-MOVEP 2012-

Implementation of Timed Systems: Theory and Practice

Aleksandra Jovanović, Didier Lime, Olivier H. Roux
IRCCyN, Ecole Centrale de Nantes

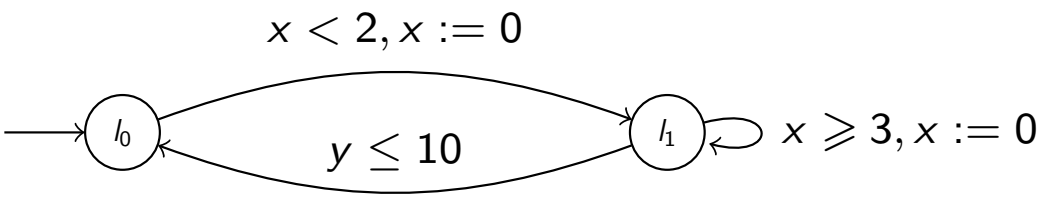
December 4, 2012

Outline

Parametric Approach in Automata Theory

Timed Automaton (TA)

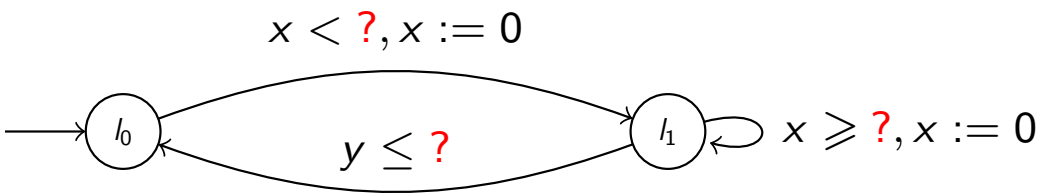
- Finite automaton extended with a finite set of clocks



Parametric Approach in Automata Theory

Timed Automaton (TA)

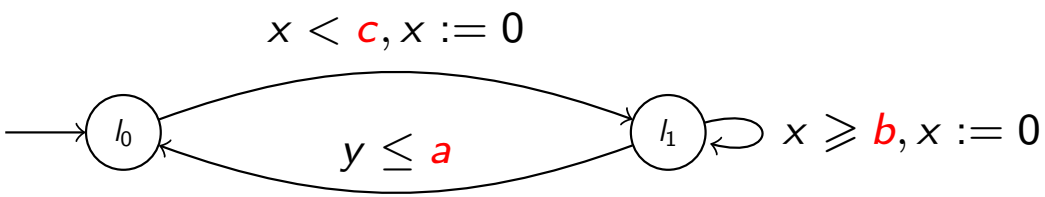
- Finite automaton extended with a finite set of clocks



Parametric Approach in Automata Theory

Timed Automaton (TA)

- Finite automaton extended with a finite set of clocks

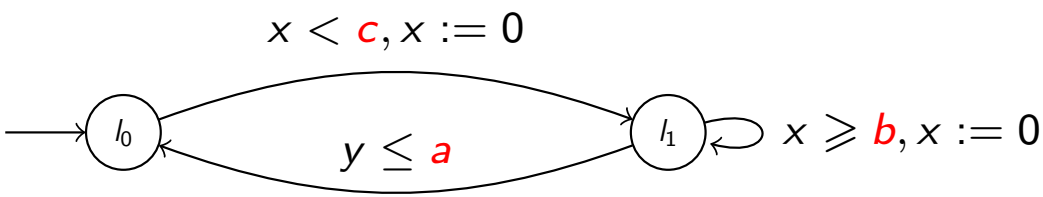


Parametric Timed Automaton (PTA)

Parametric Approach in Automata Theory

Timed Automaton (TA)

- Finite automaton extended with a finite set of clocks



Parametric Timed Automaton (PTA)

- Timed automata with parameters as bounds on clocks

Challenges of the Parametric Approach

Parametric verification

Challenges of the Parametric Approach

Parametric verification

Reachability emptiness for PTA

Is the set of parameter valuations v, such that l_i is reachable in $v(\mathcal{A})$, empty?

Challenges of the Parametric Approach

Parametric verification

Reachability emptiness for PTA

Is the set of parameter valuations v, such that l_i is reachable in $v(\mathcal{A})$, empty?

Unavoidability emptiness for PTA

Is the set of parameter valuations v, such that all maximal runs of $v(\mathcal{A})$ go through l_i, empty?

Challenges of the Parametric Approach

Parametric verification

Reachability emptiness for PTA

Is the set of parameter valuations v, such that l_i is reachable in $v(\mathcal{A})$, empty?

Unavoidability emptiness for PTA

Is the set of parameter valuations v, such that all maximal runs of $v(\mathcal{A})$ go through l_i, empty?

Synthesis problem

Can we compute all of these valuations?

Outline

Undecidability Results

Theorem — Alur & Dill '93

Reachability emptiness problem is undecidable for PTA.

Undecidability Results

Theorem — Alur & Dill '93

Reachability emptiness problem is undecidable for PTA.

We restrict the problem to *bounded parameters*:

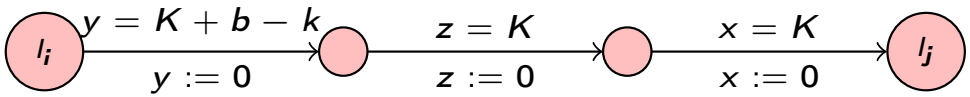
Undecidability Results

Theorem — Alur & Dill '93

Reachability emptiness problem is undecidable for PTA.

We restrict the problem to *bounded parameters*:

- New encoding of the 2-counter machine with parameters bounded by K and k:



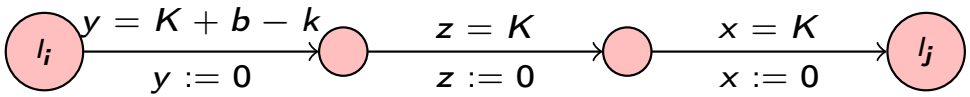
Undecidability Results

Theorem — Alur & Dill '93

Reachability emptiness problem is undecidable for PTA.

We restrict the problem to *bounded parameters*:

- New encoding of the 2-counter machine with parameters bounded by K and k:



Theorem

Reachability emptiness problem with bounded parameters is undecidable for PTA.

Undecidability Results *cont.*

Subclass of PTA: L/U automaton [Hune & al. '02]:

- Two sets of parameters: lower bounds on clocks ($x \geq a$) upper bounds on clocks ($x \leq b$)
- Reachability emptiness is decidable for L/U automata

Undecidability Results *cont.*

Subclass of PTA: L/U automaton [Hune & al. '02]:

- Two sets of parameters: lower bounds on clocks ($x \geq a$) upper bounds on clocks ($x \leq b$)
- Reachability emptiness is decidable for L/U automata

But:

Undecidability Results *cont.*

Subclass of PTA: L/U automaton [Hune & al. '02]:

- Two sets of parameters: lower bounds on clocks ($x \geq a$) upper bounds on clocks ($x \leq b$)
- Reachability emptiness is decidable for L/U automata

But:

- transform a PTA into a L/U automaton
- we obtain: $v_p \Leftrightarrow v_{L/U} \cap \{p_i^l = p_i^u\} \stackrel{?}{=} \{\emptyset\} \implies$ undecidable

Undecidability Results *cont.*

Subclass of PTA: L/U automaton [Hune & al. '02]:

- Two sets of parameters: lower bounds on clocks ($x \geq a$) upper bounds on clocks ($x \leq b$)
- Reachability emptiness is decidable for L/U automata

But:

- transform a PTA into a L/U automaton
- we obtain: $v_p \Leftrightarrow v_{L/U} \cap \{p_i^l = p_i^u\} \stackrel{?}{=} \{\emptyset\} \implies$ undecidable

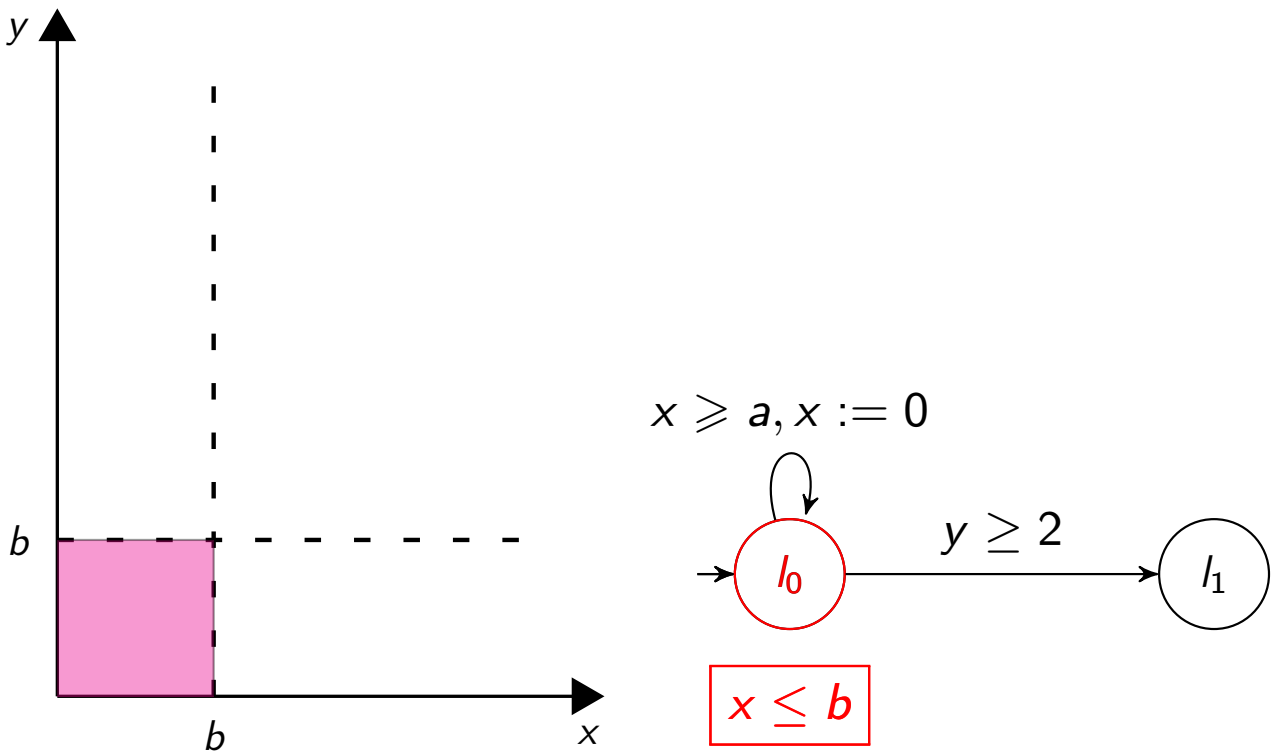
Theorem

The solution to the reachability emptiness problem for L/U automata cannot be represented using any formalism for which the emptiness of the intersection with equality constraints is decidable.

Motivating example

Forward state-space exploration of PTA

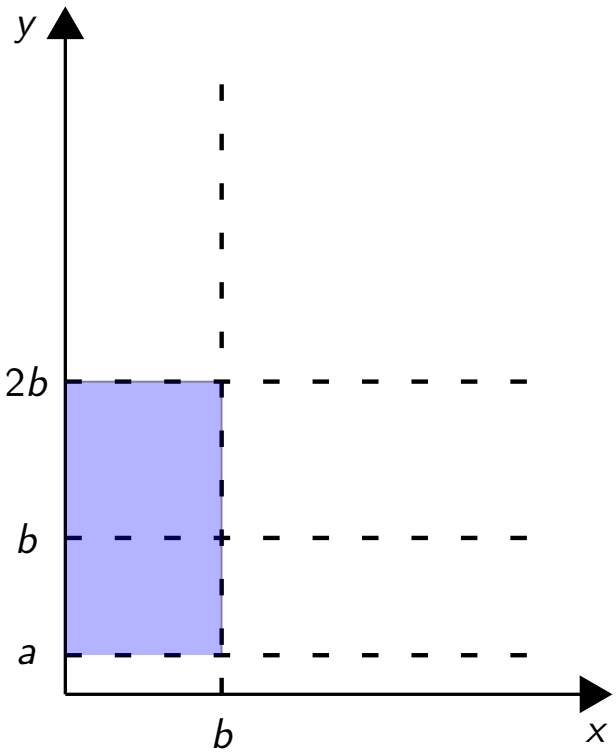
- Condition for termination: $Z_{n+1} \subseteq Z_n$

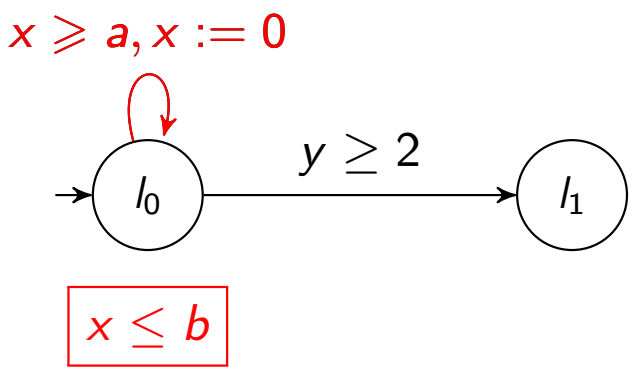


Motivating example

Forward state-space exploration of PTA

- Condition for termination: $Z_{n+1} \subseteq Z_n$

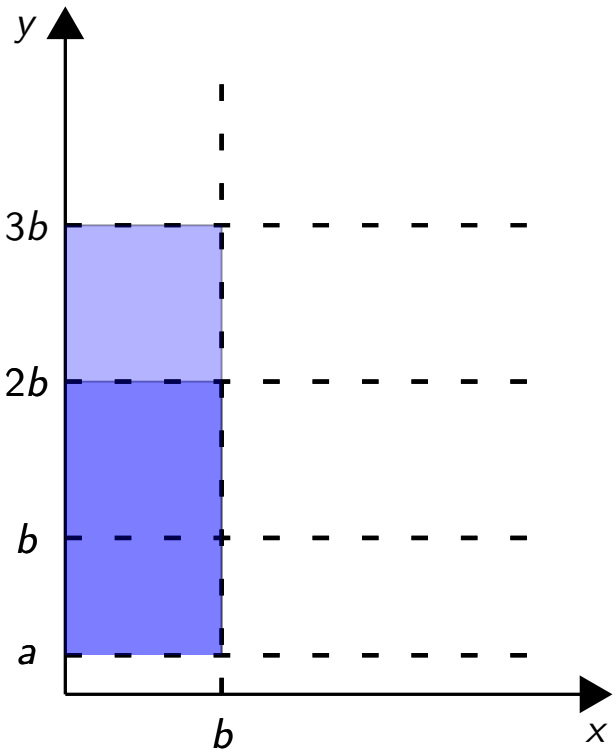


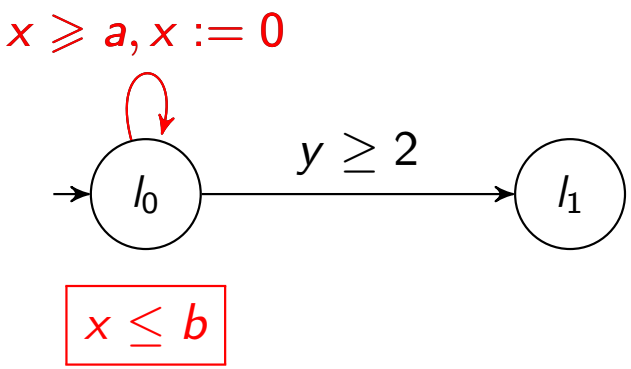


Motivating example

Forward state-space exploration of PTA

- Condition for termination: $Z_{n+1} \subseteq Z_n$

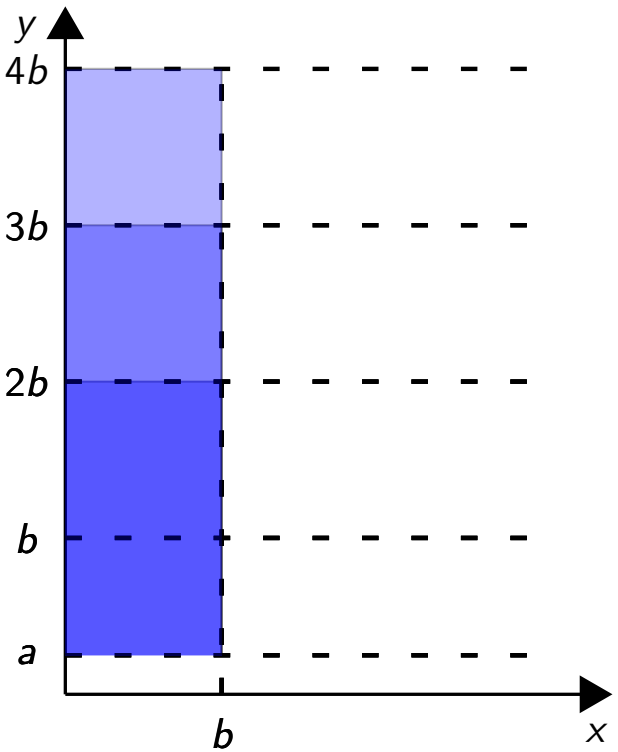


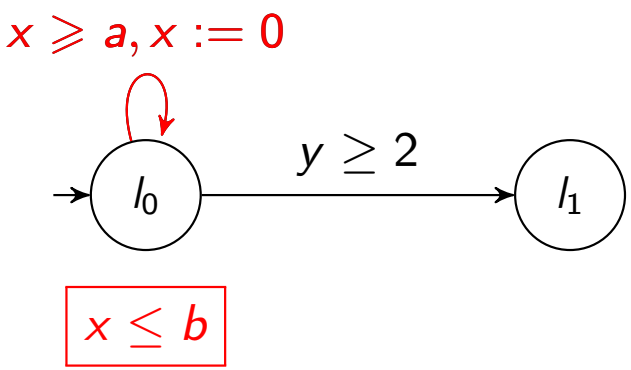


Motivating example

Forward state-space exploration of PTA

- Condition for termination: $Z_{n+1} \subseteq Z_n$

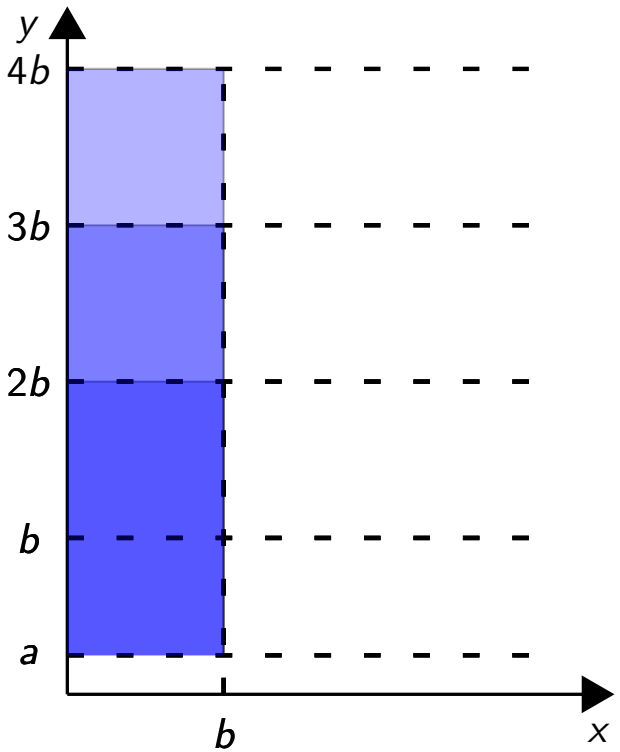


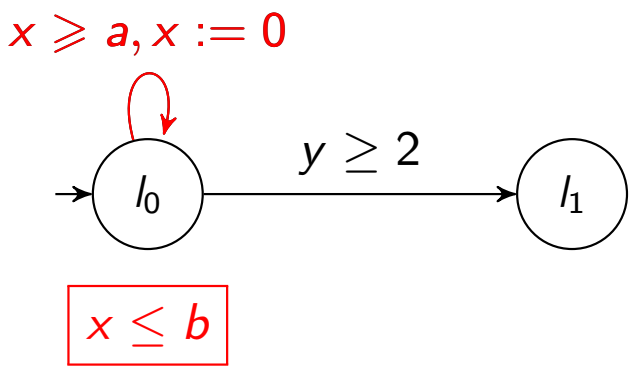


Motivating example

Forward state-space exploration of PTA

- Condition for termination: $Z_{n+1} \subseteq Z_n$





- $Z_n = \{0 \leq x \leq b, 0 \leq na \leq y \leq (n+1)b\}$

Outline

Integer Parameter Synthesis for PTA

Current problem:

- undecidability

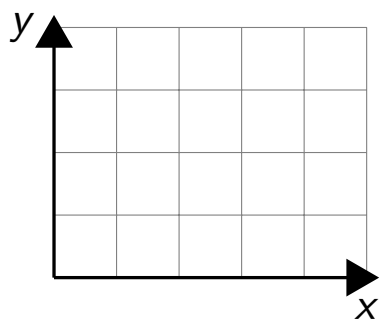
Integer Parameter Synthesis for PTA

Current problem:

- undecidability

Proposed solution:

- computation of integer parameter valuations
- symbolic approach: integer hulls



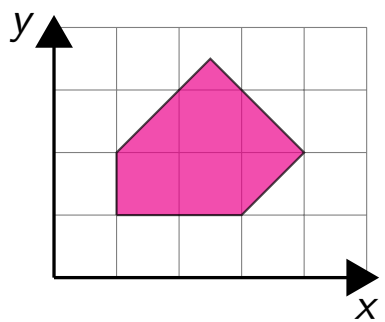
Integer Parameter Synthesis for PTA

Current problem:

- undecidability

Proposed solution:

- computation of integer parameter valuations
- symbolic approach: integer hulls



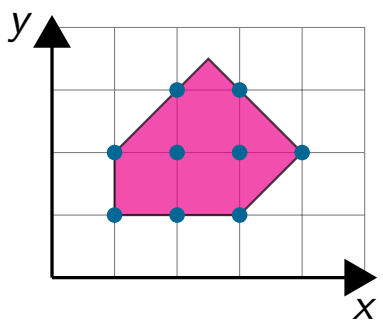
Integer Parameter Synthesis for PTA

Current problem:

- undecidability

Proposed solution:

- computation of integer parameter valuations
- symbolic approach: integer hulls



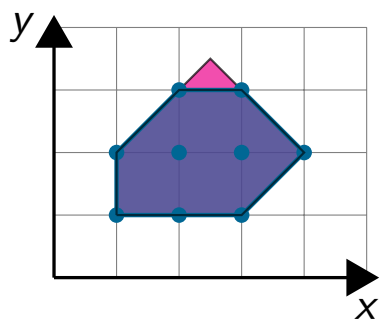
Integer Parameter Synthesis for PTA

Current problem:

- undecidability

Proposed solution:

- computation of integer parameter valuations
- symbolic approach: integer hulls



IntHull(Z): smallest subset of elements of Z with *integer coordinates*

Termination

Problem: termination of the algorithm

Termination

Problem: termination of the algorithm

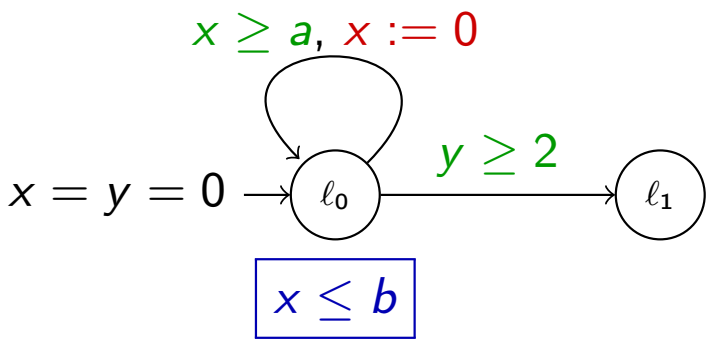
Proposed solution: bound the parameter valuations

Termination

Problem: termination of the algorithm

Proposed solution: bound the parameter valuations

- Clocks are *upper bounded* by N



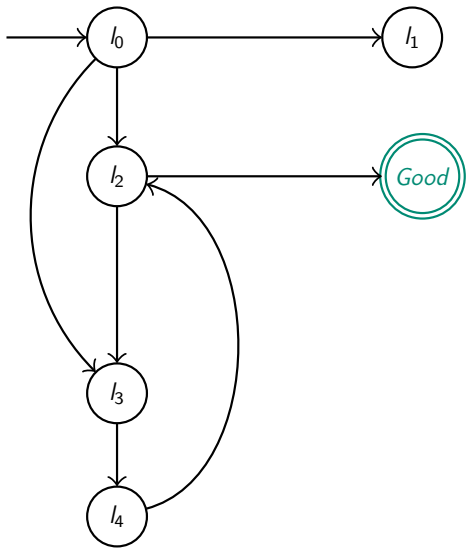
- Suppose $N = 3$ and (ℓ_0, Z_0) with $Z_0 = \{x = y, x \leq b \leq 3\}$;
- After one loop: $Z_1' = Z_1 \cap \{y \leq b + 1\}$;
- After two loops: $Z_2' = Z_2 \cap \{a \leq 1 \text{ and } a \leq b\}$
- After $n > 3$ loops:

$$Z_n' = Z_{n+1}' = \{a = 0, 0 \leq x \leq b, x \leq 3, 0 \leq y \leq 3b, y \leq 3\}$$

Outline

Parametric Timed Game Automata

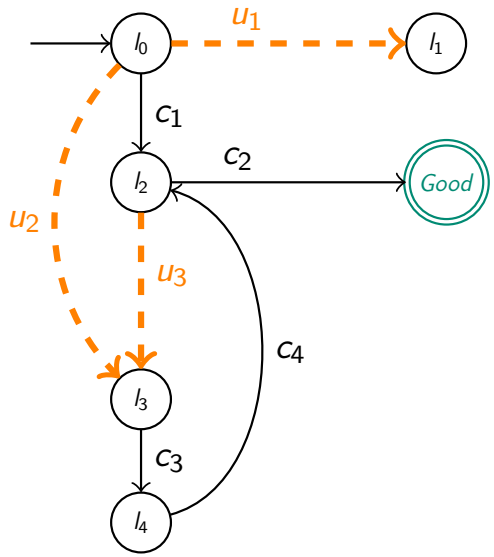
Control problems on TA:



Parametric Timed Game Automata

Control problems on TA:

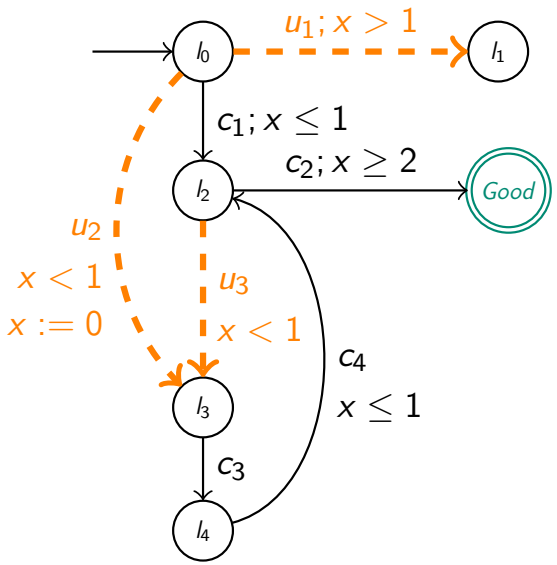
- *uncontrollable* events



Parametric Timed Game Automata

Control problems on TA:

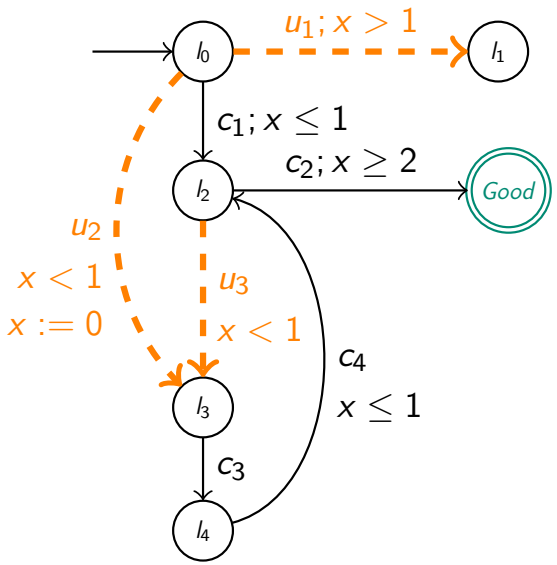
- *uncontrollable* events
- timed game: controller vs. environment



Parametric Timed Game Automata

Control problems on TA:

- *uncontrollable* events
- timed game: controller vs. environment
- find a *winning strategy*

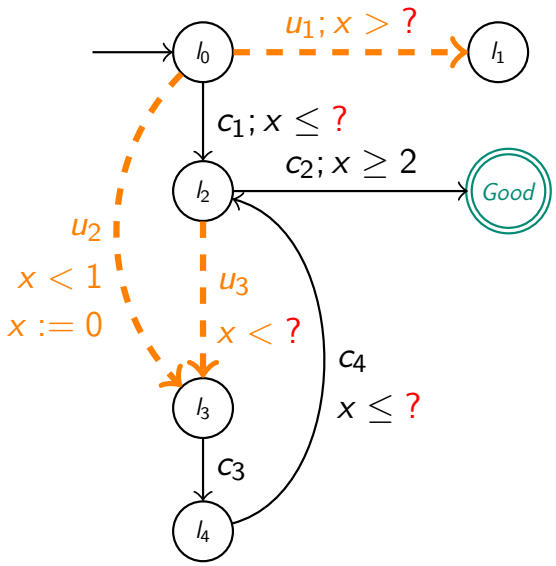


Parametric Timed Game Automata

Control problems on TA:

- *uncontrollable* events
- timed game: controller vs. environment
- find a *winning strategy*

Extension with parameters:



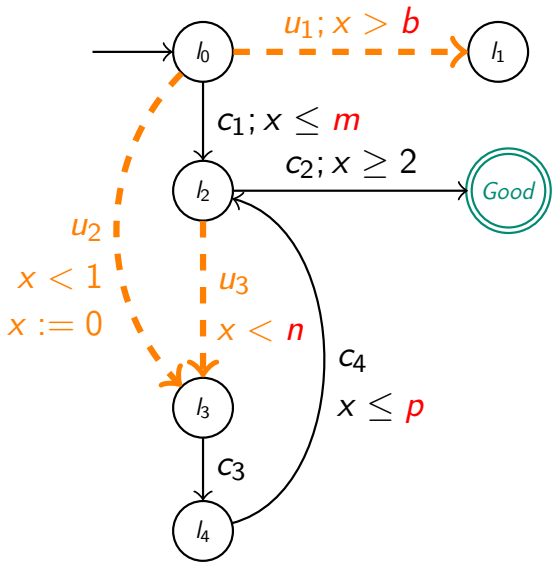
Parametric Timed Game Automata

Control problems on TA:

- *uncontrollable* events
- timed game: controller vs. environment
- find a *winning strategy*

Extension with parameters:

- Parametric game automata (PGA)



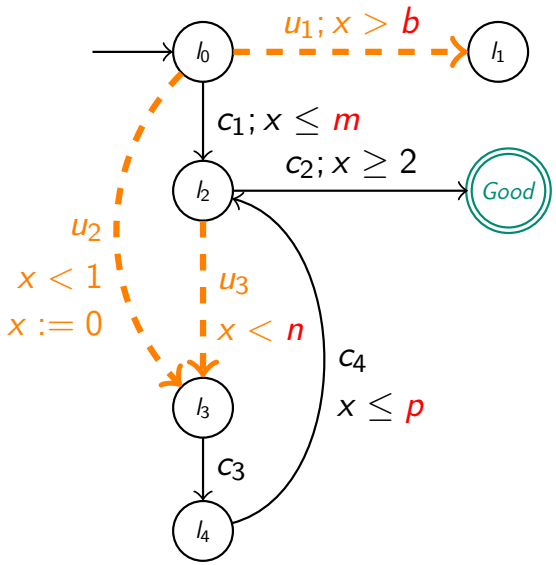
Parametric Timed Game Automata

Control problems on TA:

- *uncontrollable* events
- timed game: controller vs. environment
- find a *winning strategy*

Extension with parameters:

- Parametric game automata (PGA)



Reachability emptiness problem for PGA

Is there a parameter valuation v such that there is a winning strategy?

Decidability Issues for PGA

Theorem

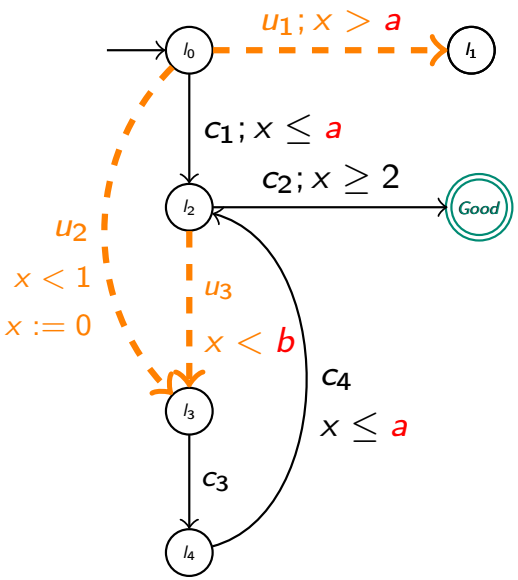
Reachability emptiness problem for PGA is undecidable.

Decidability Issues for PGA

Theorem

Reachability emptiness problem for PGA is undecidable.

New subclass of PGA: L/U game automata



Syntactical restrictions:

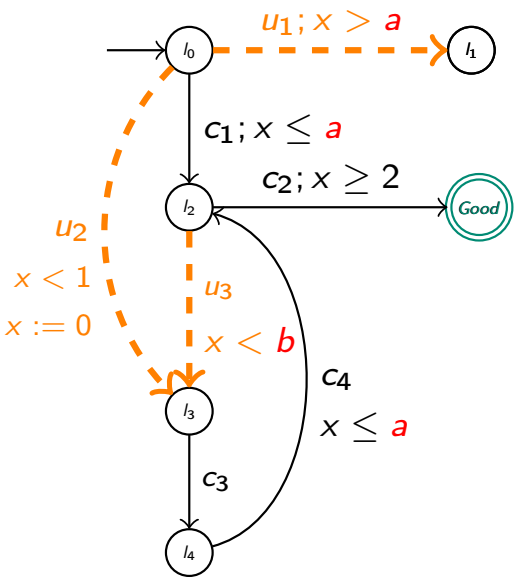
- the set of parameters P is partitioned as:
- P^l - lower bounds in controllable trans. and upper bounds in uncontrollable trans.
- P^u - upper bounds in controllable trans. and lower bounds in uncontrollable trans.

Decidability Issues for PGA

Theorem

Reachability emptiness problem for PGA is undecidable.

New subclass of PGA: L/U game automata



Syntactical restrictions:

- the set of parameters P is partitioned as:
- P^l - lower bounds in controllable trans. and upper bounds in uncontrollable trans.
- P^u - upper bounds in controllable trans. and lower bounds in uncontrollable trans.

Theorem

Reachability emptiness problem for L/U games is decidable.

Algorithm for Solving Parametric Timed Games

Symbolic on-the-fly algorithm for solving TGA [Cassez & al. '05]

- winning set of states

Extend the algorithm for the parametric approach

- set of parameter valuations with the set of winning states

We use extended notion of the symbolic state:

- parametric zone - set of pairs (w, v) satisfying clock constraint
- w - clock valuation
- v - parameter valuation

Theorem

In the case of termination, if the initial state belongs to the winning set of states, set of parameter valuations is obtained and the winning strategy can be extracted from the winning set of states.

Outline

Conclusions

Parameter synthesis for PTA:

- Integer parameter synthesis for PTA - decidability
- Bounded integers - termination
- Integer hulls - efficiency

Conclusions

Parameter synthesis for PTA:

- Integer parameter synthesis for PTA - decidability
- Bounded integers - termination
- Integer hulls - efficiency

Parametric model for timed games:

- Timed games with parameters
  - parametric timed games
- Reachability emptiness decidable subclass
  - L/U game automata
- Extension of the algorithm for solving timed games
  - parameter synthesis