Imperfection is better!

1-clock priced TA with imprecisions on energy level

Nicolas Markey[1] Pierre-Alain Reynier[2]

[1] LSV – CNRS & ENS Cachan

[2] LIF – CNRS & Univ. Aix-Marseille

2nd GASICS Workshop
Paris, September 2010

Outline of the presentation

1. Introduction
2. 1-clock PTA with imperfect energy level
3. Where Presburger arithmetic helps us
4. Robust strategies
5. A case study
6. Conclusion

Outline of the presentation

Time is necessary

we need a quantitative notion of time for modelization:

- the behaviour of most systems actually depends on time,
- modelling has to take it into account

➜ Timed Automata, Timed Petri nets...

and also for specifications:

- to faithfully represent the specification,
- untimed specifications are not enough (e.g. bounded response time property)

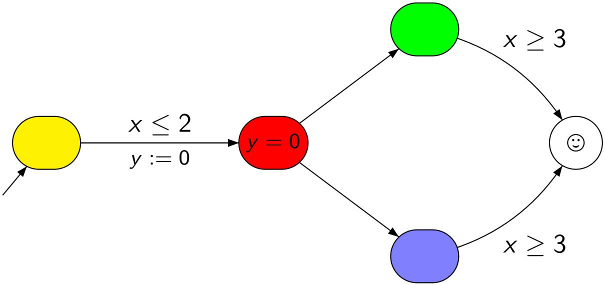
➜ TCTL, MTL, TPTL, timed μ-calculus...

But time may not be sufficient

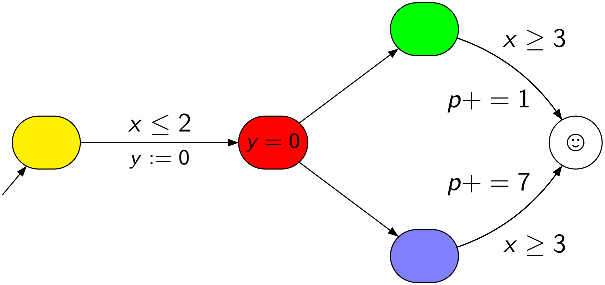
In some cases we don't want to measure time, but rather energy consumption to achieve some goal.

- stopwatch automata: allows to stop/start some clocks,
  ➜ useful for scheduling
- hybrid automata: allows variables whose derivative is not constant,
  ➜ leaking gas burner, water-level monitor...
- priced (=weighted) timed automata: similar to linear hybrid automata, but the behaviour only depends on clock variables

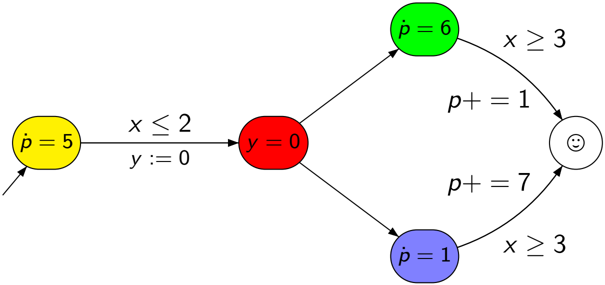
Priced timed automata [ALP01, BFH+01]



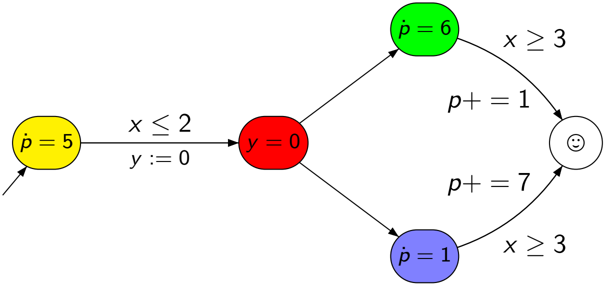
Priced timed automata [ALP01, BFH+01]



Priced timed automata [ALP01, BFH+01]



Priced timed automata [ALP01, BFH+01]

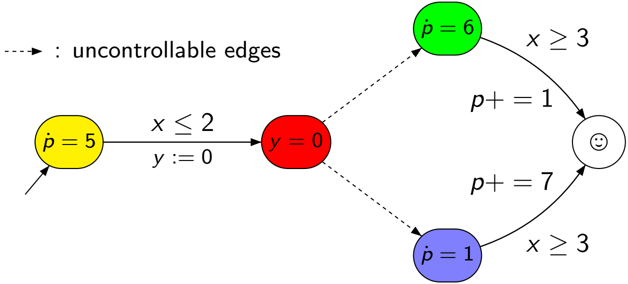


Main known results:

- Optimal infinite behaviours are computable (in PSPACE) minimal cost for reaching ☺
- Model Checking logic WCTL: $\mathrm{EF}_{p\leq 10}$☺, $\mathrm{AG}_{t=2}(\mathrm{EF}_{p\leq 6}$☺$)$
  - decidable over PTAs with ≤ 1 clocks (in PSPACE)
  - undecidable over PTAs with ≥ 3 clocks

Note: Prices and price rates are non-negative

Priced timed games



Main known results:

- Computing (almost) optimal strategies for 1-clock turn-based PTGs is decidable
- It is undecidable for PTGs with ≥ 3 clocks

Note: Again, prices and price rates are non-negative

Energy Constraints

Energy is not only consumed, but can be regained.

Energy Constraints

Energy is not only consumed, but can be regained.

$\rightsquigarrow$ "prices" can be negative;

$\rightsquigarrow$ the aim is to continuously satisfy cost constraints

Energy Constraints

Energy is not only consumed, but can be regained.

$\rightsquigarrow$ "prices" can be negative;
$\rightsquigarrow$ the aim is to continuously satisfy cost constraints

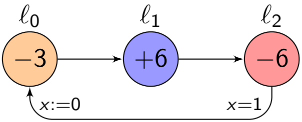
$\rightsquigarrow$ in this paper, we focus on infinite runs.

Energy Constraints

Energy is not only consumed, but can be regained.

- ⇝ "prices" can be negative;
- ⇝ the aim is to continuously satisfy cost constraints
- ⇝ in this paper, we focus on infinite runs.

Example



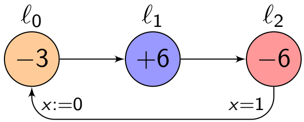
Energy Constraints

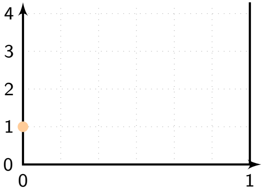
Energy is not only consumed, but can be regained.

$\rightsquigarrow$ "prices" can be negative;
$\rightsquigarrow$ the aim is to continuously satisfy cost constraints

$\rightsquigarrow$ in this paper, we focus on infinite runs.

Example





lower-bound problem

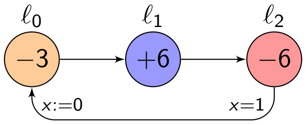
Energy Constraints

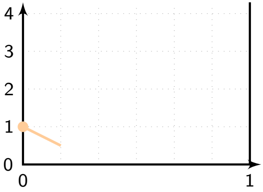
Energy is not only consumed, but can be regained.

⇝ "prices" can be negative;
⇝ the aim is to continuously satisfy cost constraints

⇝ in this paper, we focus on infinite runs.

Example





lower-bound problem

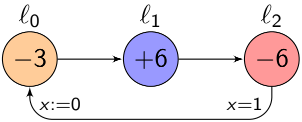
Energy Constraints

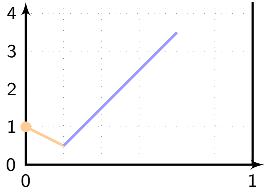
Energy is not only consumed, but can be regained.

$\leadsto$ "prices" can be negative;
$\leadsto$ the aim is to continuously satisfy cost constraints

$\leadsto$ in this paper, we focus on infinite runs.

Example





lower-bound problem

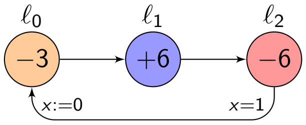
Energy Constraints

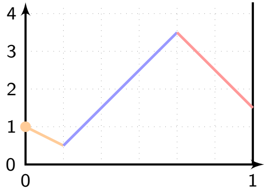
Energy is not only consumed, but can be regained.

$\leadsto$ "prices" can be negative;
$\leadsto$ the aim is to continuously satisfy cost constraints

$\leadsto$ in this paper, we focus on infinite runs.

Example





lower-bound problem

Energy Constraints

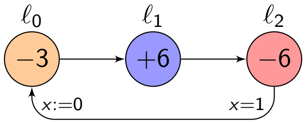
Energy is not only consumed, but can be regained.

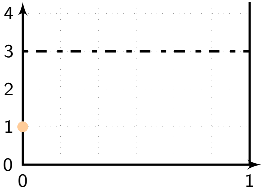
$\leadsto$ "prices" can be negative;

$\leadsto$ the aim is to continuously satisfy cost constraints

$\leadsto$ in this paper, we focus on infinite runs.

Example





lower-upper-bound problem

Energy Constraints

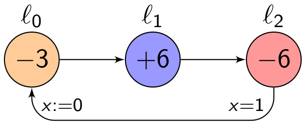
Energy is not only consumed, but can be regained.

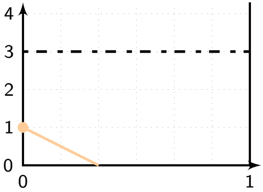
$\rightsquigarrow$ "prices" can be negative;

$\rightsquigarrow$ the aim is to continuously satisfy cost constraints

$\rightsquigarrow$ in this paper, we focus on infinite runs.

Example





lower-upper-bound problem

Energy Constraints

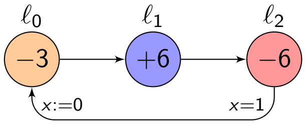
Energy is not only consumed, but can be regained.

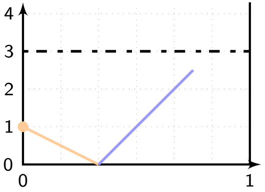
$\rightsquigarrow$ "prices" can be negative;

$\rightsquigarrow$ the aim is to continuously satisfy cost constraints

$\rightsquigarrow$ in this paper, we focus on infinite runs.

Example





lower-upper-bound problem

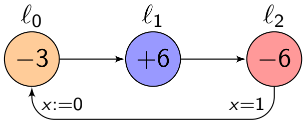
Energy Constraints

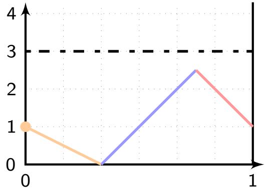
Energy is not only consumed, but can be regained.

$\rightsquigarrow$ "prices" can be negative;
$\rightsquigarrow$ the aim is to continuously satisfy cost constraints

$\rightsquigarrow$ in this paper, we focus on infinite runs.

Example





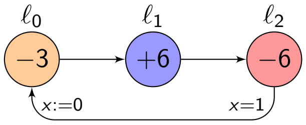
lower-upper-bound problem

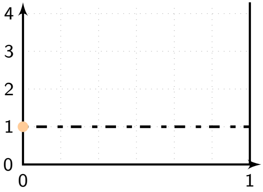
Energy Constraints

Energy is not only consumed, but can be regained.

- ⇝ "prices" can be negative;
- ⇝ the aim is to continuously satisfy cost constraints
- ⇝ in this paper, we focus on infinite runs.

Example





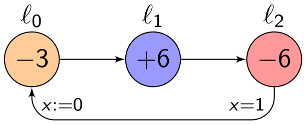
lower-weak-upper-bound problem

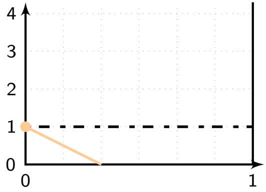
Energy Constraints

Energy is not only consumed, but can be regained.

- ⇝ "prices" can be negative;
- ⇝ the aim is to continuously satisfy cost constraints
- ⇝ in this paper, we focus on infinite runs.

Example





lower-weak-upper-bound problem

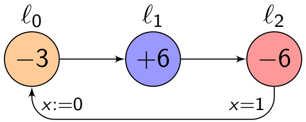
Energy Constraints

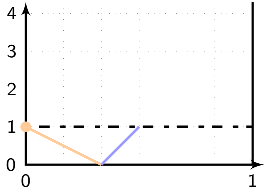
Energy is not only consumed, but can be regained.

$\rightsquigarrow$ "prices" can be negative;
$\rightsquigarrow$ the aim is to continuously satisfy cost constraints

$\rightsquigarrow$ in this paper, we focus on infinite runs.

Example





lower-weak-upper-bound problem

Energy Constraints

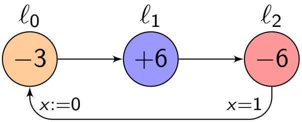
Energy is not only consumed, but can be regained.

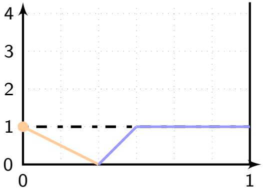
$\leadsto$ "prices" can be negative;

$\leadsto$ the aim is to continuously satisfy cost constraints

$\leadsto$ in this paper, we focus on infinite runs.

Example





lower-weak-upper-bound problem

Existing results for the perfect 1-clock case

[BFLMS08], [BFLM10]

	exist. problem	**univ. problem**	**games**
L	$\in$ *PTIME*	$\in$ *PTIME*	?
L+W	$\in$ *PTIME*	$\in$ *PTIME*	?
L+U	?	?	undecidable

Note: PTIME membership results hold if there are no discrete costs (EXPTIME otherwise).

Existing results for the perfect 1-clock case

[BFLMS08], [BFLM10]

	exist. problem	**univ. problem**	**games**
L	$\in$ *PTIME*	$\in$ *PTIME*	?
L+W	$\in$ *PTIME*	$\in$ *PTIME*	?
L+U	?	?	undecidable

Note: PTIME membership results hold if there are no discrete costs (EXPTIME otherwise).

➜ We will introduce imperfect information on the energy level to solve a L+U problem

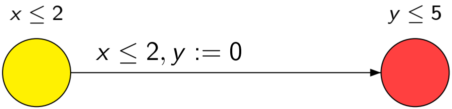
Outline of the presentation

1-clock PTA with imperfect energy level

- The exact value of the energy level (=price) is not known in general
- The energy level is only observed when firing so-called update transitions
- Derivative of the price is defined by a non-punctual interval

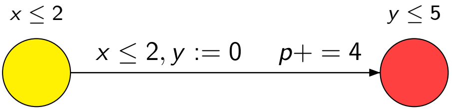
1-clock PTA with imperfect energy level

- The exact value of the energy level (=price) is not known in general
- The energy level is only observed when firing so-called update transitions
- Derivative of the price is defined by a non-punctual interval



1-clock PTA with imperfect energy level

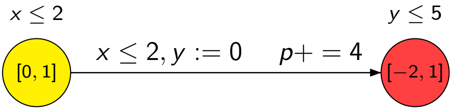
- The exact value of the energy level (=price) is not known in general
- The energy level is only observed when firing so-called update transitions
- Derivative of the price is defined by a non-punctual interval



- We allow discrete updates of the price

1-clock PTA with imperfect energy level

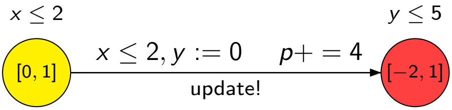
- The exact value of the energy level (=price) is not known in general
- The energy level is only observed when firing so-called update transitions
- Derivative of the price is defined by a non-punctual interval



- We allow discrete updates of the price
- The dynamics of the price is defined as in rectangular hybrid automata: $\dot{p} \in [0,1]$

1-clock PTA with imperfect energy level

- The exact value of the energy level (=price) is not known in general
- The energy level is only observed when firing so-called update transitions
- Derivative of the price is defined by a non-punctual interval

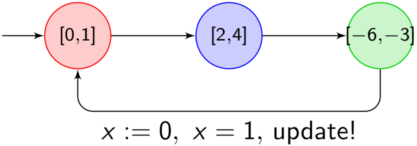


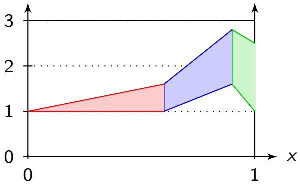
- We allow discrete updates of the price
- The dynamics of the price is defined as in rectangular hybrid automata: $\dot{p} \in [0,1]$
- Transitions with "update!" mean that after having fired this transition, the exact value of the energy level is observed.

1-clock PTA with imperfect energy level (2)

We see this model as a two-player game:

- the controller chooses the transitions and the delays.
- the environment chooses the rate of the energy





The controller only observes the energy level after having fired "update!" transtitions.

More formally

A *strategy* for the controller represents here a mapping:
Finite prefixes of runs $\longrightarrow$ Discrete transitions $\cup$ Delays

A strategy is *admissible* if it respects the imperfect information:
if two runs give the same observation, then the strategy
must give the same decision.

A strategy is *winning* if all its outcomes are safe runs.

Problem: Given a 1cPTA with imp. energy level, an initial state s_0 and a safe interval S, does there exist a winning admissible alternating strategy?

Theorem

Under some assumptions on 1c-PTAs, this problem is decidable.

Outline of the presentation

Outline of the proof

We build a Presburger formula with real variables which characterizes the existence of a winning admissible strategy.

If one has a winning predicate, one can express that in a given configuration, there exists a move which only leads to winning states.

Key ingredient: we use imperfect information to show that winning configurations can be gathered into a finite number of intervals.

➜ The Presburger formula expresses the existence of these intervals.

Outline of the proof

We build a Presburger formula with real variables which characterizes the existence of a winning admissible strategy.

If one has a winning predicate, one can express that in a given configuration, there exists a move which only leads to winning states.

Key ingredient: we use imperfect information to show that winning configurations can be gathered into a finite number of intervals.

➜ The Presburger formula expresses the existence of these intervals.

Our Hypothesis:

- each cycle carries at least one “update!” transition,
- when the energy is observed, the clock is reset, and it is compared to a positive lower bound.

How imperfect information helps

In the following we consider "meta-transitions" that consist in sequence of non-update transitions ending by an update transition.

Using our hypothesis on the model, we prove:

Lemma

There exists a positive value $\Delta > 0$ such that after having fired a meta-transition, the imprecision on the value of the energy is at least Δ.

How imperfect information helps

In the following we consider "meta-transitions" that consist in sequence of non-update transitions ending by an update transition.

Using our hypothesis on the model, we prove:

Lemma

There exists a positive value $\Delta > 0$ *such that after having fired a meta-transition, the imprecision on the value of the energy is at least* Δ.

Corollary

Let S *be a safe interval. If a configuration is winning and has an entering meta-transition, then there exists a winning interval of size at least* Δ *containing it.*
As a consequence, in each location, winning configurations are included in at most $N := \lceil \frac{|S|}{\Delta} \rceil$ *intervals.*

Construction of the formula

Let e be an energy level, t be a meta-transition and $\overrightarrow{\tau}$ be a vector of timestamps for t. We define the following operators:

- the predicate $\mathit{Safe}(e, t, \overrightarrow{\tau})$
- the interval $\mathit{Outcomes}(e, t, \overrightarrow{\tau})$

Construction of the formula

Let e be an energy level, t be a meta-transition and $\overrightarrow{\tau}$ be a vector of timestamps for t. We define the following operators:

- the predicate $\mathit{Safe}(e, t, \overrightarrow{\tau})$
- the interval $\mathit{Outcomes}(e, t, \overrightarrow{\tau})$

Let $Q = \{q_1, \ldots q_n\}$ denote the set of states.
We consider variables $a_{i,j}, b_{i,j}$, with $1 \leq i \leq n$ and $1 \leq j \leq N$.

Construction of the formula

Let e be an energy level, t be a meta-transition and $\overrightarrow{\tau}$ be a vector of timestamps for t. We define the following operators:

- the predicate $\mathit{Safe}(e, t, \overrightarrow{\tau})$
- the interval $\mathit{Outcomes}(e, t, \overrightarrow{\tau})$

Let $Q = \{q_1, \ldots q_n\}$ denote the set of states.
We consider variables $a_{i,j}, b_{i,j}$, with $1 \leq i \leq n$ and $1 \leq j \leq N$.

Let $q \in Q$. We define the winning predicate:

$$\mathit{Win}(q, e) \iff \bigvee_{q \xrightarrow{t} q_k} \exists \overrightarrow{\tau} \text{ s.t.} \left\{ \begin{array}{ll} & \mathit{Safe}(e, t, \overrightarrow{\tau}) \\ \wedge & \\ & \bigvee_{\ell=1}^{N} \mathit{Outcomes}(e, t, \overrightarrow{\tau}) \subseteq [a_{k,\ell}, b_{k,\ell}] \end{array} \right.$$

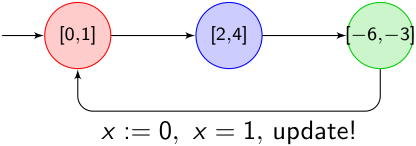
Construction of the formula (2)

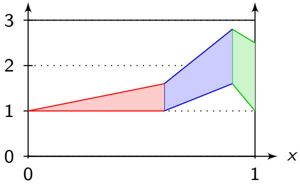
Let q_0 (resp. e_0) denote the initial location (resp. energy).
We define the Presburger formula as follows:

$$\Phi(q_0, e_0) = \exists_{i=1}^{n} \exists_{j=1}^{N} a_{i,j}, b_{i,j} \text{ s.t. } \begin{cases} \bigwedge_{i,j} [a_{i,j}, b_{i,j}] \subseteq S \\ \wedge \; Win(q_0, e_0) \\ \bigwedge_{i,j} \forall e, a_{i,j} \leq e \leq b_{i,j} \Rightarrow Win(q_i, e) \end{cases}$$

Bonus: Using Fourier-Motzkin elimination, we end up with the set of initial values of the energy for which there exists a winning strategy.

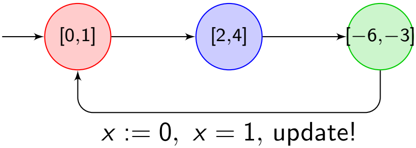
Example

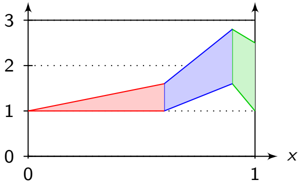




There is only one meta-transition: the cycle. Its minimal imprecision is $\Delta = 1$. We thus obtain $N = \frac{3}{1} = 3$.

Example



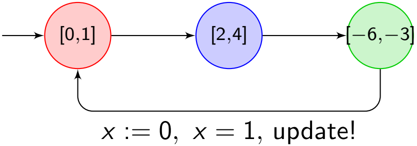


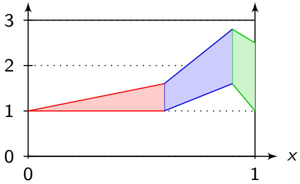
There is only one meta-transition: the cycle. Its minimal imprecision is $\Delta = 1$. We thus obtain $N = \frac{3}{1} = 3$.

We consider three timestamps τ_1, τ_2 and τ_3 (which verify $\sum_i \tau_i = 1$).

$$
\mathit{Safe}(e, t, \overrightarrow{\tau}) \iff \begin{cases} \quad 0 \leq e & \wedge \quad e \leq 3 \\ \wedge \quad 0 \leq e & \wedge \quad e + \tau_1 \leq 3 \\ \wedge \quad 0 \leq e + 2\tau_2 & \wedge \quad e + \tau_1 + 4\tau_2 \leq 3 \\ \wedge \quad 0 \leq e + 2\tau_2 - 6\tau_3 & \wedge \quad e + \tau_1 + 4\tau_2 - 3\tau_3 \leq 3 \end{cases}
$$

Example





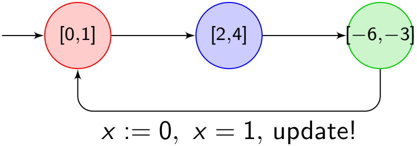
There is only one meta-transition: the cycle. Its minimal imprecision is $\Delta = 1$. We thus obtain $N = \frac{3}{1} = 3$.

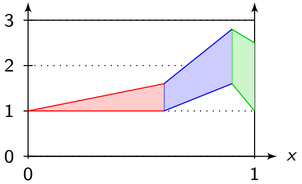
We consider three timestamps τ_1, τ_2 and τ_3 (which verify $\sum_i \tau_i = 1$).

$$Safe(e, t, \overrightarrow{\tau}) \iff \begin{cases} \quad 0 \leq e & \wedge \quad e \leq 3 \\ \wedge \quad 0 \leq e & \wedge \quad e + \tau_1 \leq 3 \\ \wedge \quad 0 \leq e + 2\tau_2 & \wedge \quad e + \tau_1 + 4\tau_2 \leq 3 \\ \wedge \quad 0 \leq e + 2\tau_2 - 6\tau_3 & \wedge \quad e + \tau_1 + 4\tau_2 - 3\tau_3 \leq 3 \end{cases}$$

$$Outcomes(e, t, \overrightarrow{\tau}) = [e + 2\tau_2 - 6\tau_3, e + \tau_1 + 4\tau_2 - 3\tau_3]$$

Example





There is only one meta-transition: the cycle. Its minimal imprecision is $\Delta = 1$. We thus obtain $N = \frac{3}{1} = 3$.

We consider three timestamps τ_1, τ_2 and τ_3 (which verify $\sum_i \tau_i = 1$).

$$Safe(e, t, \overrightarrow{\tau}) \iff \begin{cases} \quad 0 \leq e & \wedge \quad e \leq 3 \\ \wedge \quad 0 \leq e & \wedge \quad e + \tau_1 \leq 3 \\ \wedge \quad 0 \leq e + 2\tau_2 & \wedge \quad e + \tau_1 + 4\tau_2 \leq 3 \\ \wedge \quad 0 \leq e + 2\tau_2 - 6\tau_3 & \wedge \quad e + \tau_1 + 4\tau_2 - 3\tau_3 \leq 3 \end{cases}$$

$$Outcomes(e, t, \overrightarrow{\tau}) = [e + 2\tau_2 - 6\tau_3, e + \tau_1 + 4\tau_2 - 3\tau_3]$$

Here we end up with the constraint $0 \leq e_0 \leq \frac{12}{5}$

Outline of the presentation

Robust strategies

Recall that a strategy is a sequence of transitions and timestamps.

What happens if the timestamps given by the strategy are slightly perturbed?

Robust strategies

Recall that a strategy is a sequence of transitions and timestamps.

What happens if the timestamps given by the strategy are slightly perturbed?

Let $\delta > 0$ be a parameter of perturbation. We consider a norm on $\mathbb{R}_+^k$, for instance $||\overrightarrow{\tau}||_\infty = \max_{1 \le i \le d} |\tau_i|$.

We can modify operators $\mathit{Safe}(e, t, \overrightarrow{\tau})$ and $\mathit{Outcomes}(e, t, \overrightarrow{\tau})$ to include this perturbation:

Robust strategies

Recall that a strategy is a sequence of transitions and timestamps.

What happens if the timestamps given by the strategy are slightly perturbed?

Let $\delta > 0$ be a parameter of perturbation. We consider a norm on $\mathbb{R}_+^k$, for instance $||\overrightarrow{\tau}||_\infty = \max_{1 \leq i \leq d} |\tau_i|$.

We can modify operators $\mathit{Safe}(e, t, \overrightarrow{\tau})$ and $\mathit{Outcomes}(e, t, \overrightarrow{\tau})$ to include this perturbation:

$$\mathit{Safe}_\delta(e, t, \overrightarrow{\tau}) \stackrel{def}{=} \forall \overrightarrow{\tau}' \in \mathbb{R}_+^d, ||\overrightarrow{\tau}' - \overrightarrow{\tau}||_\infty \leq \delta \Rightarrow \mathit{Safe}(e, t, \overrightarrow{\tau}')$$

Robust strategies

Recall that a strategy is a sequence of transitions and timestamps.

What happens if the timestamps given by the strategy are slightly perturbed?

Let $\delta > 0$ be a parameter of perturbation. We consider a norm on $\mathbb{R}_+^k$, for instance $||\overrightarrow{\tau}||_\infty = \max_{1 \leq i \leq d} |\tau_i|$.

We can modify operators $Safe(e, t, \overrightarrow{\tau})$ and $Outcomes(e, t, \overrightarrow{\tau})$ to include this perturbation:

$$Safe_\delta(e, t, \overrightarrow{\tau}) \stackrel{def}{=} \forall \overrightarrow{\tau}' \in \mathbb{R}_+^d, ||\overrightarrow{\tau}' - \overrightarrow{\tau}||_\infty \leq \delta \Rightarrow Safe(e, t, \overrightarrow{\tau}')$$

$$Outcomes_\delta(e, t, \overrightarrow{\tau}) \stackrel{def}{=} \{e' \mid \exists \overrightarrow{\tau}'.||\overrightarrow{\tau}' - \overrightarrow{\tau}||_\infty \leq \delta \wedge e' \in Out(e, t, \overrightarrow{\tau}')\}$$

Robust strategies

Recall that a strategy is a sequence of transitions and timestamps.

What happens if the timestamps given by the strategy are slightly perturbed?

Let $\delta > 0$ be a parameter of perturbation. We consider a norm on $\mathbb{R}_+^k$, for instance $||\overrightarrow{\tau}||_\infty = \max_{1 \leq i \leq d} |\tau_i|$.

We can modify operators $Safe(e, t, \overrightarrow{\tau})$ and $Outcomes(e, t, \overrightarrow{\tau})$ to include this perturbation:

$$Safe_\delta(e, t, \overrightarrow{\tau}) \stackrel{def}{=} \forall \overrightarrow{\tau}' \in \mathbb{R}_+^d, ||\overrightarrow{\tau}' - \overrightarrow{\tau}||_\infty \leq \delta \Rightarrow Safe(e, t, \overrightarrow{\tau}')$$

$$Outcomes_\delta(e, t, \overrightarrow{\tau}) \stackrel{def}{=} \{e' \mid \exists \overrightarrow{\tau}'.||\overrightarrow{\tau}' - \overrightarrow{\tau}||_\infty \leq \delta \wedge e' \in Out(e, t, \overrightarrow{\tau}')\}$$

➜ definition of Win_δ ➜ definition of $\Phi_\delta(q_0, e_0)$

New Presburger formula

For a fixed value of δ, the Presburger formula $\Phi_\delta(q_0, e_0)$ characterizes the initial values of the energy which own δ-robust winning strategies.

New Presburger formula

For a fixed value of δ, the Presburger formula $\Phi_\delta(q_0, e_0)$ characterizes the initial values of the energy which own δ-robust winning strategies.

Can we get rid of δ?

New Presburger formula

For a fixed value of δ, the Presburger formula $\Phi_\delta(q_0, e_0)$ characterizes the initial values of the energy which own δ-robust winning strategies.

Can we get rid of δ?

Yes we can!

New Presburger formula

For a fixed value of δ, the Presburger formula $\Phi_\delta(q_0, e_0)$ characterizes the initial values of the energy which own δ-robust winning strategies.

Can we get rid of δ?

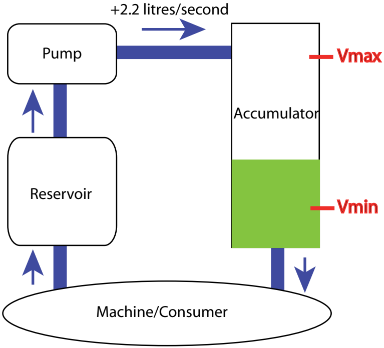
Yes we can!

➜ Consider the formula $\Phi_{robust}(q_0, e_0) \stackrel{def}{=} \exists \delta > 0 \mid \Phi_\delta(q_0, e_0)$

Outline of the presentation

A case study

The study of L+U energy problems has been motivated by a collaboration within the european research project Quasimodo.



Synthesis of a pump controller for an oil-accumulator system.

L+U: The oil volume must stay within a safety interval.

Infinite run: The machine repeats a cycle of production of plactic cells forever.

A case study (2)

The oil level can be modelled as a price:

- it is a linear hybrid variable,
- it can both increase (pump on) and decrease (machine consumes oil)
- price rates are not singletons: there are imprecisions in the machine rates.

A case study (2)

The oil level can be modelled as a price:

- it is a linear hybrid variable,
- it can both increase (pump on) and decrease (machine consumes oil)
- price rates are not singletons: there are imprecisions in the machine rates.

We need to modify the model to solve some difficulties:

- remove one clock!
- how many update! transitions?

A case study (2)

The oil level can be modelled as a price:

- it is a linear hybrid variable,
- it can both increase (pump on) and decrease (machine consumes oil)
- price rates are not singletons: there are imprecisions in the machine rates.

We need to modify the model to solve some difficulties:

- remove one clock!
- how many update! transitions?

➜ We have to develop a tool to perform this analysis!
We plan to rely on the SMT solver Z3 of Nikolaj Bjorner.

Outline of the presentation

Conclusion

Contributions:

- decidability for a L+U problem
- Presburger arithmetic as a new tool for energy constraints problems
- extends for free to robustness issues

Challenges/Perspectives:

- extraction of strategies
- develop a tool (case study)
- works also for 1-clock prices timed games
- other extensions? (multiple costs, optimization...)
- exact complexity of the procedure?