller for G that avoids Bad ?

Sampling Control

- Let $a \in \mathbb{Q}^*$ be a sampling rate
- An a-controller is a controller that can do actions only at $k \cdot a, k \geq 1$ and $k \in \mathbb{N}$

Known Sampling Rate Control Problem (KSR)

Input: $a \in \mathbb{Q}^*$, Bad (states), G a TGA
Problem: Is there a a-controller for G that avoids Bad ?

Theorem ([Henzinger & Kopke'99])

The Known Sampling Rate Control Problem is decidable.

Sampling Control

- Let $a \in \mathbb{Q}^*$ be a sampling rate
- An a-controller is a controller that can do actions only at $k \cdot a, k \geq 1$ and $k \in \mathbb{N}$

Unknown Sampling Rate Control Problem (USR)

Input: Bad (states), G a TGA
Problem: Is there a sampling rate $a \in \mathbb{Q}^*$ such that there is a a-controller for G that avoids Bad ?

Sampling Control

- Let $a \in \mathbb{Q}^*$ be a sampling rate
- An a-controller is a controller that can do actions only at $k \cdot a, k \geq 1$ and $k \in \mathbb{N}$

Unknown Sampling Rate Control Problem (USR)

Input: Bad (states), G a TGA
Problem: Is there a sampling rate $a \in \mathbb{Q}^*$ such that there is a a-controller for G that avoids Bad ?

Theorem ([HSCC'02])

The Unknown Sampling Rate Control Problem is undecidable.

Summary of the Results

Decidability results for the safety control problem on LHA:

	Known Switch Cond.	Unknown Switch Cond.
Timed Auto.	√ [Maler et al.'95]	√ [Maler et al.'95]
Init. Rect. Auto	√ [Henzinger et al.'99]	× [Henzinger et al.'95]
Rect. Auto.	× [Henzinger et al.'99]	× [Henzinger et al.'99]

	Known Sampling Rate	Unknown SR
Timed Auto.	√ [Hoffmann & Wong-Toi'92]	× [HSCC'02]
Init. Rect. Auto.	√ [Henzinger & Kopke'97]	× [HSCC'02]
Rect. Auto.	√ [Henzinger & Kopke'97]	× [HSCC'02]

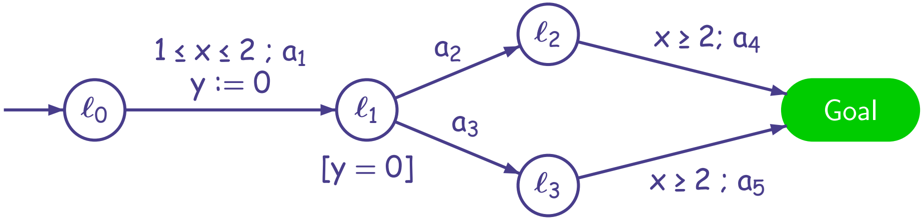
√: Decidable ×: Undecidable

Recent result [Bouyer et al.'06]
The reachability USC-CP is decidable for o-minimal automata.
Results on implementation of Timed Automata
[De Wulf et al.'04b, De Wulf et al.'04a, De Wulf et al.'05b]

Selection 2
Optimal Controllers

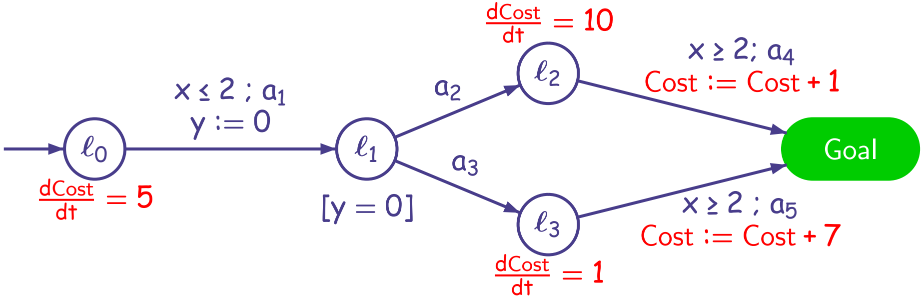
Joint work with Patricia Bouyer, Emmanuel Fleury and Kim G. Larsen
[FSTTCS'04, GDV'04]

Optimal Reachability for Timed Automata



- Reachability for Timed Automata [Alur & Dill'94]

Optimal Reachability for Timed Automata

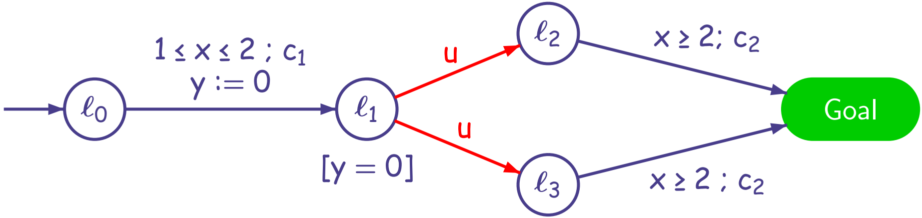


- Reachability for Timed Automata [Alur & Dill'94]
- Optimal Reachability for Priced (or Weighted) Timed Automata [Larsen et al.'01, Alur et al.'01]

$$(\ell_0,0,0) \xrightarrow{1} (\ell_0,1,1) \xrightarrow{a_1\ a_2} (\ell_2,1,0) \xrightarrow{3} (\ell_2,4,3) \xrightarrow{a_4} (Goal,4,3)$$

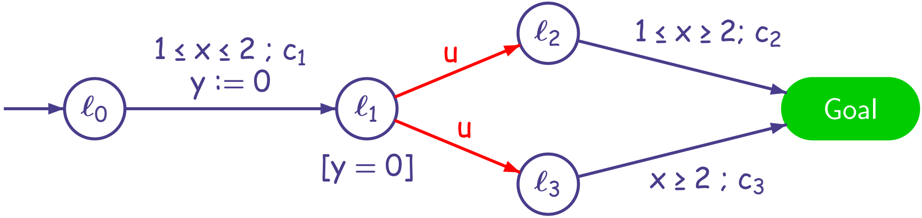
$$Cost = 1 \cdot 5 + 3 \cdot 10 + 1 = 36$$

Optimal Reachability for Timed Automata



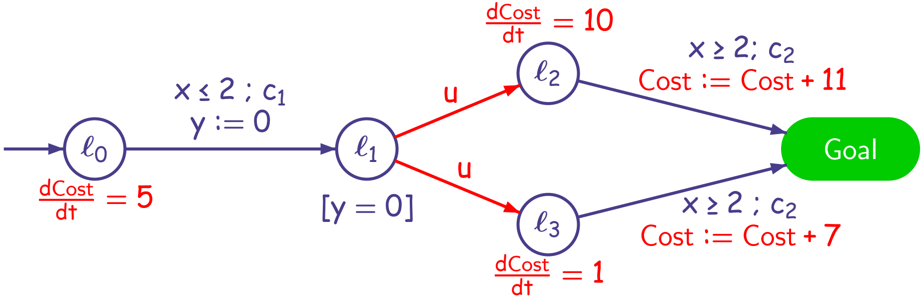
- Reachability for Timed Automata [Alur & Dill'94]
- Optimal Reachability for Priced (or Weighted) Timed Automata [Larsen et al.'01, Alur et al.'01]
- Control for Timed *Game* Automata [Maler et al.'95]

Optimal Reachability for Timed Automata



- Reachability for Timed Automata [Alur & Dill'94]
- Optimal Reachability for Priced (or Weighted) Timed Automata [Larsen et al.'01, Alur et al.'01]
- Control for Timed Game Automata [Maler et al.'95]
- Time Optimal Control (Reachability) [Asarin & Maler'99]

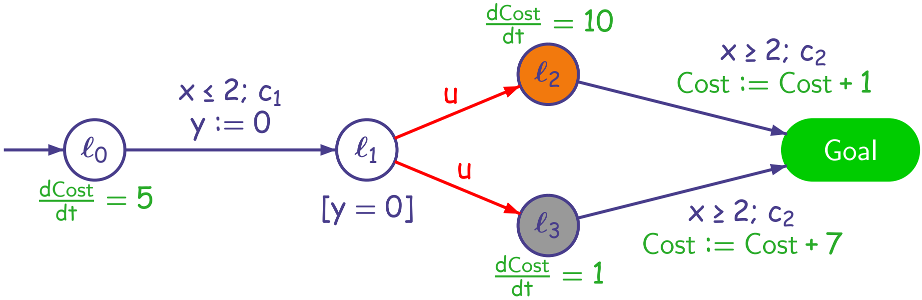
Optimal Reachability for Timed Automata



- Reachability for Timed Automata [Alur & Dill'94]
- Optimal Reachability for Priced (or Weighted) Timed Automata [Larsen et al.'01, Alur et al.'01]
- Control for Timed Game Automata [Maler et al.'95]
- Time Optimal Control (Reachability) [Asarin & Maler'99]

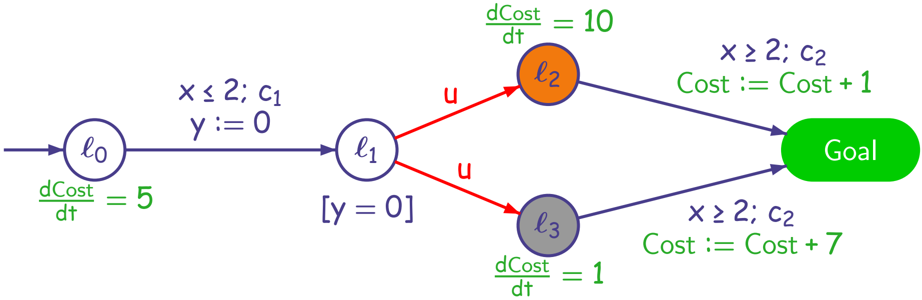
Optimal Control for Priced Timed Game Automata ?

A Small Example



- What is the **best** cost **whatever** the environment does ?

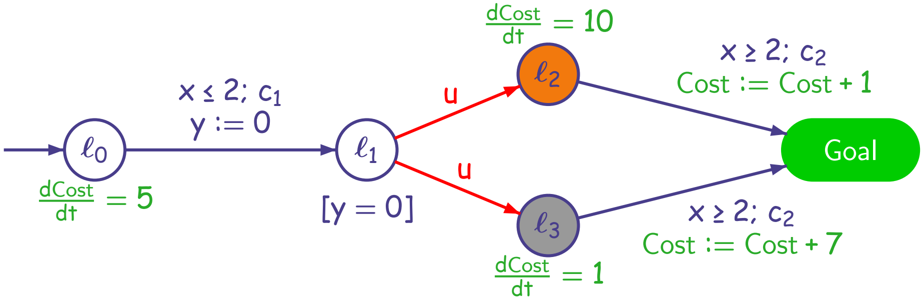
A Small Example



- What is the best cost whatever the environment does ?

$$\inf_{0 \leq t \leq 2} \max\{5t + 10(2-t) + 1, 5t + (2-t) + 7\} = 14 + \frac{1}{3}$$

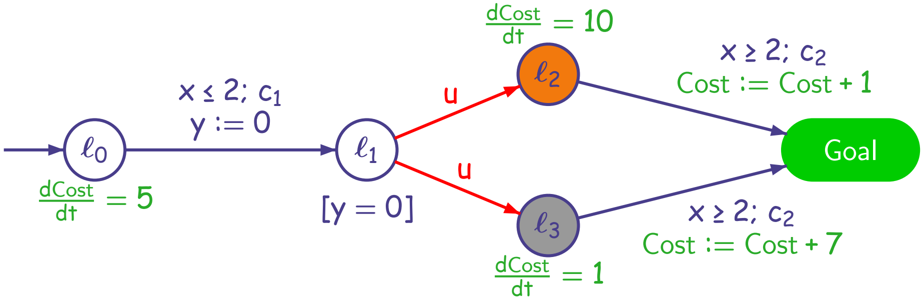
A Small Example



- What is the best cost whatever the environment does ?

$$\inf_{0 \leq t \leq 2} \max\{5t + 10(2-t) + 1, 5t + (2-t) + 7\} = 14 + \frac{1}{3}$$

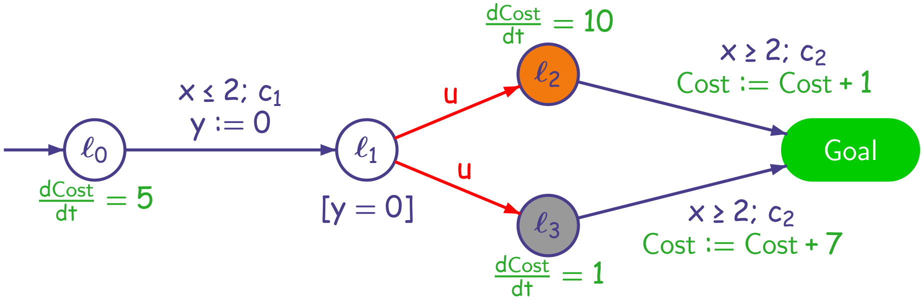
A Small Example



- What is the best cost whatever the environment does ?

$$\inf_{0 \leq t \leq 2} \max\{5t + 10(2 - t) + 1, 5t + (2 - t) + 7\} = 14 + \frac{1}{3}$$

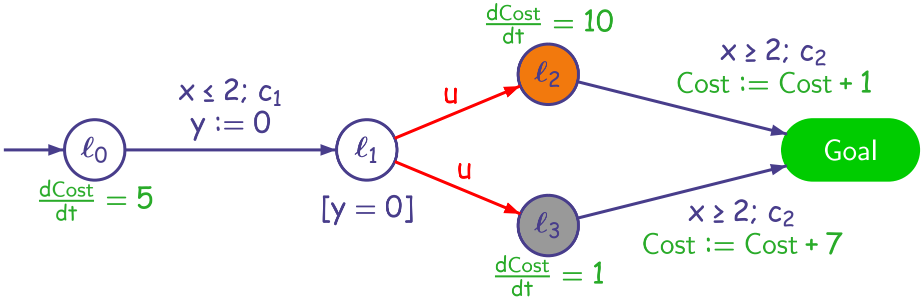
A Small Example



- What is the best cost whatever the environment does ?

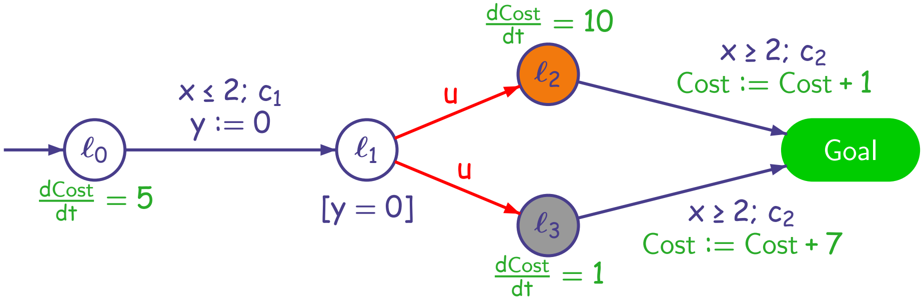
$$\inf_{0 \leq t \leq 2} \max\{5t + 10(2-t) + 1, 5t + (2-t) + 7\} = 14 + \frac{1}{3}$$

A Small Example



- What is the best cost whatever the environment does ?
- Is there a strategy to achieve this optimal cost ?

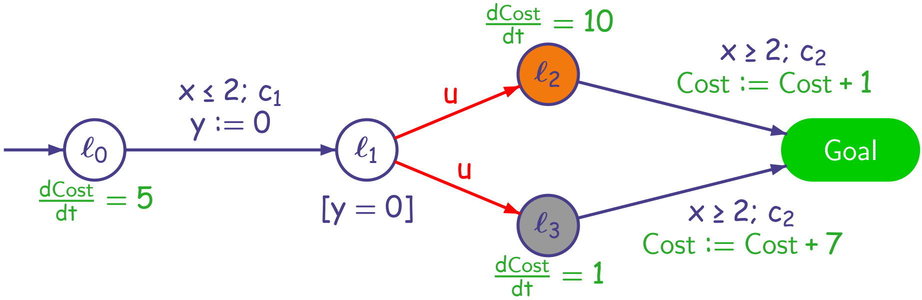
A Small Example



- What is the best cost whatever the environment does ?
- Is there a strategy to achieve this optimal cost ?

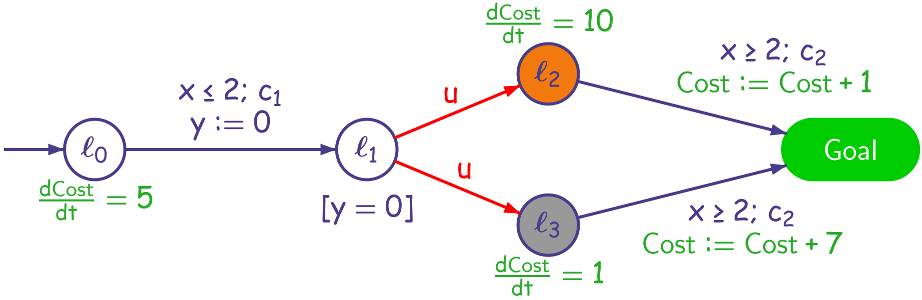
Yes: wait in ℓ_0 until $t = \frac{4}{3}$ and then fire c_1

A Small Example



- What is the best cost whatever the environment does ?
- Is there a strategy to achieve this optimal cost ?
  Yes: wait in ℓ_0 until $t = \frac{4}{3}$ and then fire c_1
- Can we compute such a strategy ?
  Yes: but need memory sometimes

Optimal Control Problems

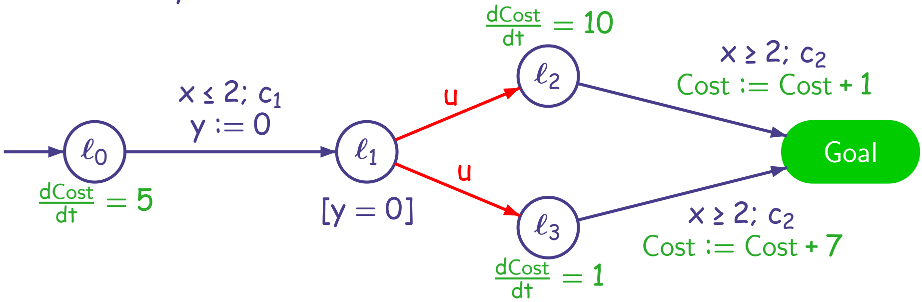


Can we find algorithms for these problems on PTGA ?

1. Compute the optimal cost
2. Decide if there is an optimal strategy
3. Compute an optimal strategy (if one exists)

From Optimal Control to Control

A Reachability TGA $\mathcal{A}$

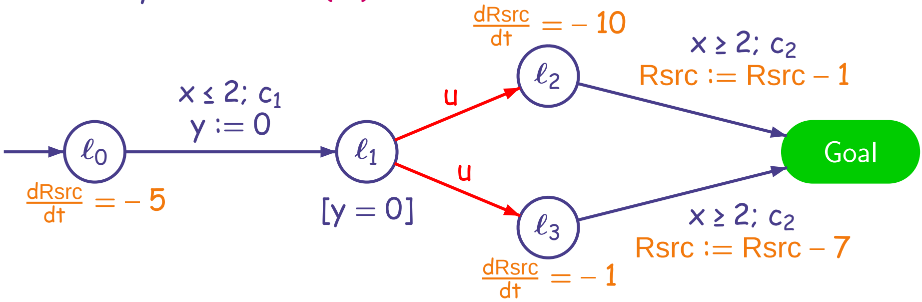


- Transform $\mathcal{A}$ in Linear Hybrid Game Automaton $H(\mathcal{A})$
- Define the reachability game for $H(\mathcal{A})$ with goal: $Goal \wedge Rsrc \geq 0$

Optimal Control for $\mathcal{A}$ $\Longleftrightarrow$ Reachability Control for $H(\mathcal{A})$

From Optimal Control to Control

A Linear Hybrid Game $H(\mathcal{A})$

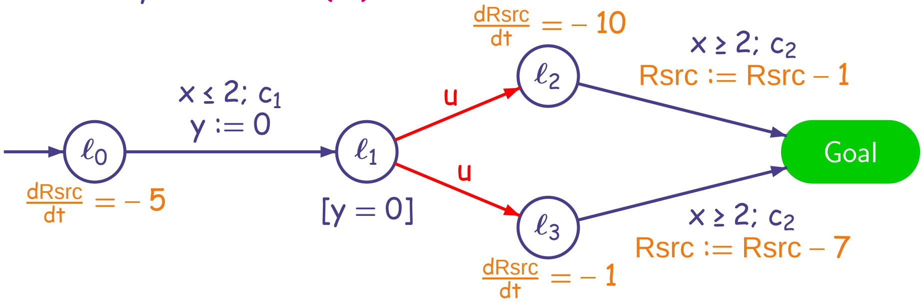


- Transform $\mathcal{A}$ in Linear Hybrid Game Automaton $H(\mathcal{A})$
- Define the reachability game for $H(\mathcal{A})$ with goal: $\text{Goal} \wedge \text{Rsrc} \geq 0$

Optimal Control for $\mathcal{A}$ $\Longleftrightarrow$ Reachability Control for $H(\mathcal{A})$

From Optimal Control to Control

A Linear Hybrid Game $H(\mathcal{A})$

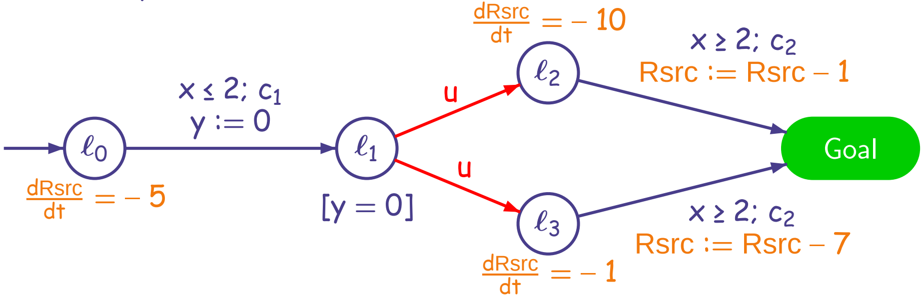


- Transform $\mathcal{A}$ in Linear Hybrid Game Automaton $H(\mathcal{A})$
- Define the reachability game for $H(\mathcal{A})$ with goal: $\text{Goal} \wedge Rsrc \geq 0$

Optimal Control for $\mathcal{A}$ $\Longleftrightarrow$ Reachability Control for $H(\mathcal{A})$

From Optimal Control to Control

A Linear Hybrid Game $H(\mathcal{A})$



- Transform $\mathcal{A}$ in Linear Hybrid Game Automaton $H(\mathcal{A})$
- Define the reachability game for $H(\mathcal{A})$ with goal: $Goal \wedge Rsrc \geq 0$

Optimal Control for $\mathcal{A} \iff$ Reachability Control for $H(\mathcal{A})$

Results for Optimal Control

Theorem (Reachability Control for LHA)

There is a semi-algorithm CompWin that computes the set of winning states for LHA.
Uses polyhedra instead of zones.

Results for Optimal Control

Let A be a Reachability Priced Timed Game Automaton such that:

- A is cost non-zeno *i.e.* $\exists\kappa$ s.t. every cycle in the region automaton of A has cost at least κ
- A is bounded *i.e.* all clocks in A are bounded

Results for Optimal Control

Let A be a Reachability Priced Timed Game Automaton such that:

- A is cost non-zeno *i.e.* $\exists \kappa$ s.t. every cycle in the region automaton of A has cost at least κ
- A is bounded *i.e.* all clocks in A are bounded

Theorem (Termination for Non-Zeno Cost)

The algorithm CompWin terminates for $H(A)$.

Results for Optimal Control

Let A be a Reachability Priced Timed Game Automaton such that:

- A is cost non-zeno *i.e.* $\exists\kappa$ s.t. every cycle in the region automaton of A has cost at least κ
- A is bounded *i.e.* all clocks in A are bounded

Theorem (Termination for Non-Zeno Cost)

The algorithm CompWin terminates for $H(A)$.

Theorem (Optimal Cost Computation)

1. Optimal Cost is computable.
2. Optimal Strategy Existence Problem is decidable.

Results for Optimal Control

Let A be a Reachability Priced Timed Game Automaton such that:

- A is cost non-zeno *i.e.* $\exists\kappa$ s.t. every cycle in the region automaton of A has cost at least κ
- A is bounded *i.e.* all clocks in A are bounded

Theorem (Termination for Non-Zeno Cost)

The algorithm CompWin terminates for $H(A)$.

Theorem (Optimal Cost Computation)

1. Optimal Cost is computable.
2. Optimal Strategy Existence Problem is decidable.

Theorem ([Brihaye et al.'05])

Non-Zeno Cost is a necessary assumption.

Summary of the Results

What's decidable about optimal control?

- Non-Zeno Cost [FSTTCS'04]
- O-minimal automata [Bouyer et al.'07]
- 1-clock PTGA (3EXPTIME) [Bouyer et al.'06a]

What's undecidable about optimal control?

- 5-clock Zeno PTGA [Brihaye et al.'05]
- 3-clock Zeno PTGA [Bouyer et al.'06b]

What's decidable for infinite schedules (safety) ?

- Mean Cost decidable for PTA [Bouyer et al.'04a]

What's open?

Optimal Mean Cost for PTGA

Summary of the Results

What's decidable about optimal control?

- Non-Zeno Cost [FSTTCS'04]
- O-minimal automata [Bouyer et al.'07]
- 1-clock PTGA (3EXPTIME) [Bouyer et al.'06a]

What's undecidable about optimal control?

- 5-clock Zeno PTGA [Brihaye et al.'05]
- 3-clock Zeno PTGA [Bouyer et al.'06b]

What's decidable for infinite schedules (safety) ?

- Mean Cost decidable for PTA [Bouyer et al.'04a]

What's open?

Optimal Mean Cost for PTGA

Summary of the Results

What's decidable about optimal control?

- Non-Zeno Cost [FSTTCS'04]
- O-minimal automata [Bouyer et al.'07]
- 1-clock PTGA (3EXPTIME) [Bouyer et al.'06a]

What's undecidable about optimal control?

- 5-clock Zeno PTGA [Brihaye et al.'05]
- 3-clock Zeno PTGA [Bouyer et al.'06b]

What's decidable for infinite schedules (safety) ?

- Mean Cost decidable for PTA [Bouyer et al.'04a]

What's open?

Optimal Mean Cost for PTGA

Summary of the Results

What's decidable about optimal control?

- Non-Zeno Cost [FSTTCS'04]
- O-minimal automata [Bouyer et al.'07]
- 1-clock PTGA (3EXPTIME) [Bouyer et al.'06a]

What's undecidable about optimal control?

- 5-clock Zeno PTGA [Brihaye et al.'05]
- 3-clock Zeno PTGA [Bouyer et al.'06b]

What's decidable for infinite schedules (safety) ?

- Mean Cost decidable for PTA [Bouyer et al.'04a]

What's open?

Optimal Mean Cost for PTGA

Next:

- Control of Timed Systems: Basics
- Selected Contributions
- **Conclusion & Perspectives**

Conclusion

- Other Recent Research Results:
  - Efficient algorithms for solving Timed Games
  - Expressiveness of timed automata vs. timed Petri nets
  - Fault Diagnosis
- Ongoing Collaborations:
  - In France:
    LSV (Cachan),
    LAMSADE (Paris, Dauphine),
    VERIMAG (Grenoble),
    IRISA (Rennes),
    LaBRI (Bordeaux)
    Funded Projects CHRONO, CORTOS, DOTS
  - Abroad:
    Aalborg University (Denmark),
    Université Libre de Bruxelles (Belgium)
    NICTA Sydney (Australia)

Conclusion

- Other Recent Research Results:
  - Efficient algorithms for solving Timed Games
  - Expressiveness of timed automata vs. timed Petri nets
  - Fault Diagnosis
- Ongoing Collaborations:
  - In France:
    LSV (Cachan),
    LAMSADE (Paris, Dauphine),
    VERIMAG (Grenoble),
    IRISA (Rennes),
    LaBRI (Bordeaux)
    Funded Projects CHRONO, CORTOS, DOTS
  - Abroad:
    Aalborg University (Denmark),
    Université Libre de Bruxelles (Belgium)
    NICTA Sydney (Australia)

Research Perspectives

- Efficient Algorithms for Safety, Büchi games
- Concurrent Semantics (unfoldings) for Network of Timed Automata
- Applications of Control Theory to Other Domain
  Non-Interference
- Application of theories and tools to real systems
  e.g. L4 based-technology developped at NICTA/Sydney

Tak !

Research Perspectives

- Efficient Algorithms for Safety, Büchi games
- Concurrent Semantics (unfoldings) for Network of Timed Automata
- Applications of Control Theory to Other Domain
  Non-Interference
- Application of theories and tools to real systems
  e.g. L4 based-technology developped at NICTA/Sydney

Tak !

References

[Alur et al.'01] R. Alur, S. La Torre, and G. J. Pappas.
Optimal paths in weighted timed automata.
In *Proc. 4th Int. Work. Hybrid Systems: Computation and Control (HSCC'01)*, volume 2034 of *LNCS*, pages 49–62. Springer, 2001.

[Alur et al.'04] R. Alur, M, Bernadsky, and P. Madhusudan.
Optimal reachability in weighted timed games.
In *Proc. 31st International Colloquium on Automata, Languages and Programming (ICALP'04)*, Lecture Notes in Computer Science. Springer, 2004.

[Asarin & Maler'99] E. Asarin and O. Maler.
As soon as possible: Time optimal control for timed automata.
In *Proc. 2nd Int. Work. Hybrid Systems: Computation and Control (HSCC'99)*, volume 1569 of *LNCS*, pages 19–30. Springer, 1999.

[Alur & Dill'94] R. Alur and D. Dill.
A theory of timed automata.
Theoretical Computer Science B, 126:183–235, 1994.

[De Alfaro et al.'01] Luca de Alfaro, Thomas A. Henzinger, and Rupak Majumdar.
Symbolic algorithms for infinite-state games.
In *Proc. 12th International Conference on Concurrency Theory (CONCUR'01)*, volume 2154 of *LNCS*, pages 536–550. Springer, 2001.

[Asarin et al.'98] Eugene Asarin, Oded Maler, Amir Pnueli, and Joseph Sifakis.
Controller synthesis for timed automata.
In *Proc. IFAC Symposium on System Structure and Control*, pages 469–474. Elsevier Science, 1998.

References (cont.)

[Arnold et al.'03] André Arnold, Aymeric Vincent, and Igor Walukiewicz.
Games for synthesis of controllers with partial observation.
Theoretical Computer Science, 303(1):7–34,2003.

[Larsen et al.'01] Kim G. Larsen, Gerd Behrmann, Ansgar Fehnker, Thomas Hune, Paul Pettersson, Judi Romijn, and Frits Vaandrager.
Minimum-cost reachability for priced timed automata.
In *Proc. 4th International Workshop on Hybrid Systems: Computation and Control (HSCC'01)*, volume 2034 of *Lecture Notes in Computer Science*, pages 147–161. Springer, 2001.

[Bouyer et al.'06] Patricia Bouyer, Thomas Brihaye, and Fabrice Chevalier.
Control in o-minimal hybrid systems.
In *Proceedings of the 21st Annual IEEE Symposium on Logic in Computer Science (LICS'06)*, pages 367–378, Seattle, Washington, USA, August 2006. IEEE Computer Society Press.

[Büchi & Landweber'69] J.R. Büchi and L.H. Landweber.
Solving sequential conditions by finite-state operators.
Trans. of the AMS; 138:295–311.

[FSTTCS'04] Patricia Bouyer, Franck Cassez, Emmanuel Fleury, and Kim G. Larsen.
Optimal strategies in priced timed game automata.
In *Proc. of the 24th Int. Conf. on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'04)*, volume 3328 of *LNCS*, pages 148–160. Springer, 2004.

[GDV'04] Patricia Bouyer, Franck Cassez, Emmanuel Fleury, and Kim G. Larsen.
Synthesis of optimal strategies using HyTech.
In *Proc. of the Workshop on Games in Design and Verification (GDV'04)*, volume 119 of *Elec. Notes in Theo. Comp. Science*, pages 11–31. Elsevier, 2005.

References (cont.)

[Bouyer et al.'07] Patricia Bouyer, Thomas Brihaye, and Fabrice Chevalier.
Weighted o-minimal hybrid systems are more decidable than weighted timed automata!
In Sergei N. Artemov, editor, *Proceedings of the Symposium on Logical Foundations of Computer Science (LFCS'07)*, Lecture Notes in Computer Science, New-York, NY, USA, June 2007. Springer.
To appear.

[Bouyer et al.'06a] Patricia Bouyer, Kim G. Larsen, Nicolas Markey, and Jacob Illum Rasmussen.
Almost optimal strategies in one-clock priced timed automata.
In Naveen Garg and S. Arun-Kumar, editors, *Proceedings of the 26th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'06)*, volume 4337 of *Lecture Notes in Computer Science*, pages 345–356, Kolkata, India, December 2006. Springer.

[Bouyer et al.'06b] Patricia Bouyer, Thomas Brihaye, and Nicolas Markey.
Improved undecidability results on weighted timed automata.
Information Processing Letters, 98(5):188–194, June 2006.

[Bouyer et al.'04a] Patricia Bouyer, Ed Brinksma, and Kim G. Larsen.
Staying alive as cheaply as possible.
In Rajeev Alur and George J. Pappas, editors, *Proceedings of the 7th International Conference on Hybrid Systems: Computation and Control (HSCC'04)*, volume 2993 of *Lecture Notes in Computer Science*, pages 203–218, Philadelphia, Pennsylvania, USA, March 2004. Springer.

[De Wulf et al.'04a] Martin De Wulf, Laurent Doyen, Nicoals Markey, and Jean-François Raskin.
Robustness and implementability of timed automata.
In *Proceedings of FORMATS-FTRTFT 2004: Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant Systems*, Lecture Notes in Computer Science 3253, pages 118–133. Springer-Verlag, 2004.

References (cont.)

[De Wulf et al.'04b] Martin De Wulf, Laurent Doyen, and Jean-François Raskin.
Almost ASAP semantics: From timed models to timed implementations.
In *Proceedings of HSCC 2004: Hybrid SystemsŠComputation and Control*, Lecture Notes in Computer Science 2993, pages 296–310. Springer-Verlag, 2004.

[De Wulf et al.'05a] Martin De Wulf, Laurent Doyen, and Jean-François Raskin.
Almost ASAP semantics: From timed models to timed implementations.
Formal Aspects of Computing, 17(3):319–341, 2005.

[De Wulf et al.'05b] Martin De Wulf, Laurent Doyen, and Jean-François Raskin.
Systematic implementation of real-time models.
In *Proceedings of FM 2005: Formal Methods*, Lecture Notes in Computer Science 3582, pages 139–156. Springer-Verlag, 2005.

[HSCC'02] Franck Cassez, Thomas A. Henzinger, and Jean-François Raskin.
A comparison of control problems for timed and hybrid systems.
In *Proc. 5th Int. Workshop on Hybrid Systems: Computation and Control (HSCC'02)*, volume 2289 of *LNCS*, pages 134–148. Springer, 2002.

[Henzinger & Kopke'99] T.A. Henzinger and P.W. Kopke.
Discrete-time control for rectangular hybrid automata.
Theoretical Computer Science, 221:369–392, 1999.

[Henzinger et al.'99] Thomas A. Henzinger, Benjamin Horowitz, and Rupak Majumdar.
Rectangular hybrid games.
In *Proc. 10th International Conference on Concurrency Theory (CONCUR'99)*, volume 1664 of *Lecture Notes in Computer Science*, pages 320–335. Springer, 1999.

References (cont.)

[Henzinger et al.'95] Thomas A. Henzinger, Peter W. Kopke, Anuj Puri, and Pravin Varaiya. **What's decidable about hybrid automata?** *Journal of Computer and System Sciences*, 57:94–124, 1998.

[Henzinger & Kopke'97] Thomas A. Henzinger and Peter W. Kopke. **Discrete-time control for rectangular hybrid automata.** *Theoretical Computer Science*, 221:369–392, 1999.

[Hoffmann & Wong-Toi'92] G. Hoffmann and Howard Wong-Toi. **The input-output control of real-time discrete-event systems.** In *Proceedings of the 13th Annual Real-time Systems Symposium*, pages 256-265. IEEE Computer Society Press, 1992.

[La Torre et al.'02] Salvatore La Torre, Supratik Mukhopadhyay, and Aniello Murano. **Optimal-reachability and control for acyclic weighted timed automata.** In *Proc. 2nd IFIP International Conference on Theoretical Computer Science (TCS 2002)*, volume 223 of *IFIP Conference Proceedings*, pages 485–497. Kluwer, 2002.

[Maler et al.'95] Oded Maler, Amir Pnueli, and Joseph Sifakis. **On the synthesis of discrete controllers for timed systems.** In *Proc. 12th Annual Symposium on Theoretical Aspects of Computer Science (STACS'95)*, volume 900, pages 229–242. Springer, 1995.

[Ramadge & Wonham'87] P.J. Ramadge and W.M. Wonham. **Supervisory control of a class of discrete event processes.** *SIAM J. of Control and Optimization*, 25:206–230, 1987

[Ramadge & Wonham'89] P.J. Ramadge and W.M. Wonham. **The control of discrete event processes.** *Proc. of IEEE*, 77:81–98, 1989

References (cont.)

[Brihaye et al.'05] Thomas Brihaye, Véronique Bruyère, and Jean-François Raskin.
On optimal timed strategies.
In *FORMATS*, pages 49–64, 2005.

[Thistle & Wonham'94] J.G. Thistle and W.M. Wonham.
Control of infinite behavior of finite automata.
SIAM J. of Control and Optimization, 32:1075–1097, 1994

Timed Automata

[Alur & Dill'94]

A Timed Automaton $\mathcal{A}$ is a tuple $(L, \ell_0, Act, X, \text{inv}, \longrightarrow)$ where:

- L is a finite set of locations
- ℓ_0 is the initial location
- X is a finite set of clocks
- Act is a finite set of actions
- $\longrightarrow$ is a set of transitions of the form $\ell \xrightarrow{g,a,R} \ell'$ with:
  - $\ell, \ell' \in L$,
  - $a \in Act$
  - a guard g which is a clock constraint over X
  - a reset set R which is the set of clocks to be reset to 0

Clock constraints are boolean combinations of $x \sim k$ with $x \in C$ and $k \in \mathbb{Z}$ and $\sim \in \{\leq, <\}$.

Semantics of Timed Automata

Let $\mathcal{A} = (L, \ell_0, Act, X, inv, \longrightarrow)$ be a Timed Automaton.

A state (ℓ, v) of $\mathcal{A}$ is in $L \times \mathbb{R}_{\geq 0}^X$

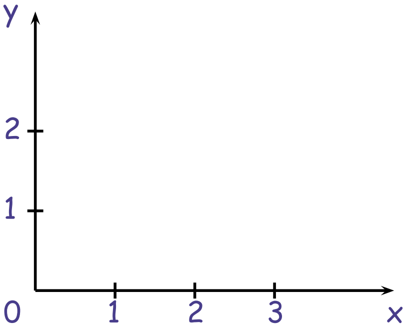
The semantics of $\mathcal{A}$ is a Timed Transition System $S_{\mathcal{A}} = (Q, q_0, Act \cup \mathbb{R}_{\geq 0}, \longrightarrow)$ with:

- $Q = L \times \mathbb{R}_{\geq 0}^X$
- $q_0 = (\ell_0, \overline{0})$
- $\longrightarrow$ consists in:

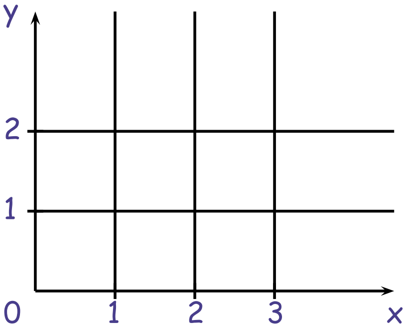
discrete transition: $(\ell, v) \xrightarrow{a} (\ell', v') \iff \begin{cases} \exists\, \ell \xrightarrow{g,a,r} \ell' \in \mathcal{A} \\ v \models g \\ v' = v[r \leftarrow 0] \\ v' \models inv(\ell') \end{cases}$

delay transition: $(\ell, v) \xrightarrow{d} (\ell, v + d) \iff d \in \mathbb{R}_{\geq 0} \land v + d \models inv(\ell)$

The Region Abstraction [Alur & Dill'94]



The Region Abstraction [Alur & Dill'94]

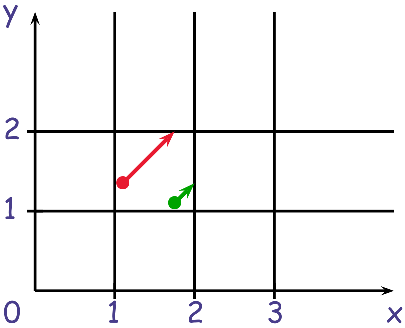


Build an equivalence relation which is of finite index and is:

- "compatible" with clock constraints ($g ::= x \sim c \quad g \wedge g$)

  $r, r' \in R \implies \forall$ constraints $g, \quad r \models g \iff r' \models g$

The Region Abstraction [Alur & Dill'94]



Build an equivalence relation which is of finite index and is:

- "compatible" with clock constraints ($g ::= x \sim c \quad g \wedge g$)

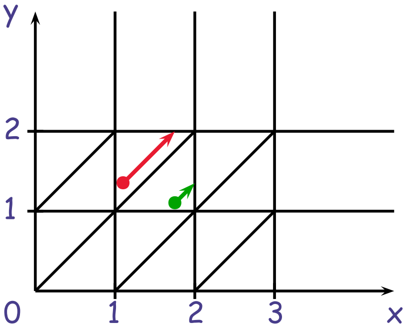
  $r, r' \in R \implies \forall$ constraints $g, \quad r \models g \iff r' \models g$

- "compatible" with time elapsing

  $r, r' \in R \implies$ same delay successor regions

The Region Abstraction

[Alur & Dill'94]

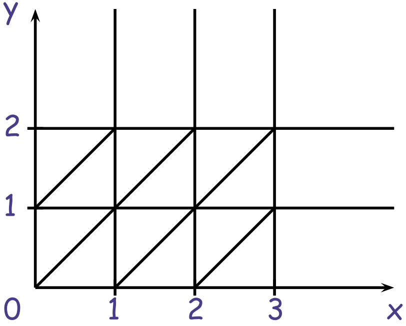


Build an equivalence relation which is of finite index and is:

- "compatible" with clock constraints ($g ::= x \sim c \quad g \wedge g$)
  $r, r' \in R \implies \forall$ constraints $g, \quad r \models g \iff r' \models g$
- "compatible" with time elapsing
  $r, r' \in R \implies$ same delay successor regions

The Region Abstraction

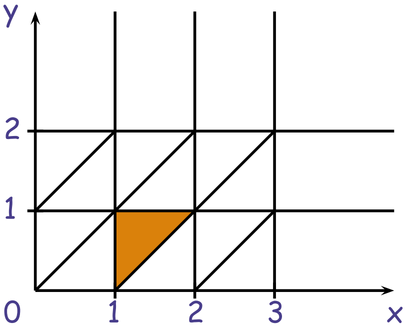
[Alur & Dill'94]



Build an equivalence relation which is of finite index and is:

- "compatible" with clock constraints $(g ::= x \sim c \quad g \wedge g)$
  $r, r' \in R \implies \forall$ constraints $g, \quad r \models g \iff r' \models g$
- "compatible" with time elapsing
  $r, r' \in R \implies$ same delay successor regions

The Region Abstraction [Alur & Dill'94]



region defined by

$I_x =]1;2[\quad I_y =]0;1[$

$\{x\} < \{y\}$

Build an equivalence relation which is of finite index and is:

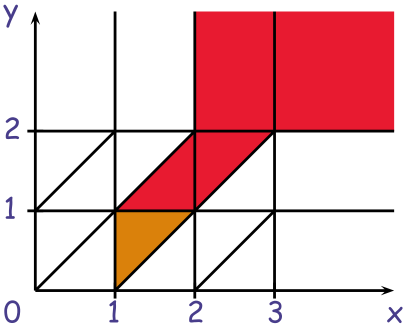
- "compatible" with clock constraints $(g ::= x \sim c \quad g \wedge g)$

  $r, r' \in R \implies \forall$ constraints g, $\quad r \models g \iff r' \models g$

- "compatible" with time elapsing

  $r, r' \in R \implies$ same delay successor regions

The Region Abstraction [Alur & Dill'94]



region defined by
$I_x =]1;2[I_y =]0;1[$
$\{x\} < \{y\}$

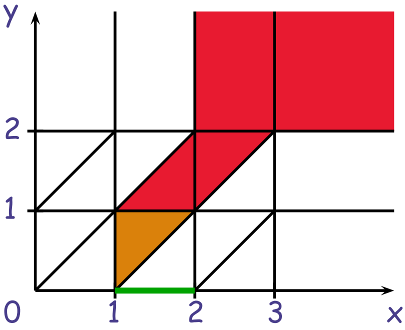
delay successors

Build an equivalence relation which is of finite index and is:

- "compatible" with clock constraints ($g ::= x \sim c \quad g \wedge g$)
  $r, r' \in R \implies \forall$ constraints g, $\quad r \models g \iff r' \models g$
- "compatible" with time elapsing
  $r, r' \in R \implies$ same delay successor regions

The Region Abstraction

[Alur & Dill'94]



region defined by
$I_x =]1;2[\; I_y =]0;1[$
$\{x\} < \{y\}$

delay successors

successor by reset

Build an equivalence relation which is of finite index and is:

- "compatible" with clock constraints ($g ::= x \sim c \quad g \wedge g$)
  $r, r' \in R \implies \forall$ constraints g, $\quad r \models g \iff r' \models g$
- "compatible" with time elapsing
  $r, r' \in R \implies$ same delay successor regions

The Region Automaton

- For each transition $\ell \xrightarrow{g,a,C:=0} \ell'$ of the TA
- Build transitions in the region automaton RA: $(\ell,R) \xrightarrow{a} (\ell',R')$ if:
  - there exists R″ a delay successor of R s.t.
  - R″ satisfies the guard g ($R'' \subseteq [\![g]\!]$)
  - $R''[C \leftarrow 0]$ is included in R′

a TA and its region automaton RA are time-abstract bisimilar

- The region automaton is finite
- Language accepted by the RA = untimed language accepted by the TA

  a timed word $w = (a,1.2)(b,3.4)(a,6.256)$; untimed$(w) = aba$
- Language Emptyness can be decided on the RA

The Region Automaton

- For each transition $\ell \xrightarrow{g,a,C:=0} \ell'$ of the TA
- Build transitions in the region automaton RA: $(\ell, R) \xrightarrow{a} (\ell', R')$ if:
  - there exists R'' a delay successor of R s.t.
  - R'' satisfies the guard g ($R'' \subseteq [\![g]\!]$)
  - $R''[C \leftarrow 0]$ is included in R'

a TA and its region automaton RA are time-abstract bisimilar

- The region automaton is finite
- Language accepted by the RA = untimed language accepted by the TA
  a timed word $w = (a, 1.2)(b, 3.4)(a, 6.256)$; $untimed(w) = aba$
- Language Emptyness can be decided on the RA

The Region Automaton

- For each transition $\ell \xrightarrow{g,a,C:=0} \ell'$ of the TA
- Build transitions in the region automaton RA: $(\ell, R) \xrightarrow{a} (\ell', R')$ if:
  - there exists R'' a delay successor of R s.t.
  - R'' satisfies the guard g ($R'' \subseteq [\![g]\!]$)
  - $R''[C \leftarrow 0]$ is included in R'

a TA and its region automaton RA are time-abstract bisimilar

- The region automaton is finite
- Language accepted by the RA = untimed language accepted by the TA

  a timed word $w = (a, 1.2)(b, 3.4)(a, 6.256)$; $untimed(w) = aba$
- Language Emptyness can be decided on the RA

The Region Automaton

- For each transition $\ell \xrightarrow{g,a,C:=0} \ell'$ of the TA
- Build transitions in the region automaton RA: $(\ell, R) \xrightarrow{a} (\ell', R')$ if:
  - there exists R'' a delay successor of R s.t.
  - R'' satisfies the guard g ($R'' \subseteq [\![g]\!]$)
  - $R''[C \leftarrow 0]$ is included in R'

a TA and its region automaton RA are time-abstract bisimilar

- The region automaton is finite
- Language accepted by the RA = untimed language accepted by the TA

  a timed word $w = (a, 1.2)(b, 3.4)(a, 6.256)$; untimed$(w) = aba$
- Language Emptyness can be decided on the RA

The Region Automaton

- For each transition $\ell \xrightarrow{g,a,C:=0} \ell'$ of the TA
- Build transitions in the region automaton RA: $(\ell, R) \xrightarrow{a} (\ell', R')$ if:
  - there exists R'' a delay successor of R s.t.
  - R'' satisfies the guard g ($R'' \subseteq [\![g]\!]$)
  - $R''[C \leftarrow 0]$ is included in R'

a TA and its region automaton RA are time-abstract bisimilar

- The region automaton is finite
- Language accepted by the RA = untimed language accepted by the TA

  a timed word $w = (a, 1.2)(b, 3.4)(a, 6.256)$; untimed$(w) = aba$
- Language Emptyness can be decided on the RA

The Region Automaton

- For each transition $\ell \xrightarrow{g,a,C:=0} \ell'$ of the TA
- Build transitions in the region automaton RA: $(\ell, R) \xrightarrow{a} (\ell', R')$ if:
  - there exists R'' a delay successor of R s.t.
  - R'' satisfies the guard g ($R'' \subseteq [\![g]\!]$)
  - $R''[C \leftarrow 0]$ is included in R'

a TA and its region automaton RA are time-abstract bisimilar

- The region automaton is finite
- Language accepted by the RA = untimed language accepted by the TA

  a timed word $w = (a, 1.2)(b, 3.4)(a, 6.256)$; untimed$(w) = aba$
- Language Emptyness can be decided on the RA

The Region Automaton

- For each transition $\ell \xrightarrow{g,a,C:=0} \ell'$ of the TA
- Build transitions in the region automaton RA: $(\ell, R) \xrightarrow{a} (\ell', R')$ if:
  - there exists R'' a delay successor of R s.t.
  - R'' satisfies the guard g ($R'' \subseteq [\![g]\!]$)
  - $R''[C \leftarrow 0]$ is included in R'

a TA and its region automaton RA are time-abstract bisimilar

- The region automaton is finite
- Language accepted by the RA = untimed language accepted by the TA

  a timed word $w = (a, 1.2)(b, 3.4)(a, 6.256)$; untimed$(w) = aba$
- Language Emptyness can be decided on the RA

The Region Automaton

- For each transition $\ell \xrightarrow{g,a,C:=0} \ell'$ of the TA
- Build transitions in the region automaton RA: $(\ell, R) \xrightarrow{a} (\ell', R')$ if:
  - there exists R'' a delay successor of R s.t.
  - R'' satisfies the guard g ($R'' \subseteq [\![g]\!]$)
  - $R''[C \leftarrow 0]$ is included in R'

a TA and its region automaton RA are time-abstract bisimilar

- The region automaton is finite
- Language accepted by the RA = untimed language accepted by the TA

  a timed word $w = (a, 1.2)(b, 3.4)(a, 6.256)$; $untimed(w) = aba$
- Language Emptyness can be decided on the RA

The Region Automaton

- For each transition $\ell \xrightarrow{g,a,C:=0} \ell'$ of the TA
- Build transitions in the region automaton RA: $(\ell, R) \xrightarrow{a} (\ell', R')$ if:
  - there exists R'' a delay successor of R s.t.
  - R'' satisfies the guard g ($R'' \subseteq [\![g]\!]$)
  - $R''[C \leftarrow 0]$ is included in R'

a TA and its region automaton RA are time-abstract bisimilar

- The region automaton is finite
- Language accepted by the RA = untimed language accepted by the TA
  a timed word $w = (a, 1.2)(b, 3.4)(a, 6.256)$; $untimed(w) = aba$
- Language Emptyness can be decided on the RA

The Region Automaton

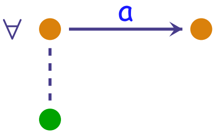
- For each transition $\ell \xrightarrow{g,a,C:=0} \ell'$ of the TA
- Build transitions in the region automaton RA: $(\ell, R) \xrightarrow{a} (\ell', R')$ if:
  - there exists R'' a delay successor of R s.t.
  - R'' satisfies the guard g ($R'' \subseteq [\![g]\!]$)
  - $R''[C \leftarrow 0]$ is included in R'

a TA and its region automaton RA are time-abstract bisimilar

- The region automaton is finite
- Language accepted by the RA = untimed language accepted by the TA

  a timed word $w = (a, 1.2)(b, 3.4)(a, 6.256)$; $untimed(w) = aba$
- Language Emptyness can be decided on the RA

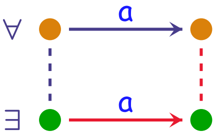
Time-abstract bisimulation



$$
\begin{array}{ccccccc}
(\ell_0, v_0) & \xrightarrow{a_1, t_1} & (\ell_1, v_1) & \xrightarrow{a_2, t_2} & (\ell_2, v_2) & \xrightarrow{a_3, t_3} & \cdots \\
\updownarrow & & \updownarrow & & \updownarrow & & \\
(\ell_0, R_0) & \xrightarrow{a_1} & (\ell_1, R_1) & \xrightarrow{a_2} & (\ell_2, R_2) & \xrightarrow{a_3} & \cdots
\end{array}
$$

with $v_i \in R_i$ for all i.

Time-abstract bisimulation



$$(\ell_0, v_0) \xrightarrow{a_1, t_1} (\ell_1, v_1) \xrightarrow{a_2, t_2} (\ell_2, v_2) \xrightarrow{a_3, t_3} \cdots$$

$$(\ell_0, R_0) \xrightarrow{a_1} (\ell_1, R_1) \xrightarrow{a_2} (\ell_2, R_2) \xrightarrow{a_3} \cdots$$

with $v_i \in R_i$ for all i.

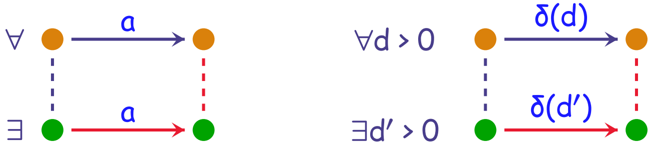
Time-abstract bisimulation

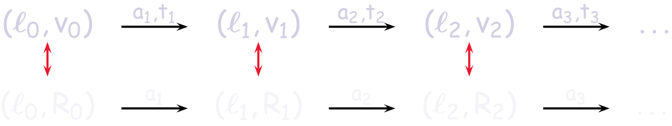
$$(\ell_0, v_0) \xrightarrow{a_1, t_1} (\ell_1, v_1) \xrightarrow{a_2, t_2} (\ell_2, v_2) \xrightarrow{a_3, t_3} \cdots$$

$$(\ell_0, R_0) \xrightarrow{a_1} (\ell_1, R_1) \xrightarrow{a_2} (\ell_2, R_2) \xrightarrow{a_3} \cdots$$

with $v_i \in R_i$ for all i.

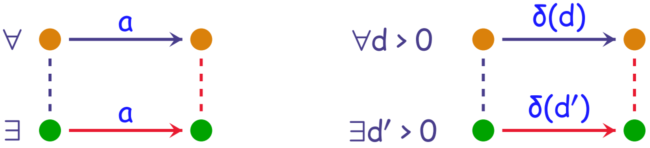
Time-abstract bisimulation





with $v_i \in R_i$ for all i.

Time-abstract bisimulation



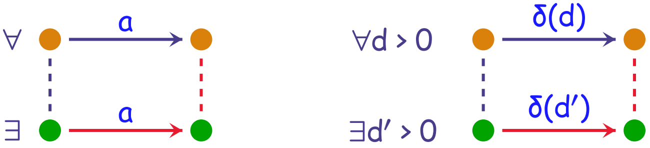
$$(\ell_0, v_0) \xrightarrow{a_1, t_1} (\ell_1, v_1) \xrightarrow{a_2, t_2} (\ell_2, v_2) \xrightarrow{a_3, t_3} \dots$$

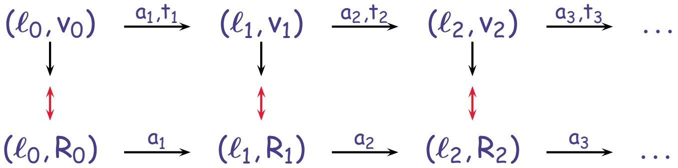
$$\updownarrow \qquad \updownarrow \qquad \updownarrow$$

$$(\ell_0, R_0) \xrightarrow{a_1} (\ell_1, R_1) \xrightarrow{a_2} (\ell_2, R_2) \xrightarrow{a_3} \dots$$

with $v_i \in R_i$ for all i.

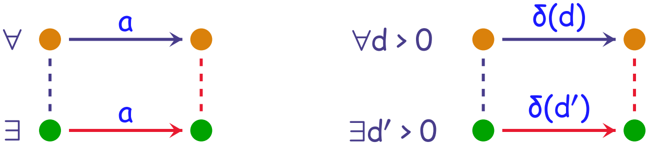
Time-abstract bisimulation





with $v_i \in R_i$ for all i.

Time-abstract bisimulation



$$
\begin{array}{ccccccc}
(\ell_0, v_0) & \xrightarrow{a_1, t_1} & (\ell_1, v_1) & \xrightarrow{a_2, t_2} & (\ell_2, v_2) & \xrightarrow{a_3, t_3} & \cdots \\
\updownarrow & & \updownarrow & & \updownarrow & & \\
(\ell_0, R_0) & \xrightarrow{a_1} & (\ell_1, R_1) & \xrightarrow{a_2} & (\ell_2, R_2) & \xrightarrow{a_3} & \cdots
\end{array}
$$

with $v_i \in R_i$ for all i.

Definition (Outcome in Timed Games)

Let $G = (L, \ell_0, Act, X, E, inv)$ be a TGA and f a strategy over G. The **outcome** $Outcome((\ell, v), f)$ of f from configuration (ℓ, v) in G is the subset of $Runs((\ell, v), G)$ defined inductively by:

- $(\ell, v) \in Outcome((\ell, v), f)$,
- if $\rho \in Outcome((\ell, v), f)$ then $\rho' = \rho \xrightarrow{e} (\ell', v') \in Outcome((\ell, v), f)$ if $\rho' \in Runs((\ell, v), G)$ and one of the following three conditions hold:
  1. $e \in Act_u$,
  2. $e \in Act_c$ and $e = f(\rho)$,
  3. $e \in \mathbb{R}_{\geq 0}$ and $\forall 0 \leq e' < e, \exists (\ell'', v'') \in (L \times \mathbb{R}^X_{\geq 0})$ s.t. $last(\rho) \xrightarrow{e'} (\ell'', v'') \wedge f(\rho \xrightarrow{e'} (\ell'', v'')) = \lambda$.
- an infinite run ρ is in $\in Outcome((\ell, v), f)$ if all the finite prefixes of ρ are in $Outcome((\ell, v), f)$.

States & Symbolic States

- $Q = L \times \mathbb{R}_{\geq 0}^{Clock}$ is the set of states of the TGA
  $$q = (\ell, v) \in Q$$
- Discrete predecessors of $X \subseteq Q$ by an action a:
  $$\mathrm{Pred}^a(X) = \{q \in Q \mid q \xrightarrow{a} q' \text{ and } q' \in X\}$$
- Time predecessors of $X \subseteq Q$:
  $$\mathrm{Pred}^\delta(X) = \{q \in Q \mid \exists t \geq 0 \mid q \xrightarrow{t} q' \text{ and } q' \in X\}$$
- Zone = conjunction of triangular constraints
  $x - y < 3, x \geq 2 \wedge 1 < y - x < 2$
- Symbolic State is defined by a State predicate (SP)
  $P = \cup_{i \in [1..n]}(\ell_{j_i}, Z_i)$, $\ell_{j_i} \in L$, Z_i is a zone
  $(\ell_1, 2 \leq x < 4)$ or $(\ell_0, x < 1 \wedge y - x \geq 2)$ or $(\ell_0, x \leq 2) \cup (\ell_2, x > 0)$

Effectiveness of Pred^a and Pred^δ

If P is a SP then $\mathrm{Pred}^a(P), \mathrm{Pred}^\delta(P)$ are SP and can be computed effectively. (There is a symbolic version for Pred^a and Pred^δ.)

States & Symbolic States

- $Q = L \times \mathbb{R}_{\geq 0}^{Clock}$ is the set of states of the TGA
  $q = (\ell, v) \in Q$
- Discrete predecessors of $X \subseteq Q$ by an action a:
  $$\text{Pred}^a(X) = \{q \in Q \mid q \xrightarrow{a} q' \text{ and } q' \in X\}$$
- Time predecessors of $X \subseteq Q$:
  $$\text{Pred}^\delta(X) = \{q \in Q \mid \exists t \geq 0 \mid q \xrightarrow{t} q' \text{ and } q' \in X\}$$
- Zone = conjunction of triangular constraints
  $x - y < 3, x \geq 2 \wedge 1 < y - x < 2$
- Symbolic State is defined by a State predicate (SP)
  $P = \cup_{i \in [1..n]}(\ell_{j_i}, Z_i)$, $\ell_{j_i} \in L$, Z_i is a zone
  $(\ell_1, 2 \leq x < 4)$ or $(\ell_0, x < 1 \wedge y - x \geq 2)$ or $(\ell_0, x \leq 2) \cup (\ell_2, x > 0)$

Effectiveness of Pred^a and Pred^δ

If P is a SP then $\text{Pred}^a(P), \text{Pred}^\delta(P)$ are SP and can be computed effectively. (There is a symbolic version for Pred^a and Pred^δ.)

States & Symbolic States

- $Q = L \times \mathbb{R}_{\geq 0}^{Clock}$ is the set of states of the TGA
  $q = (\ell, v) \in Q$
- Discrete predecessors of $X \subseteq Q$ by an action a:
  $$\text{Pred}^a(X) = \{q \in Q \mid q \xrightarrow{a} q' \text{ and } q' \in X\}$$
- Time predecessors of $X \subseteq Q$:
  $$\text{Pred}^\delta(X) = \{q \in Q \mid \exists t \geq 0 \mid q \xrightarrow{t} q' \text{ and } q' \in X\}$$
- Zone = conjunction of triangular constraints
  $x - y < 3, x \geq 2 \wedge 1 < y - x < 2$
- Symbolic State is defined by a State predicate (SP)
  $P = \cup_{i \in [1..n]}(\ell_{j_i}, Z_i)$, $\ell_{j_i} \in L$, Z_i is a zone
  $(\ell_1, 2 \leq x < 4)$ or $(\ell_0, x < 1 \wedge y - x \geq 2)$ or $(\ell_0, x \leq 2) \cup (\ell_2, x > 0)$

Effectiveness of Pred^a and Pred^δ

If P is a SP then $\text{Pred}^a(P), \text{Pred}^\delta(P)$ are SP and can be computed effectively. (There is a symbolic version for Pred^a and Pred^δ.)

States & Symbolic States

- $Q = L \times \mathbb{R}_{\geq 0}^{Clock}$ is the set of states of the TGA
$$q = (\ell, v) \in Q$$
- Discrete predecessors of $X \subseteq Q$ by an action a:
$$Pred^a(X) = \{q \in Q \mid q \xrightarrow{a} q' \text{ and } q' \in X\}$$
- Time predecessors of $X \subseteq Q$:
$$Pred^\delta(X) = \{q \in Q \mid \exists t \geq 0 \mid q \xrightarrow{t} q' \text{ and } q' \in X\}$$
- Zone = conjunction of triangular constraints
$x - y < 3, x \geq 2 \wedge 1 < y - x < 2$
- Symbolic State is defined by a State predicate (SP)
$P = \cup_{i \in [1..n]} (\ell_{j_i}, Z_i)$, $\ell_{j_i} \in L$, Z_i is a zone
$(\ell_1, 2 \leq x < 4)$ or $(\ell_0, x < 1 \wedge y - x \geq 2)$ or $(\ell_0, x \leq 2) \cup (\ell_2, x > 0)$

Effectiveness of $Pred^a$ and $Pred^\delta$

If P is a SP then $Pred^a(P), Pred^\delta(P)$ are SP and can be computed effectively. (There is a symbolic version for $Pred^a$ and $Pred^\delta$.)

States & Symbolic States

- $Q = L \times \mathbb{R}_{\geq 0}^{Clock}$ is the set of states of the TGA
  $q = (\ell, v) \in Q$
- Discrete predecessors of $X \subseteq Q$ by an action a:
  $$\text{Pred}^a(X) = \{q \in Q \mid q \xrightarrow{a} q' \text{ and } q' \in X\}$$
- Time predecessors of $X \subseteq Q$:
  $$\text{Pred}^\delta(X) = \{q \in Q \mid \exists t \geq 0 \mid q \xrightarrow{t} q' \text{ and } q' \in X\}$$
- Zone = conjunction of triangular constraints
  $x - y < 3, x \geq 2 \wedge 1 < y - x < 2$
- Symbolic State is defined by a State predicate (SP)
  $P = \cup_{i \in [1..n]}(\ell_{j_i}, Z_i)$, $\ell_{j_i} \in L$, Z_i is a zone
  $(\ell_1, 2 \leq x < 4)$ or $(\ell_0, x < 1 \wedge y - x \geq 2)$ or $(\ell_0, x \leq 2) \cup (\ell_2, x > 0)$

Effectiveness of Pred^a and Pred^δ

If P is a SP then $\text{Pred}^a(P), \text{Pred}^\delta(P)$ are SP and can be computed effectively. (There is a symbolic version for Pred^a and Pred^δ.)

States & Symbolic States

- $Q = L \times \mathbb{R}_{\geq 0}^{Clock}$ is the set of states of the TGA
  $$q = (\ell, v) \in Q$$
- Discrete predecessors of $X \subseteq Q$ by an action a:
  $$\mathrm{Pred}^a(X) = \{q \in Q \mid q \xrightarrow{a} q' \text{ and } q' \in X\}$$
- Time predecessors of $X \subseteq Q$:
  $$\mathrm{Pred}^\delta(X) = \{q \in Q \mid \exists t \geq 0 \mid q \xrightarrow{t} q' \text{ and } q' \in X\}$$
- Zone = conjunction of triangular constraints
  $x - y < 3,\ x \geq 2 \wedge 1 < y - x < 2$
- Symbolic State is defined by a State predicate (SP)
  $P = \cup_{i \in [1..n]}(\ell_{j_i}, Z_i),\ \ell_{j_i} \in L,\ Z_i$ is a zone
  $(\ell_1, 2 \leq x < 4)$ or $(\ell_0, x < 1 \wedge y - x \geq 2)$ or $(\ell_0, x \leq 2) \cup (\ell_2, x > 0)$

Effectiveness of Pred^a and Pred^δ

If P is a SP then $\mathrm{Pred}^a(P), \mathrm{Pred}^\delta(P)$ are SP and can be computed effectively. (There is a symbolic version for Pred^a and Pred^δ.)

States & Symbolic States

- $Q = L \times \mathbb{R}_{\geq 0}^{Clock}$ is the set of states of the TGA

  $$q = (\ell, v) \in Q$$

- Discrete predecessors of $X \subseteq Q$ by an action a:

  $$\mathrm{Pred}^a(X) = \{q \in Q \mid q \xrightarrow{a} q' \text{ and } q' \in X\}$$

- Time predecessors of $X \subseteq Q$:

  $$\mathrm{Pred}^\delta(X) = \{q \in Q \mid \exists t \geq 0 \mid q \xrightarrow{t} q' \text{ and } q' \in X\}$$

- Zone = conjunction of triangular constraints

  $x - y < 3, x \geq 2 \wedge 1 < y - x < 2$

- Symbolic State is defined by a State predicate (SP)

  $P = \cup_{i \in [1..n]}(\ell_{j_i}, Z_i)$, $\ell_{j_i} \in L$, Z_i is a zone

  $(\ell_1, 2 \leq x < 4)$ or $(\ell_0, x < 1 \wedge y - x \geq 2)$ or $(\ell_0, x \leq 2) \cup (\ell_2, x > 0)$

Effectiveness of Pred^a and Pred^δ

If P is a SP then $\mathrm{Pred}^a(P), \mathrm{Pred}^\delta(P)$ are SP and can be computed effectively. (There is a symbolic version for Pred^a and Pred^δ.)

States & Symbolic States

- $Q = L \times \mathbb{R}_{\geq 0}^{Clock}$ is the set of states of the TGA
  $$q = (\ell, v) \in Q$$
- Discrete predecessors of $X \subseteq Q$ by an action a:
  $$\mathrm{Pred}^a(X) = \{q \in Q \mid q \xrightarrow{a} q' \text{ and } q' \in X\}$$
- Time predecessors of $X \subseteq Q$:
  $$\mathrm{Pred}^\delta(X) = \{q \in Q \mid \exists t \geq 0 \mid q \xrightarrow{t} q' \text{ and } q' \in X\}$$
- Zone = conjunction of triangular constraints
  $x - y < 3, x \geq 2 \wedge 1 < y - x < 2$
- Symbolic State is defined by a State predicate (SP)
  $P = \cup_{i \in [1..n]}(\ell_{j_i}, Z_i)$, $\ell_{j_i} \in L$, Z_i is a zone
  $(\ell_1, 2 \leq x < 4)$ or $(\ell_0, x < 1 \wedge y - x \geq 2)$ or $(\ell_0, x \leq 2) \cup (\ell_2, x > 0)$

Effectiveness of Pred^a and Pred^δ

If P is a SP then $\mathrm{Pred}^a(P), \mathrm{Pred}^\delta(P)$ are SP and can be computed effectively. (There is a symbolic version for Pred^a and Pred^δ.)

Symbolic Computation For Timed Games

X is a state predicate

- $\mathsf{cPred}(X) = \bigcup_{c \in Act_c} \mathsf{Pred}^c(X)$ $\qquad$ $\mathsf{uPred}(X) = \bigcup_{u \in Act_u} \mathsf{Pred}^u(X)$
  cPred and uPred are effectively computable
- $\mathsf{Pred}_\delta(X, Y)$: Time controllable predecessors of X avoiding Y:

q $\qquad$ $q' \in X$

$\mathsf{Pred}_\delta(X, Y)$ is effectively computable for state predicates X, Y

- Controllable Predecessors Operator for Timed Games

$$\pi_\delta(X) = \mathsf{Pred}_\delta\left(\mathsf{cPred}(X), \mathsf{uPred}(\overline{X})\right)$$

$\pi_\delta(X)$ is effectively computable for state predicate X.

Symbolic Computation For Timed Games

X is a state predicate

- $\text{cPred}(X) = \bigcup_{c \in Act_c} \text{Pred}^c(X)$ $\text{uPred}(X) = \bigcup_{u \in Act_u} \text{Pred}^u(X)$
  cPred and uPred are effectively computable
- $\text{Pred}_\delta(X, Y)$: Time controllable predecessors of X avoiding Y:

q $q' \in X$

$\text{Pred}_\delta(X, Y)$ is effectively computable for state predicates X, Y

- Controllable Predecessors Operator for Timed Games

$$\pi_\delta(X) = \text{Pred}_\delta\left(\text{cPred}(X), \text{uPred}(\overline{X})\right)$$

$\pi_\delta(X)$ is effectively computable for state predicate X.

Symbolic Computation For Timed Games

X is a state predicate

- $\text{cPred}(X) = \bigcup_{c \in Act_c} \text{Pred}^c(X)$ $\text{uPred}(X) = \bigcup_{u \in Act_u} \text{Pred}^u(X)$
  cPred and uPred are effectively computable
- $\text{Pred}_\delta(X, Y)$: Time controllable predecessors of X avoiding Y:

q $q' \in X$

$\text{Pred}_\delta(X, Y)$ is effectively computable for state predicates X, Y

- Controllable Predecessors Operator for Timed Games

$$\pi_\delta(X) = \text{Pred}_\delta\left(\text{cPred}(X), \text{uPred}(\overline{X})\right)$$

$\pi_\delta(X)$ is effectively computable for state predicate X.

Symbolic Computation For Timed Games

X is a state predicate

- $cPred(X) = \bigcup_{c \in Act_c} Pred^c(X)$ $\qquad$ $uPred(X) = \bigcup_{u \in Act_u} Pred^u(X)$
  cPred and uPred are effectively computable
- $Pred_\delta(X, Y)$: Time controllable predecessors of X avoiding Y:

$$q \xrightarrow{\quad t \quad} q' \in X$$

$Pred_\delta(X, Y)$ is effectively computable for state predicates X, Y

- Controllable Predecessors Operator for Timed Games

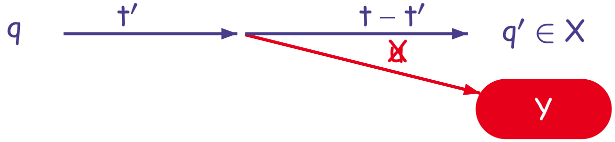
$$\pi_\delta(X) = Pred_\delta\left(cPred(X), uPred(\overline{X})\right)$$

$\pi_\delta(X)$ is effectively computable for state predicate X.

Symbolic Computation For Timed Games

X is a state predicate

- $cPred(X) = \bigcup_{c \in Act_c} Pred^c(X)$ $\quad$ $uPred(X) = \bigcup_{u \in Act_u} Pred^u(X)$
  cPred and uPred are effectively computable
- $Pred_\delta(X, Y)$: Time controllable predecessors of X avoiding Y:



$Pred_\delta(X, Y)$ is effectively computable for state predicates X, Y

- Controllable Predecessors Operator for Timed Games

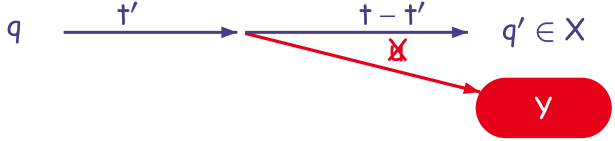
$$\pi_\delta(X) = Pred_\delta\left(cPred(X), uPred(\overline{X})\right)$$

$\pi_\delta(X)$ is effectively computable for state predicate X.

Symbolic Computation For Timed Games

X is a state predicate

- $cPred(X) = \bigcup_{c \in Act_c} Pred^c(X)$ $\qquad$ $uPred(X) = \bigcup_{u \in Act_u} Pred^u(X)$
  cPred and uPred are effectively computable
- $Pred_\delta(X, Y)$: Time controllable predecessors of X avoiding Y:



$Pred_\delta(X, Y)$ is effectively computable for state predicates X, Y

- Controllable Predecessors Operator for Timed Games

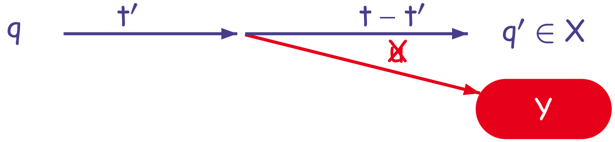
$$\pi_\delta(X) = Pred_\delta\left(cPred(X), uPred(\overline{X})\right)$$

$\pi_\delta(X)$ is effectively computable for state predicate X.

Symbolic Computation For Timed Games

X is a state predicate

- $cPred(X) = \bigcup_{c \in Act_c} Pred^c(X)$ $uPred(X) = \bigcup_{u \in Act_u} Pred^u(X)$
  cPred and uPred are effectively computable
- $Pred_\delta(X, Y)$: Time controllable predecessors of X avoiding Y:



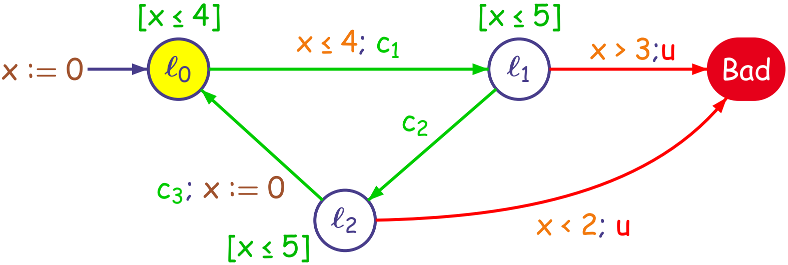
$Pred_\delta(X, Y)$ is effectively computable for state predicates X, Y

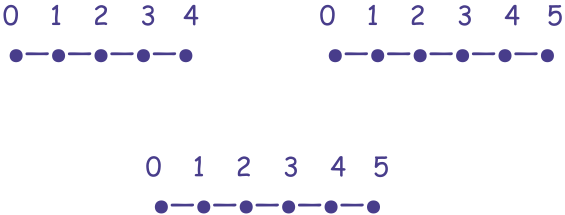
- Controllable Predecessors Operator for Timed Games

$$\pi_\delta(X) = Pred_\delta\left(cPred(X), uPred(\overline{X})\right)$$

$\pi_\delta(X)$ is effectively computable for state predicate X.

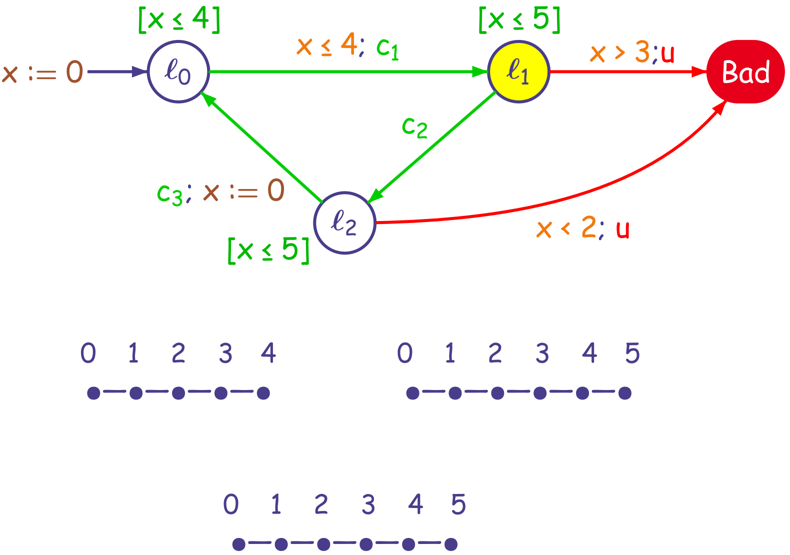
Example of Computation for Safety Games



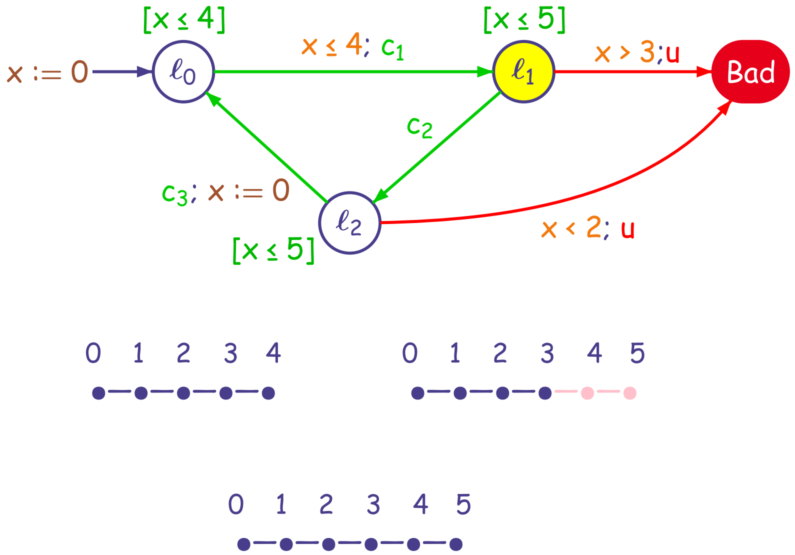


Skip

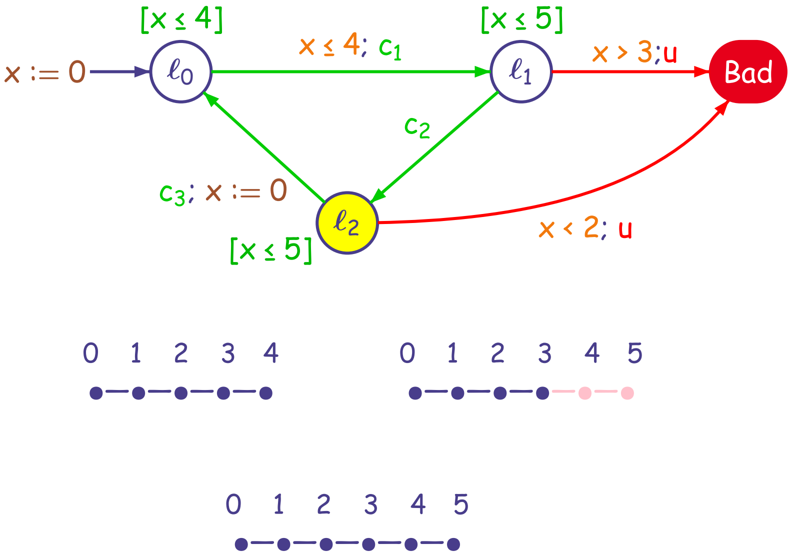
Example of Computation for Safety Games



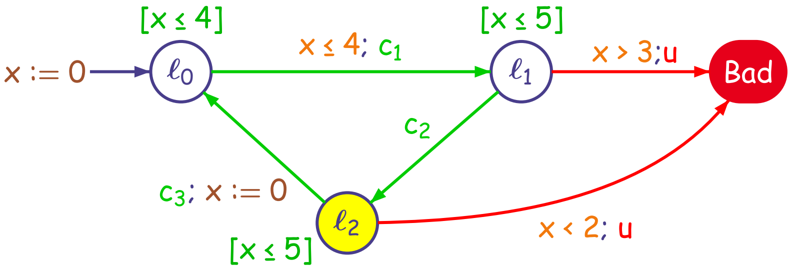
Example of Computation for Safety Games

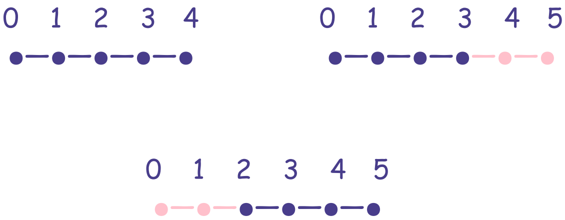


Example of Computation for Safety Games

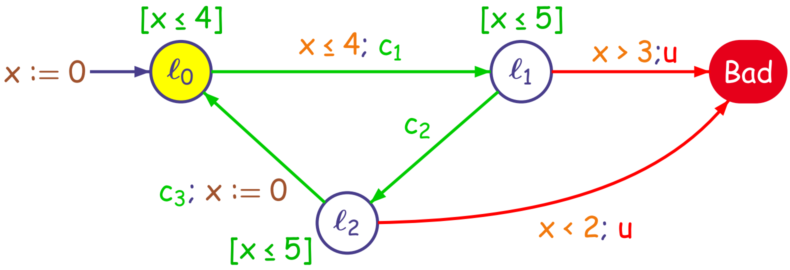


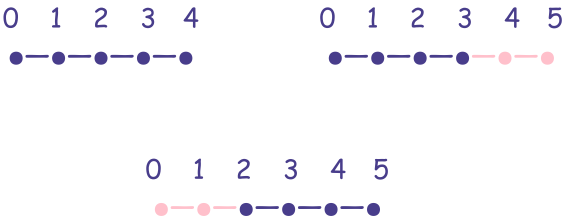
Example of Computation for Safety Games



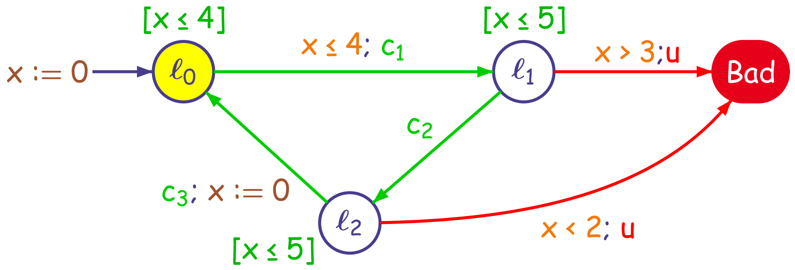


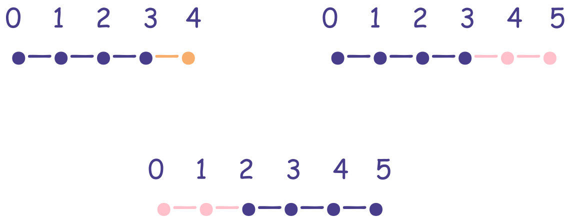
Example of Computation for Safety Games



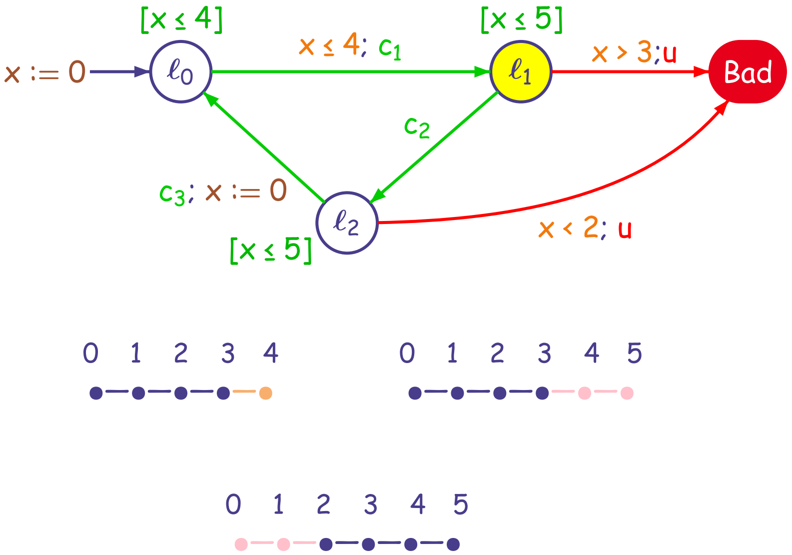


Example of Computation for Safety Games

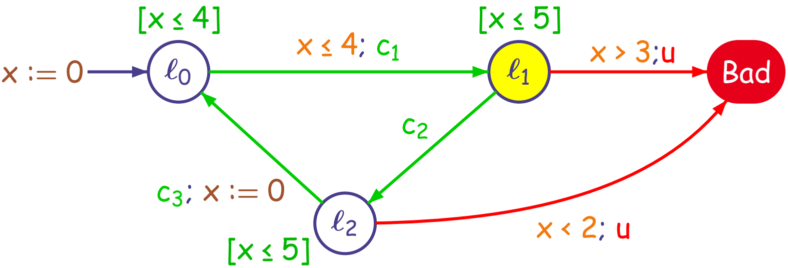


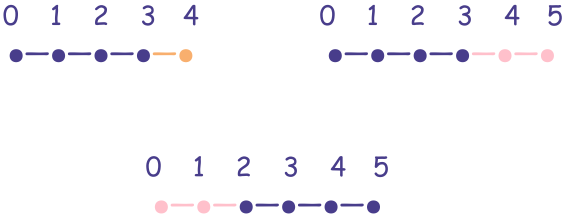


Example of Computation for Safety Games

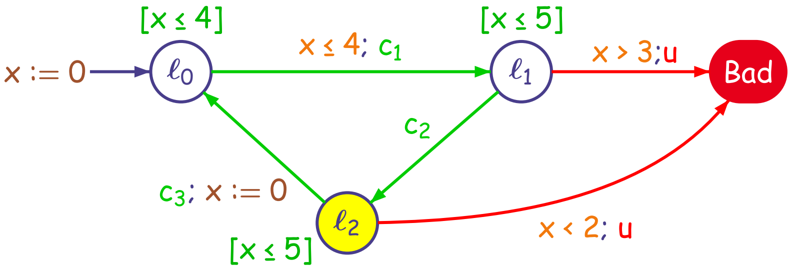


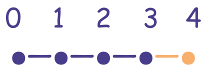
Example of Computation for Safety Games

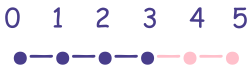


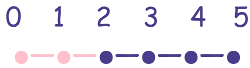


Example of Computation for Safety Games

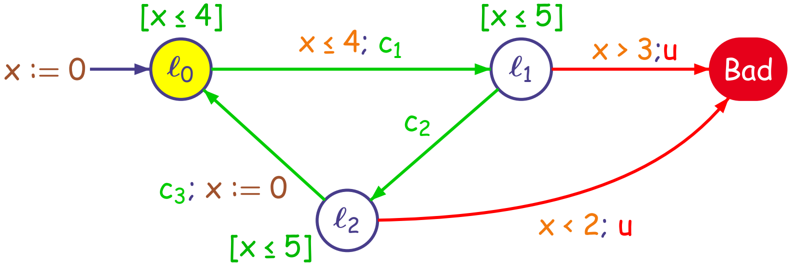


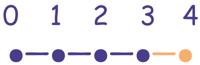


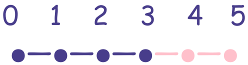


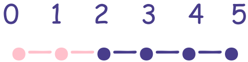


Example of Computation for Safety Games

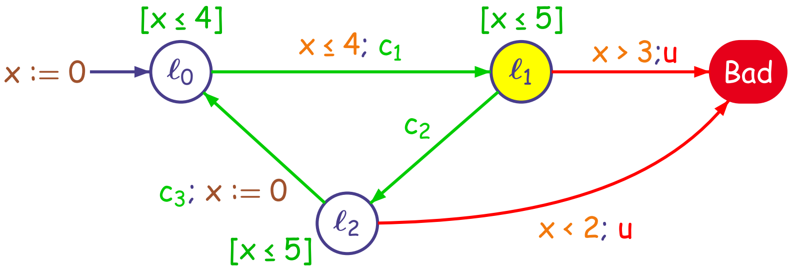


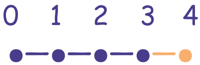


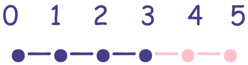


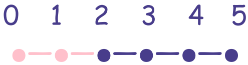


Example of Computation for Safety Games

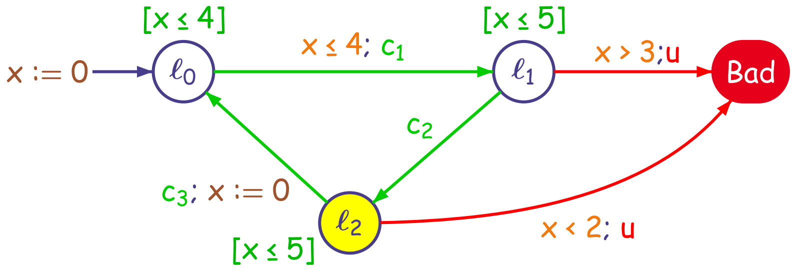


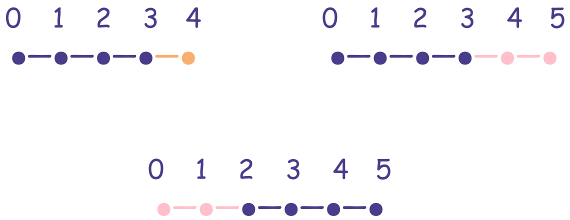




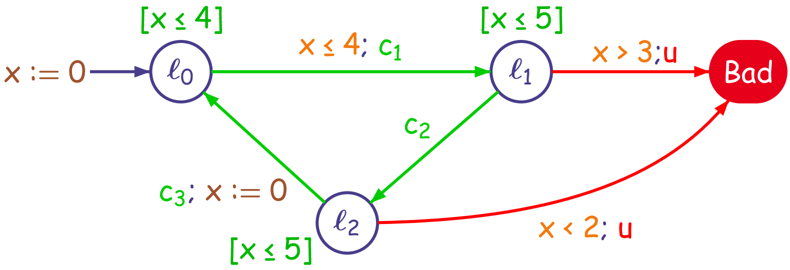


Example of Computation for Safety Games





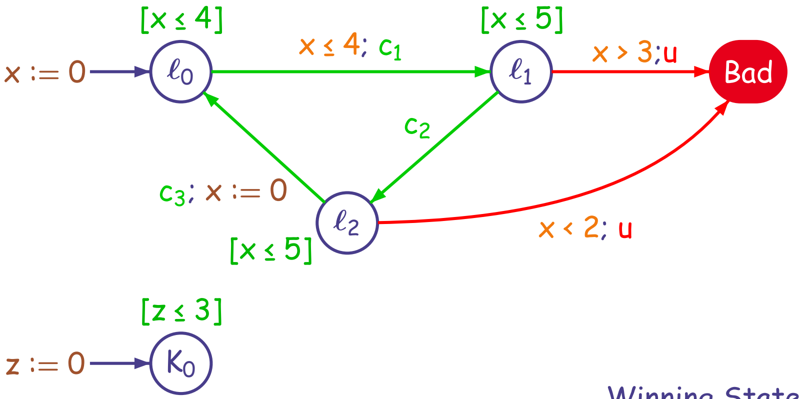
Example of Computation for Safety Games



Winning States

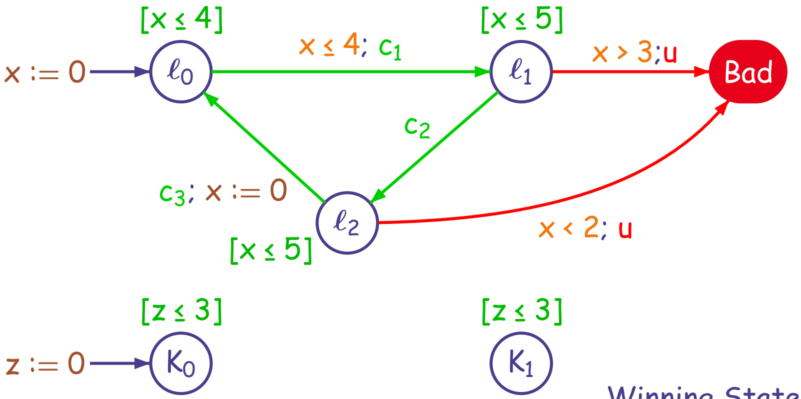
$(\ell_0, 0 \leq x \leq 3)$
$(\ell_1, 0 \leq x \leq 3)$
$(\ell_2, 2 \leq x \leq 5)$

Example of Computation for Safety Games



Winning States

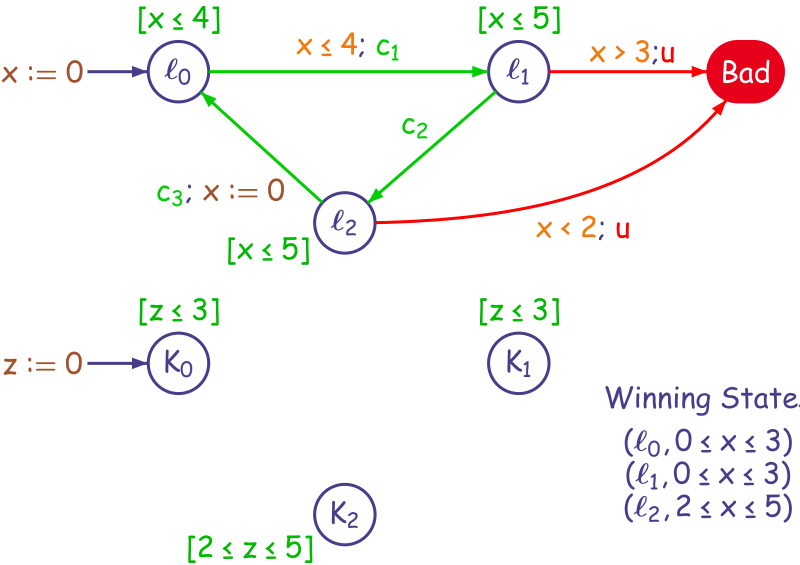
$(\ell_0, 0 \leq x \leq 3)$
$(\ell_1, 0 \leq x \leq 3)$
$(\ell_2, 2 \leq x \leq 5)$



Winning States

$(\ell_0, 0 \le x \le 3)$
$(\ell_1, 0 \le x \le 3)$
$(\ell_2, 2 \le x \le 5)$

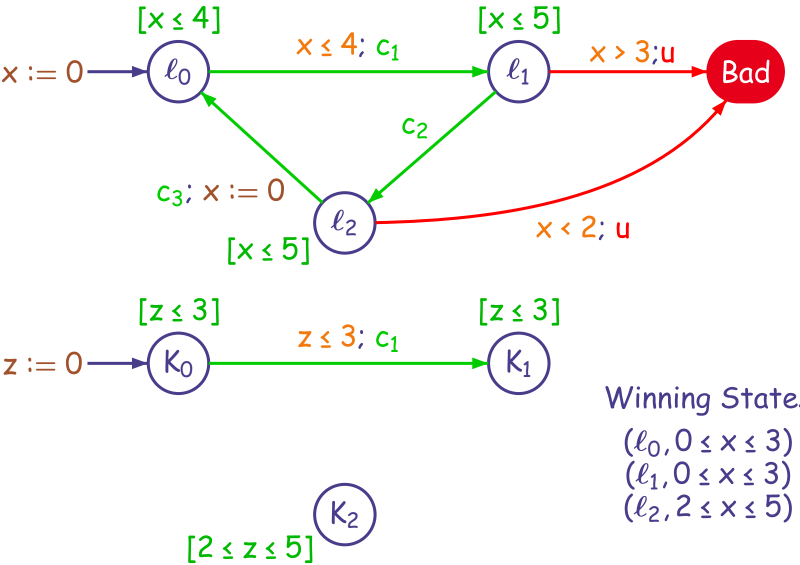
Example of Computation for Safety Games



Winning States

$(\ell_0, 0 \leq x \leq 3)$
$(\ell_1, 0 \leq x \leq 3)$
$(\ell_2, 2 \leq x \leq 5)$

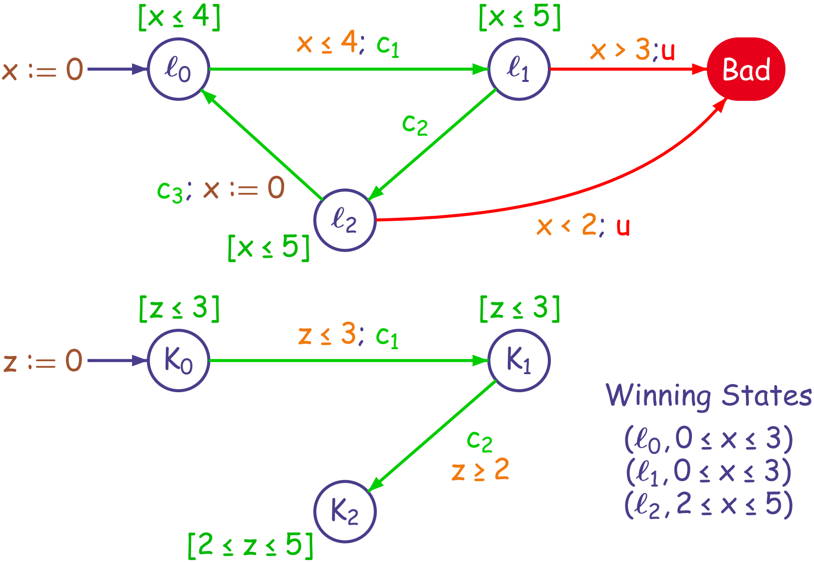
Example of Computation for Safety Games



Winning States

$(\ell_0, 0 \leq x \leq 3)$
$(\ell_1, 0 \leq x \leq 3)$
$(\ell_2, 2 \leq x \leq 5)$

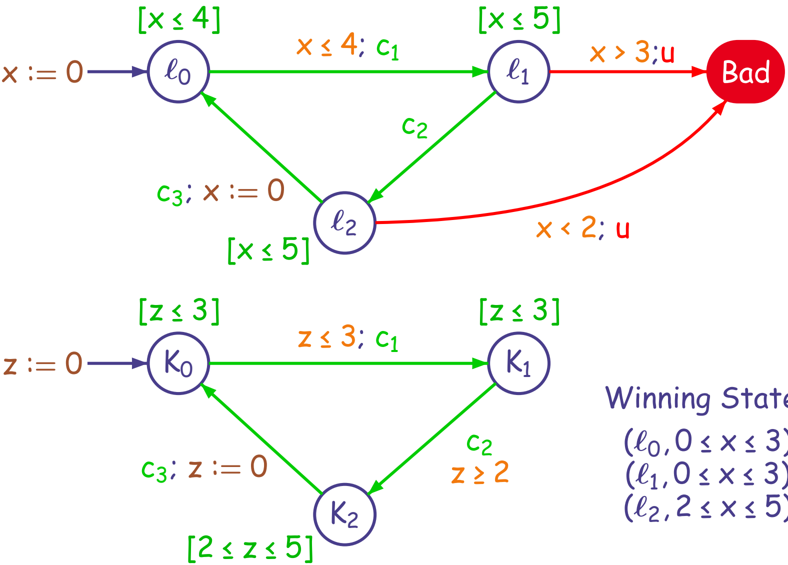
Example of Computation for Safety Games



Winning States

$(\ell_0, 0 \leq x \leq 3)$
$(\ell_1, 0 \leq x \leq 3)$
$(\ell_2, 2 \leq x \leq 5)$

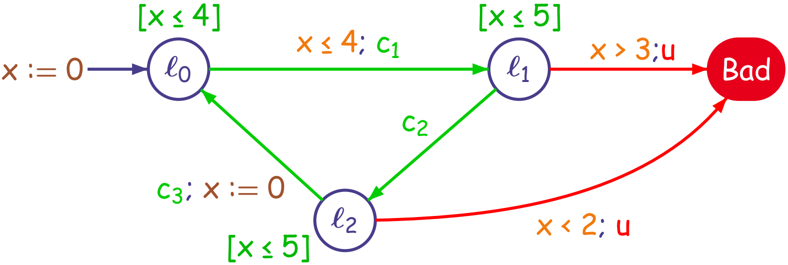
Example of Computation for Safety Games

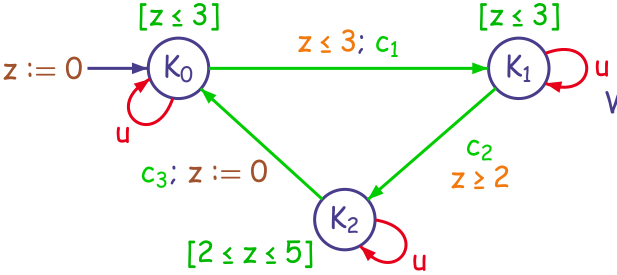


Winning States

$(\ell_0, 0 \le x \le 3)$
$(\ell_1, 0 \le x \le 3)$
$(\ell_2, 2 \le x \le 5)$

Example of Computation for Safety Games

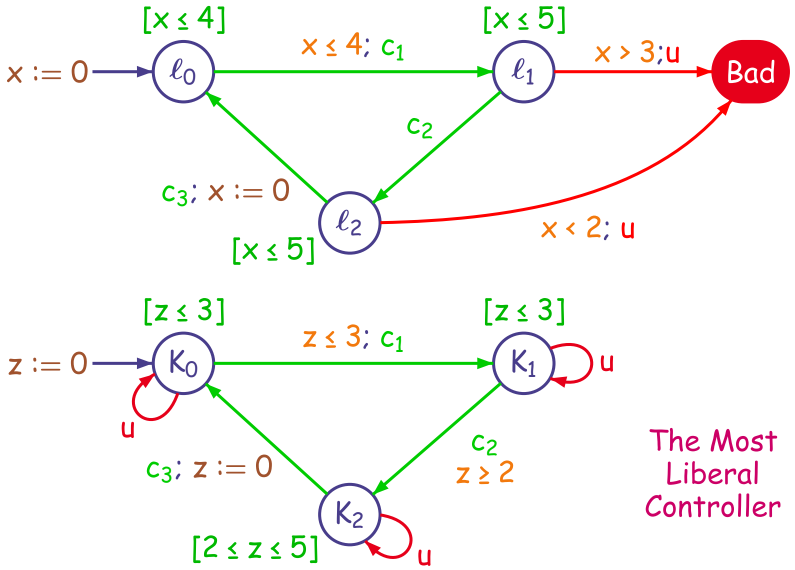




Winning States

$(\ell_0, 0 \leq x \leq 3)$
$(\ell_1, 0 \leq x \leq 3)$
$(\ell_2, 2 \leq x \leq 5)$

Example of Computation for Safety Games



The Most Liberal Controller

Existence of Cost Independent Strategies

Let A be a RPTGA such that:

- guards of u actions are strict
- guards on c actions are large

There is an optimal cost independent strategy

Is it necessary ?

Existence of Cost Independent Strategies

Let A be a RPTGA such that:

- guards of u actions are strict
- guards on c actions are large

There is an optimal cost independent strategy

Is it necessary ?

Existence of Cost Independent Strategies

Let A be a RPTGA such that:

- guards of u actions are strict
- guards on c actions are large

There is an optimal cost independent strategy

Is it necessary ?

Existence of Cost Independent Strategies

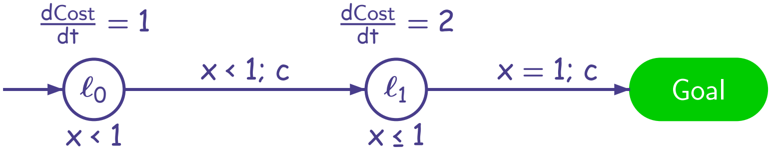
Let A be a RPTGA such that:

- guards of u actions are strict
- guards on c actions are large

There is an optimal cost independent strategy

Is it necessary ?

No Optimal Strategy

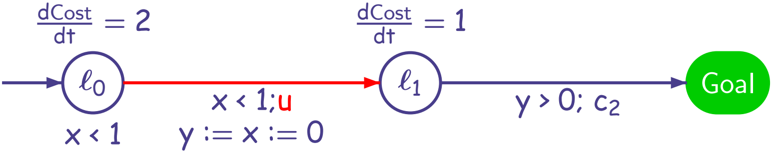


- define f_ε with $0 < \varepsilon < 1$ by:
  in ℓ_0: $f(\ell_0, x < 1 - \varepsilon) = \lambda$, $f(\ell_0, 1 - \varepsilon \leq x < 1) = c$
  in ℓ_1: $f(\ell_1, x < 1) = \lambda$, $f(\ell_1, x = 1) = c$
  $Cost(f_\varepsilon) = (1 - \varepsilon) + 2.\varepsilon = 1 + \varepsilon$ and $OptCost = 1$.
- given $\varepsilon > 0$, there is a sub-optimal strategy f_ε such that

$$|Cost((\ell_0, \vec{0}), f_\varepsilon) - OptCost((\ell_0, \vec{0}), G)| < \varepsilon$$

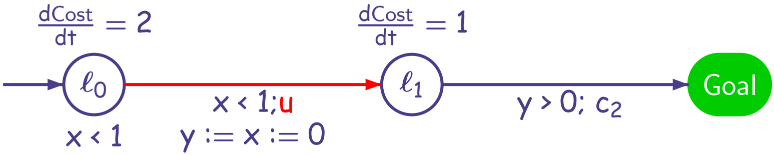
- New problem: given ε, compute such an f_ε strategy.

No Optimal Cost-Independent Strategy



- Optimal cost is 2

No Optimal Cost-Independent Strategy

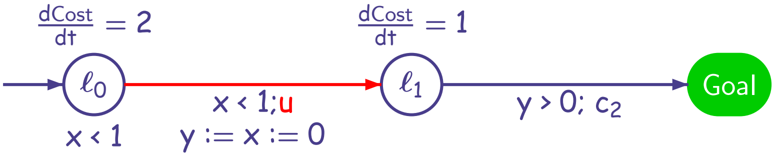


- Optimal cost is 2
- An optimal winning cost-dependent strategy f: $f(\ell_1, -, cost < 2) = \lambda$ and $f(\ell_1, -, cost = 2) = c_2$ assume u taken at time $(1 - \delta_0)$:

$$Cost(f, (\ell_0, 0)) = 2 \cdot (1 - \delta_0) + \delta_1 = 2$$

because according to f we have $\delta_1 = 2 \cdot \delta_0$

No Optimal Cost-Independent Strategy



- Optimal cost is 2
- assume $\exists f^*$ cost-independent: f^* must wait in ℓ_1 at least ε
  assume u taken at time $(1 - \delta)$:

$$\text{Cost}(f^*, (\ell_0, 0)) = 2 \cdot (1 - \delta) + \varepsilon$$

Take $\delta = \frac{\varepsilon}{4}$: $\text{Cost}(f^*, (\ell_0, 0)) = 2 + \frac{\varepsilon}{2}$ and $\text{OptCost}(f^*) = 2 + \varepsilon$

Related Work for Optimal Control

- [La Torre et al.'02]
  - Acyclic Priced Timed Game Automata
  - Recursive definition of optimal cost
  - Computation of the infimum of the optimal cost
    i.e. OptCost = 2 could mean that it is 2 or $2 + \varepsilon$
  - No strategy synthesis
- [Alur et al.'04] (ICALP'04)
  - Bounded optimality: optimal cost within k steps
  - Complexity bound: exponential in k and #states of the PTGA
  - No bound for the more general optimal problem
  - Computation of the infimum of the optimal cost
  - No strategy synthesis
- Our work [FSTTCS'04]:
  - Run-based definition of optimal cost
  - We can decide whether ∃ an optimal strategy
  - We can effectively synthesize an optimal strategy (if one exists)
  - We can prove structural properties of optimal strategies
  - Applies to Linear Hybrid Game (Automata)

Related Work for Optimal Control

- [La Torre et al.'02] Acyclic Games, infimum, no strategy synthesis
- [Alur et al.'04] (ICALP'04)
  - Bounded optimality: optimal cost within k steps
  - Complexity bound: exponential in k and #states of the PTGA
  - No bound for the more general optimal problem
  - Computation of the infimum of the optimal cost
  - No strategy synthesis
- Our work [FSTTCS'04]:
  - Run-based definition of optimal cost
  - We can decide whether ∃ an optimal strategy
  - We can effectively synthesize an optimal strategy (if one exists)
  - We can prove structural properties of optimal strategies
  - Applies to Linear Hybrid Game (Automata)

Related Work for Optimal Control

- [La Torre et al.'02] Acyclic Games, infimum, no strategy synthesis
- [Alur et al.'04] (ICALP'04)
  - Bounded optimality: optimal cost within k steps
  - Complexity bound: exponential in k and #states of the PTGA
  - No bound for the more general optimal problem
  - Computation of the infimum of the optimal cost
  - No strategy synthesis

  Bounded optimality, complexity bound, infimum, no strategy synthesis
- Our work [FSTTCS'04]:
  - Run-based definition of optimal cost
  - We can decide whether ∃ an optimal strategy
  - We can effectively synthesize an optimal strategy (if one exists)
  - We can prove structural properties of optimal strategies
  - Applies to Linear Hybrid Game (Automata)

Related Work for Optimal Control

- [La Torre et al.'02] Acyclic Games, infimum, no strategy synthesis
- [Alur et al.'04] (ICALP'04)
  - Bounded optimality: optimal cost within k steps
  - Complexity bound: exponential in k and #states of the PTGA
  - No bound for the more general optimal problem
  - Computation of the infimum of the optimal cost
  - No strategy synthesis

  Bounded optimality, complexity bound, infimum, no strategy synthesis
- Our work [FSTTCS'04]:
  - Run-based definition of optimal cost
  - We can decide whether ∃ an optimal strategy
  - We can effectively synthesize an optimal strategy (if one exists)
  - We can prove structural properties of optimal strategies
  - Applies to Linear Hybrid Game (Automata)