Energy consumption in timed systems

Patricia Bouyer

LSV – CNRS & ENS Cachan

November 13, 2008

Systems that need to be verified

$\rightarrow$ include reactive, embedded systems, (communication) protocols, ...

Systems that need to be verified

$\rightarrow$ include reactive, embedded systems, (communication) protocols, ...

Important characteristics

They have to meet numerous quantitative constraints such as:

- timing constraints

  "Will the airbag open within 5ms after the car crashes?"

Systems that need to be verified

$\rightarrow$ include reactive, embedded systems, (communication) protocols, ...

Important characteristics

They have to meet numerous quantitative constraints such as:

- timing constraints

  "Will the airbag open within 5ms after the car crashes?"

- energy/cost/resource constraints

  "Can an autonomous robot with solar cells explore a fixed area?"
  "How should one optimize the profit in a factory?"
  "Can we schedule those tasks on two processors?"

- ...

A rather general solution: hybrid systems

[Henzinger 1996]

What is a hybrid system?

  a discrete control (the mode of the system)
$+$ a continuous evolution within a mode (given by variables)

A rather general solution: hybrid systems

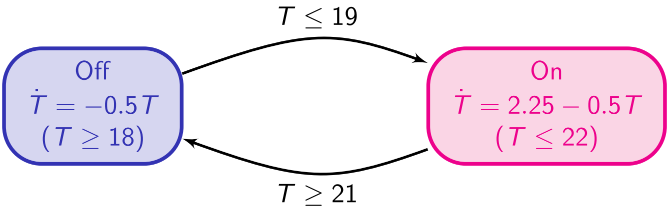
[Henzinger 1996]

What is a hybrid system?

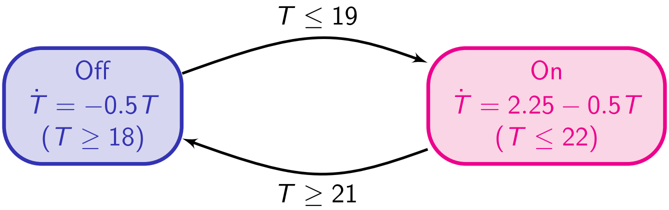
  a discrete control (the mode of the system)
$+$ a continuous evolution within a mode (given by variables)

Example (The thermostat)

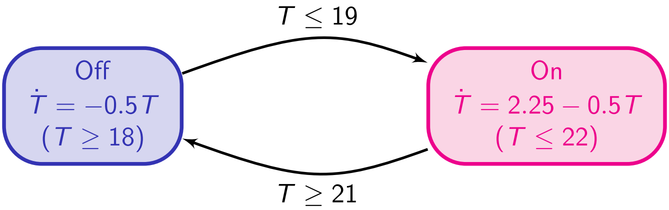
A simple thermostat, where T (the temperature) depends on the time:

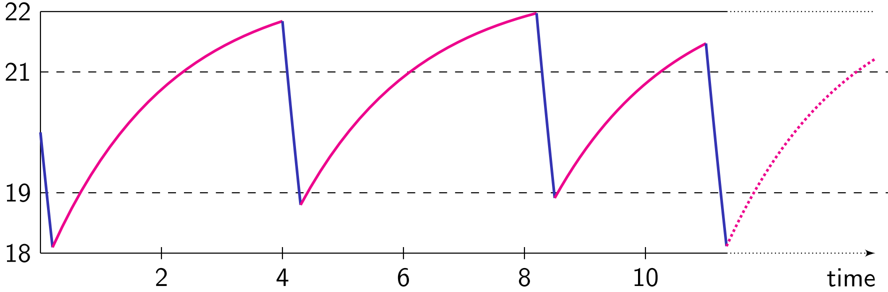


The thermostat example



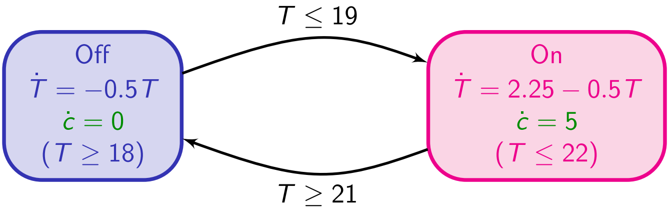
The thermostat example





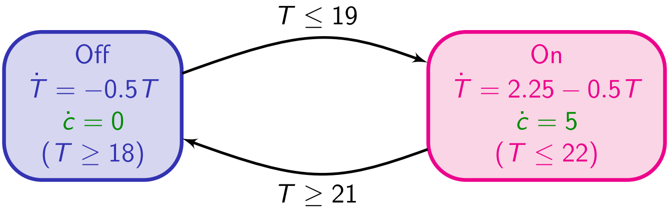
Going further with the thermostat

The new variable c represents the cost to be paid.



Going further with the thermostat

The new variable c represents the cost to be paid.

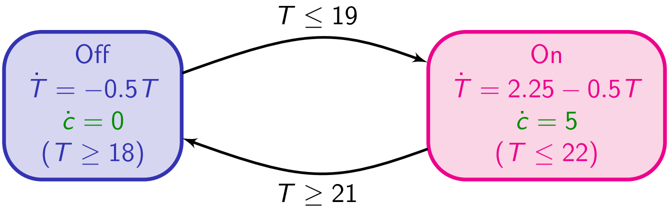


Question

Is that possible to pay no more than 3€ per hour to maintain the temperature between 18°C and 22°C?

Going further with the thermostat

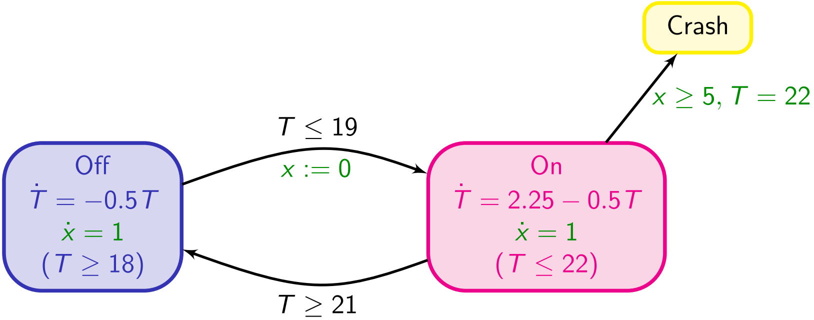
The new variable c represents the cost to be paid.



Of course, this is a complex question, and simpler questions can be asked...

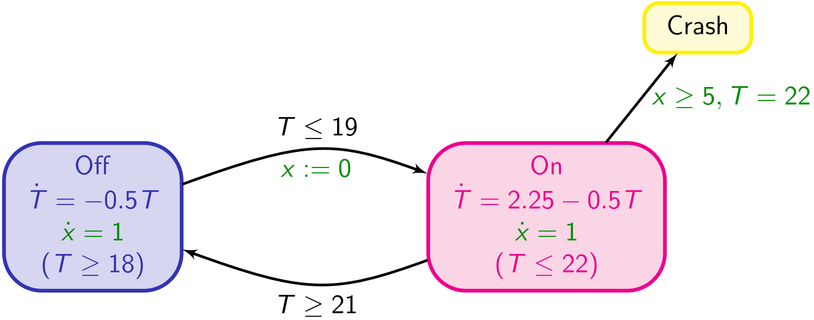
Going further with the thermostat

The variable x measures the time elapsing in mode On.



Going further with the thermostat

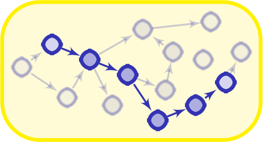
The variable x measures the time elapsing in mode On.



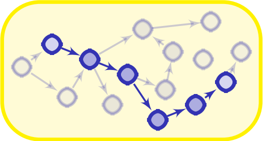
Question

Is location Crash reachable from state (Off, $T = 20, x = 0$)?

Ok...

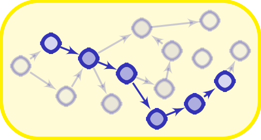


Ok...

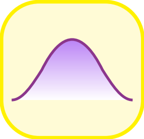


Easy...

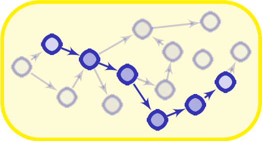
Ok...



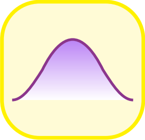
Easy...



Ok...

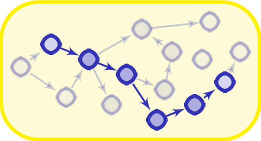


Easy...

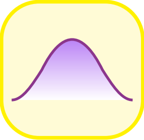


Easy...

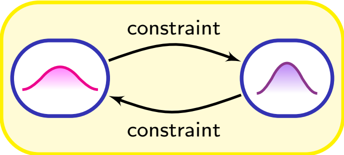
Ok... but?



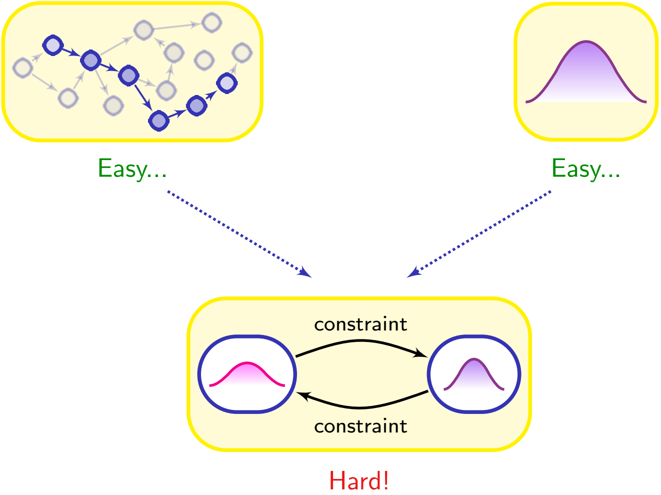
Easy...



Easy...



Ok... but?



Why is that hard?

What we do	What we don't do

Why is that hard?

What we do	What we don't do
- exhaustive search	- partial simulation

Why is that hard?

What we do	What we don't do
- exhaustive search - exact and symbolic computation (no round-off errors)	- partial simulation - approximate computation

Why is that hard?

What we do	**What we don't do**
- exhaustive search	- partial simulation
- exact and symbolic computation (no round-off errors)	- approximate computation
- fully-automated methods (for large classes of systems)	- *ad-hoc* methods

Why is that hard?

What we do	**What we don't do**
- exhaustive search	- partial simulation
- exact and symbolic computation (no round-off errors)	- approximate computation
- fully-automated methods (for large classes of systems)	- *ad-hoc* methods

Theorem [Henzinger 1996]

The hybrid system model is undecidable as soon as we use:

- differential equations of the form $\dot{x} = 0$ or $\dot{x} = 1$;
- constraints of the form $x \in [a, b]$;
- resets of the variables to 0.

$\leadsto$ There is no general algorithm (or program) to verify hybrid systems.

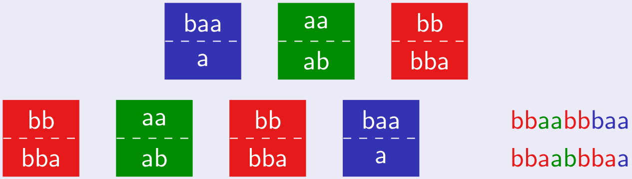
What is undecidability? The Post correspondence problem

An example

baa	aa	bb
a	ab	bba

What is undecidability? The Post correspondence problem

An example



What is undecidability? The Post correspondence problem

An example

baa	aa	bb
a	ab	bba

bb	aa	bb	baa
bba	ab	bba	a

bbaabbbaa
bbaabbbaa

Theorem [Post 1946]

PCP is undecidable.

$\rightsquigarrow$ There is no general algorithm (or program) to solve PCP.

Understanding further PCP

Another example

bab	bb	a
a	ba	abb

Understanding further PCP

Another example

bab	bb	a
a	ba	abb

There is no solution!

Understanding further PCP

Another example

bab	bb	a
a	ba	abb

There is no solution!

The PCP@home contest

aa	abab	ba	b
a	aaaa	aaab	bab

http://www.theory.informatik.uni-kassel.de/∼stamer/pcp/

Understanding further PCP

Another example

bab	bb	a
a	ba	abb

There is no solution!

The PCP@home contest

The shortest solution for

aa	abab	ba	b
a	aaaa	aaab	bab

has length 781.

http://www.theory.informatik.uni-kassel.de/~stamer/pcp/

Further undecidability

Hilbert's tenth problem

Given a multivariate polynomial $P(X_1, \dots, X_n) \in \mathbb{Q}[X_1, \dots, X_n]$, do there exist integers $(a_1, \dots, a_n) \in \mathbb{Z}^n$ such that $P(a_1, \dots, a_n) = 0$.

Further undecidability

Hilbert's tenth problem

Given a multivariate polynomial $P(X_1, \ldots, X_n) \in \mathbb{Q}[X_1, \ldots, X_n]$, do there exist integers $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ such that $P(a_1, \ldots, a_n) = 0$.

Theorem [Matiyasevich 1970]

Hilbert's tenth problem is undecidable.

Undecidability can be understood as follows

Reduction from tenth Hilbert's problem

Given a multivariate polynomial P, one can construct a hybrid system H_P such that H_P is safe iff P has an integral solution.

Undecidability can be understood as follows

Reduction from tenth Hilbert's problem

Given a multivariate polynomial P, one can construct a hybrid system H_P such that H_P is safe iff P has an integral solution.

Reduction from PCP

Given a finite set of tiles S for PCP, one can construct a hybrid system H_S such that H_S is safe iff PCP has a solution with those tiles.

Undecidability can be understood as follows

Reduction from tenth Hilbert's problem

Given a multivariate polynomial P, one can construct a hybrid system H_P such that H_P is safe iff P has an integral solution.

Reduction from PCP

Given a finite set of tiles S for PCP, one can construct a hybrid system H_S such that H_S is safe iff PCP has a solution with those tiles.

Reduction from your favorite difficult problem

Given any instance I of a difficult problem, one can construct a hybrid system H_I such that H_I is safe iff there is a solution to I.

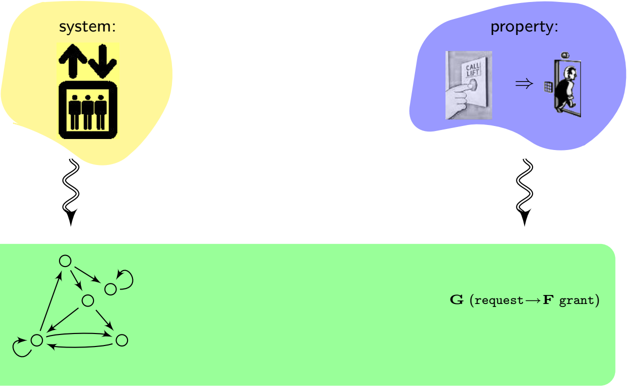
What our work consists in

system:

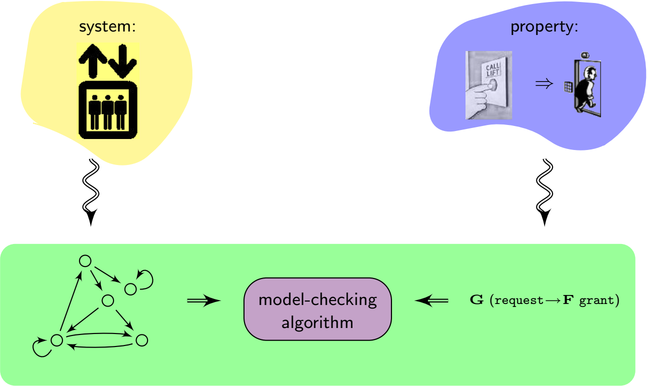
property:

$\Rightarrow$

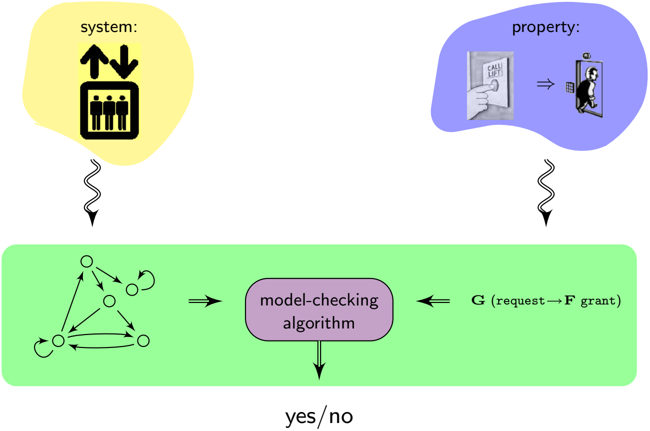
What our work consists in



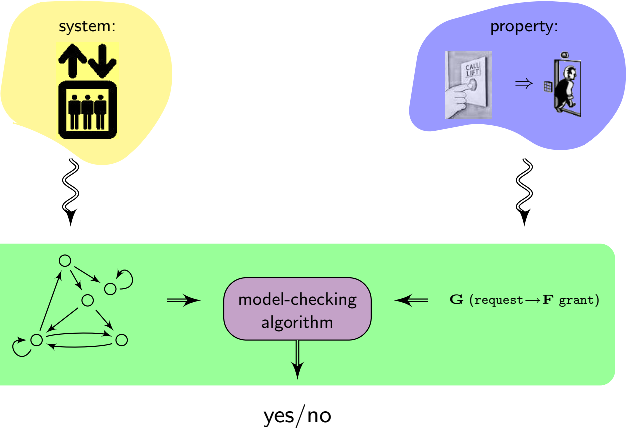
What our work consists in



What our work consists in

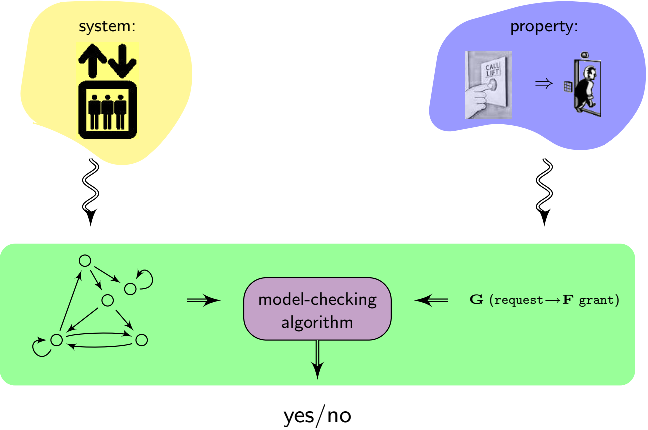


What our work consists in



- Design classes of models such that:
  - we will be able to analyze them automatically (and efficiently);
  - they will be powerful enough to represent numerous systems.

What our work consists in



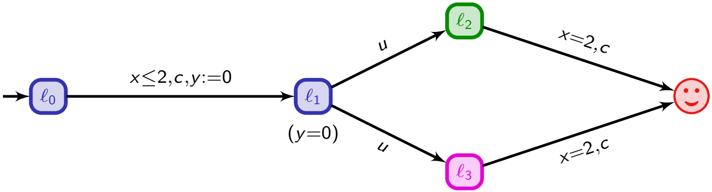
- Design classes of models such that:
  - we will be able to analyze them automatically (and efficiently);
  - they will be powerful enough to represent numerous systems.
- Design efficient model-checking algorithms

Timed automata [Alur, Dill 1990]

A timed automaton: a hybrid system with only clocks, *i.e.* variables whose derivative is always 1 ($\dot{x} = 1$) and that can be reset to 0.

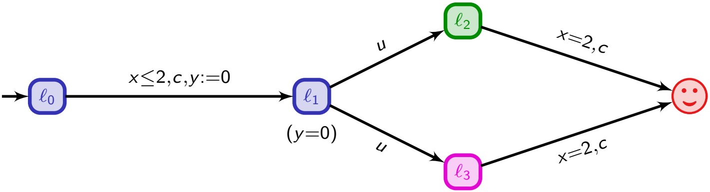
Timed automata [Alur, Dill 1990]

A timed automaton: a hybrid system with only clocks, *i.e.* variables whose derivative is always 1 ($\dot{x} = 1$) and that can be reset to 0.



Timed automata [Alur, Dill 1990]

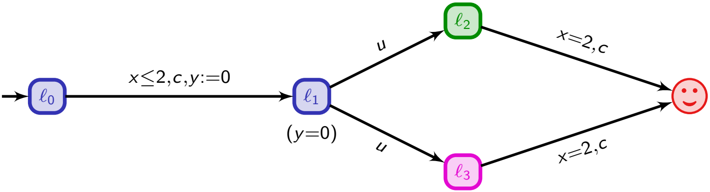
A timed automaton: a hybrid system with only clocks, *i.e.* variables whose derivative is always 1 ($\dot{x} = 1$) and that can be reset to 0.



	ℓ_0
x	0
y	0

Timed automata [Alur, Dill 1990]

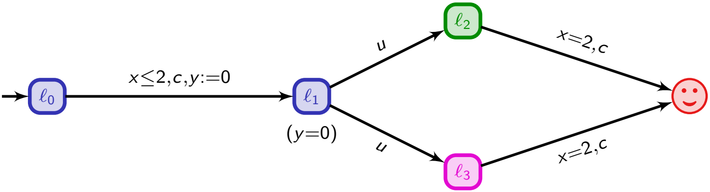
A timed automaton: a hybrid system with only clocks, *i.e.* variables whose derivative is always 1 ($\dot{x} = 1$) and that can be reset to 0.



$$
\begin{array}{cccc}
 & \ell_0 & \xrightarrow{1.3} & \ell_0 \\
x & 0 & & 1.3 \\
y & 0 & & 1.3
\end{array}
$$

Timed automata [Alur, Dill 1990]

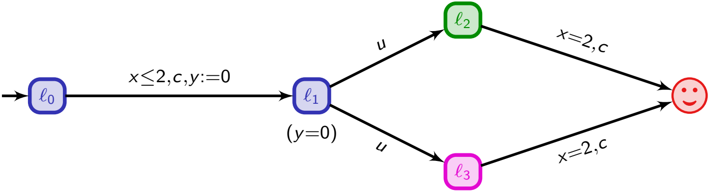
A timed automaton: a hybrid system with only clocks, *i.e.* variables whose derivative is always 1 ($\dot{x} = 1$) and that can be reset to 0.



$$\begin{array}{cccccc} & \ell_0 & \xrightarrow{1.3} & \ell_0 & \xrightarrow{c} & \ell_1 \\ x & 0 & & 1.3 & & 1.3 \\ y & 0 & & 1.3 & & 0 \end{array}$$

Timed automata [Alur, Dill 1990]

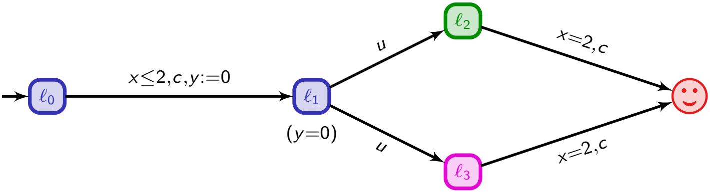
A timed automaton: a hybrid system with only clocks, *i.e.* variables whose derivative is always 1 ($\dot{x} = 1$) and that can be reset to 0.



$$\begin{array}{cccccccc} & \ell_0 & \xrightarrow{1.3} & \ell_0 & \xrightarrow{c} & \ell_1 & \xrightarrow{u} & \ell_3 \\ x & 0 & & 1.3 & & 1.3 & & 1.3 \\ y & 0 & & 1.3 & & 0 & & 0 \end{array}$$

Timed automata [Alur, Dill 1990]

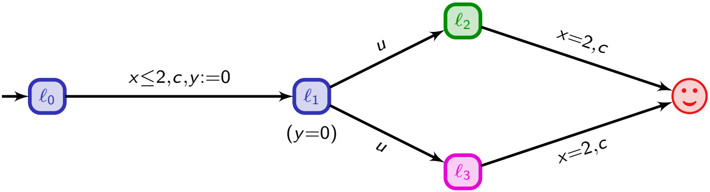
A timed automaton: a hybrid system with only clocks, *i.e.* variables whose derivative is always 1 ($\dot{x} = 1$) and that can be reset to 0.



	ℓ_0	$\xrightarrow{1.3}$	ℓ_0	$\xrightarrow{c}$	ℓ_1	$\xrightarrow{u}$	ℓ_3	$\xrightarrow{0.7}$	ℓ_3
x	0		1.3		1.3		1.3		2
y	0		1.3		0		0		0.7

Timed automata [Alur, Dill 1990]

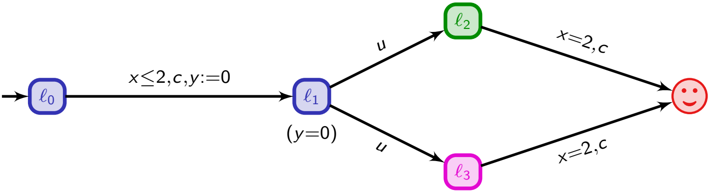
A timed automaton: a hybrid system with only clocks, *i.e.* variables whose derivative is always 1 ($\dot{x} = 1$) and that can be reset to 0.



	ℓ_0	$\xrightarrow{1.3}$	ℓ_0	$\xrightarrow{c}$	ℓ_1	$\xrightarrow{u}$	ℓ_3	$\xrightarrow{0.7}$	ℓ_3	$\xrightarrow{c}$	☺
x	0		1.3		1.3		1.3		2		
y	0		1.3		0		0		0.7		

Timed automata [Alur, Dill 1990]

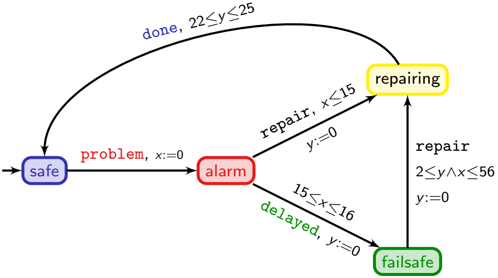
A timed automaton: a hybrid system with only clocks, *i.e.* variables whose derivative is always 1 ($\dot{x} = 1$) and that can be reset to 0.



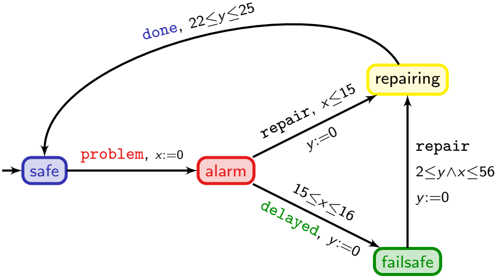
Questions

- Is that possible to reach location  ?
- How long will that take to reach location  ?

A second example

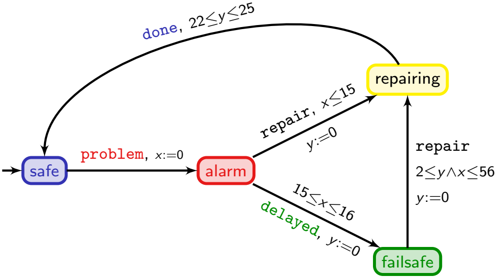


A second example



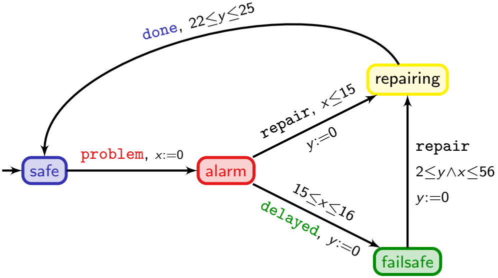
	safe
x	0
y	0

A second example



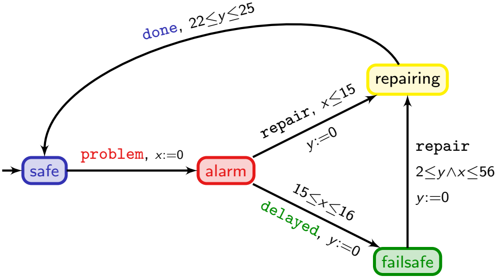
	safe	$\xrightarrow{23}$	safe
x	0		23
y	0		23

A second example



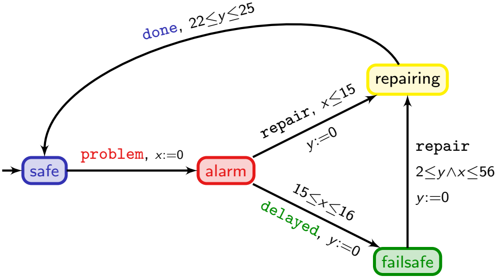
	safe	$\xrightarrow{23}$	safe	$\xrightarrow{\texttt{problem}}$	alarm
x	0		23		0
y	0		23		23

A second example



	safe	$\xrightarrow{23}$	safe	$\xrightarrow{\texttt{problem}}$	alarm	$\xrightarrow{15.6}$	alarm
x	0		23		0		15.6
y	0		23		23		38.6

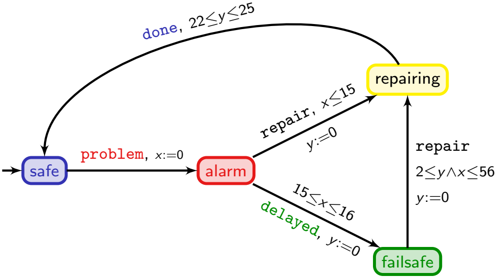
A second example



	safe	$\xrightarrow{23}$	safe	$\xrightarrow{\text{problem}}$	alarm	$\xrightarrow{15.6}$	alarm	$\xrightarrow{\text{delayed}}$	failsafe	
x	0		23		0		15.6		15.6	$\cdots$
y	0		23		23		38.6		0	

	failsafe
$\cdots$	15.6
	0

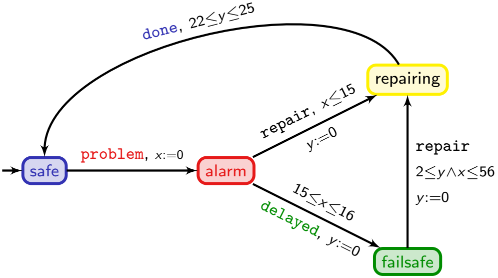
A second example



	safe	$\xrightarrow{23}$	safe	$\xrightarrow{\texttt{problem}}$	alarm	$\xrightarrow{15.6}$	alarm	$\xrightarrow{\texttt{delayed}}$	failsafe	
x	0		23		0		15.6		15.6	$\cdots$
y	0		23		23		38.6		0	

	failsafe	$\xrightarrow{2.3}$	failsafe
$\cdots$	15.6		17.9
	0		2.3

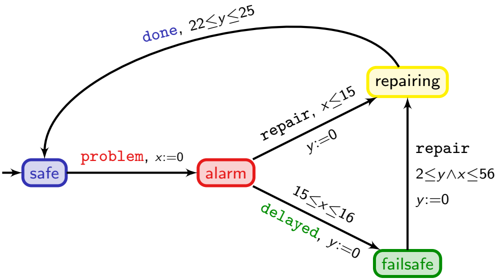
A second example



	safe	$\xrightarrow{23}$	safe	$\xrightarrow{\texttt{problem}}$	alarm	$\xrightarrow{15.6}$	alarm	$\xrightarrow{\texttt{delayed}}$	failsafe	
x	0		23		0		15.6		15.6	⋯
y	0		23		23		38.6		0	

	failsafe	$\xrightarrow{2.3}$	failsafe	$\xrightarrow{\texttt{repair}}$	repairing
⋯	15.6		17.9		17.9
	0		2.3		0

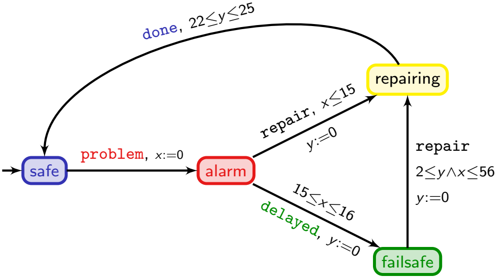
A second example



	safe	$\xrightarrow{23}$	safe	$\xrightarrow{\texttt{problem}}$	alarm	$\xrightarrow{15.6}$	alarm	$\xrightarrow{\texttt{delayed}}$	failsafe		
x	0		23		0		15.6		15.6		⋯
y	0		23		23		38.6		0		

	failsafe	$\xrightarrow{2.3}$	failsafe	$\xrightarrow{\texttt{repair}}$	repairing	$\xrightarrow{22.1}$	repairing
⋯	15.6		17.9		17.9		40
	0		2.3		0		22.1

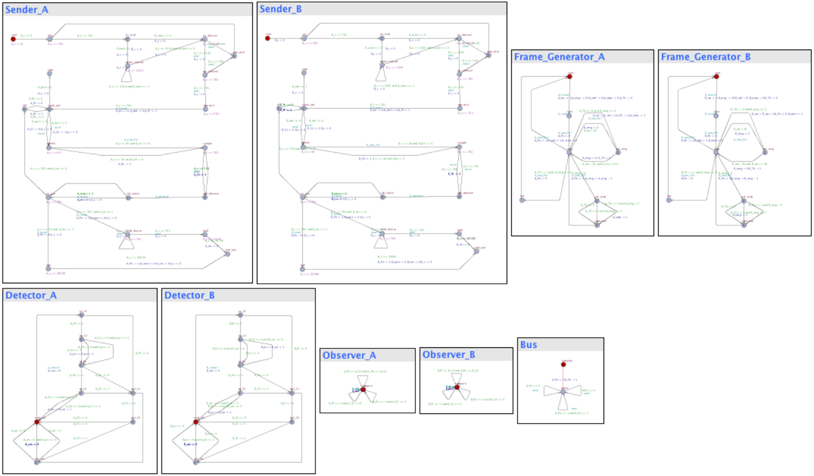
A second example



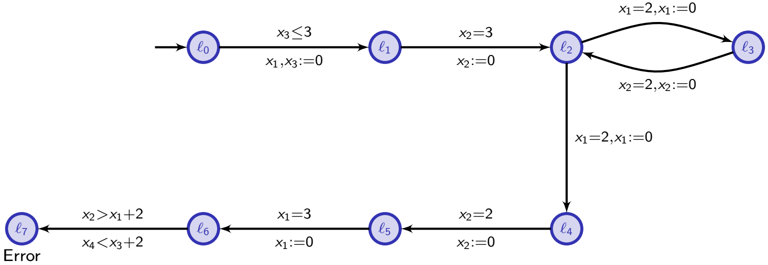
$$\begin{array}{ccccccccccc} & \text{safe} & \xrightarrow{23} & \text{safe} & \xrightarrow{\texttt{problem}} & \text{alarm} & \xrightarrow{15.6} & \text{alarm} & \xrightarrow{\texttt{delayed}} & \text{failsafe} & \\ \text{x} & 0 & & 23 & & 0 & & 15.6 & & 15.6 & \cdots \\ \text{y} & 0 & & 23 & & 23 & & 38.6 & & 0 & \end{array}$$

$$\begin{array}{ccccccccccc} & \text{failsafe} & \xrightarrow{2.3} & \text{failsafe} & \xrightarrow{\texttt{repair}} & \text{repairing} & \xrightarrow{22.1} & \text{repairing} & \xrightarrow{\texttt{done}} & \text{safe} \\ \cdots & 15.6 & & 17.9 & & 17.9 & & 40 & & 40 \\ & 0 & & 2.3 & & 0 & & 22.1 & & 22.1 \end{array}$$

A third example: B&O collision detection protocol



A fourth example



A fundamental result

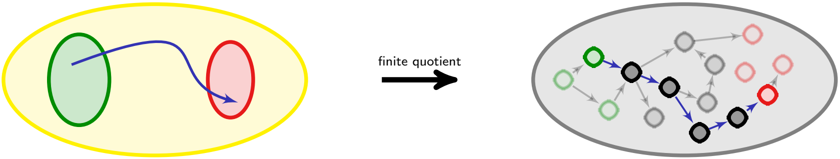
Theorem [Alur & Dill 1990]

There is a general algorithm (or program) to check whether a timed automaton is safe or not.

A fundamental result

Theorem [Alur & Dill 1990]

There is a general algorithm (or program) to check whether a timed automaton is safe or not.

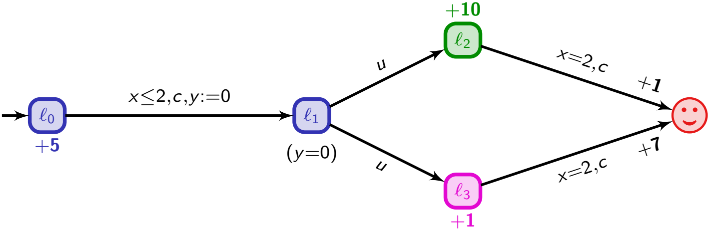


timed automaton

large (but finite) automaton

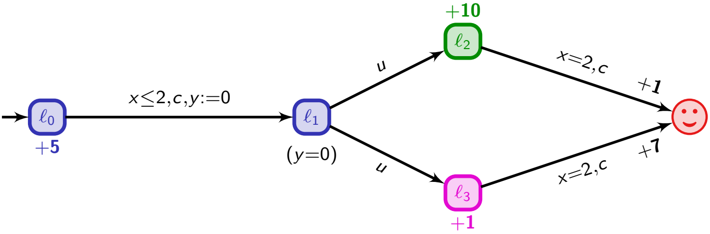
Timed automata with costs (or energy information)

[Alur *et al*, Larsen *et al* 2001]



Timed automata with costs (or energy information)

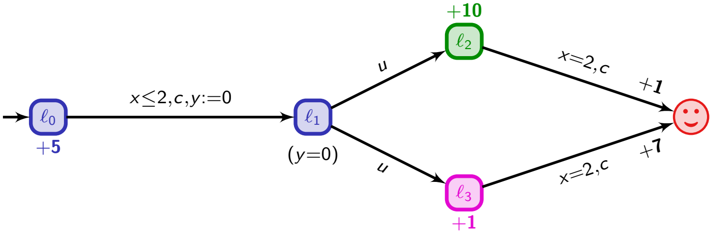
[Alur *et al*, Larsen *et al* 2001]



$$
\begin{array}{ccccccccccccc}
 & \ell_0 & \xrightarrow{1.3} & \ell_0 & \xrightarrow{c} & \ell_1 & \xrightarrow{u} & \ell_3 & \xrightarrow{0.7} & \ell_3 & \xrightarrow{c} & ☺ \\
x & 0 & & 1.3 & & 1.3 & & 1.3 & & 2 & & \\
y & 0 & & 1.3 & & 0 & & 0 & & 0.7 & &
\end{array}
$$

Timed automata with costs (or energy information)

[Alur *et al*, Larsen *et al* 2001]

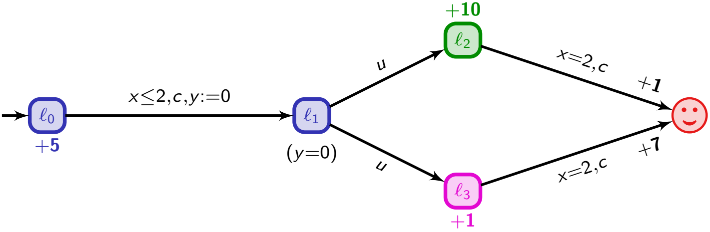


$$
\begin{array}{cccccccccccc}
 & \ell_0 & \xrightarrow{1.3} & \ell_0 & \xrightarrow{c} & \ell_1 & \xrightarrow{u} & \ell_3 & \xrightarrow{0.7} & \ell_3 & \xrightarrow{c} & ☺ \\
x & 0 & & 1.3 & & 1.3 & & 1.3 & & 2 & & \\
y & 0 & & 1.3 & & 0 & & 0 & & 0.7 & &
\end{array}
$$

cost :

Timed automata with costs (or energy information)

[Alur *et al*, Larsen *et al* 2001]

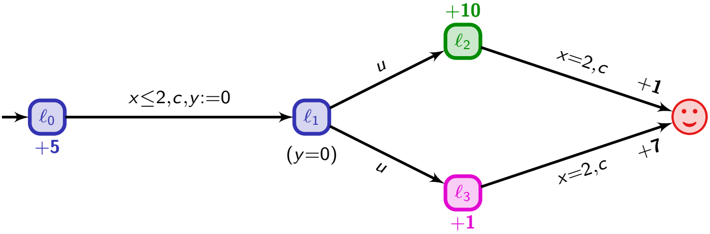


$$\begin{array}{cccccccccccc}
 & \ell_0 & \xrightarrow{1.3} & \ell_0 & \xrightarrow{c} & \ell_1 & \xrightarrow{u} & \ell_3 & \xrightarrow{0.7} & \ell_3 & \xrightarrow{c} & ☺ \\
x & 0 & & 1.3 & & 1.3 & & 1.3 & & 2 & & \\
y & 0 & & 1.3 & & 0 & & 0 & & 0.7 & &
\end{array}$$

cost : 6.5

Timed automata with costs (or energy information)

[Alur *et al*, Larsen *et al* 2001]

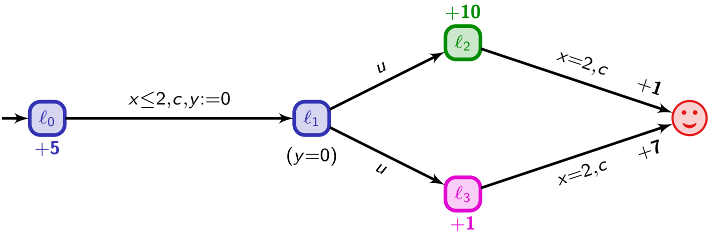


	ℓ_0	$\xrightarrow{1.3}$	ℓ_0	$\xrightarrow{c}$	ℓ_1	$\xrightarrow{u}$	ℓ_3	$\xrightarrow{0.7}$	ℓ_3	$\xrightarrow{c}$	☺
x	0		1.3		1.3		1.3		2		
y	0		1.3		0		0		0.7		

cost : 6.5 $+$ 0

Timed automata with costs (or energy information)

[Alur *et al*, Larsen *et al* 2001]

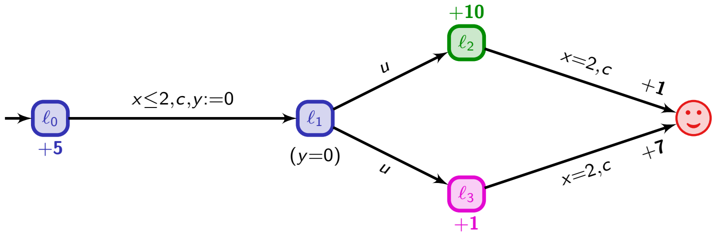


$$
\begin{array}{ccccccccccccc}
 & \ell_0 & \xrightarrow{1.3} & \ell_0 & \xrightarrow{c} & \ell_1 & \xrightarrow{u} & \ell_3 & \xrightarrow{0.7} & \ell_3 & \xrightarrow{c} & ☺ \\
x & 0 & & 1.3 & & 1.3 & & 1.3 & & 2 & & \\
y & 0 & & 1.3 & & 0 & & 0 & & 0.7 & &
\end{array}
$$

cost : 6.5 + 0 + 0

Timed automata with costs (or energy information)

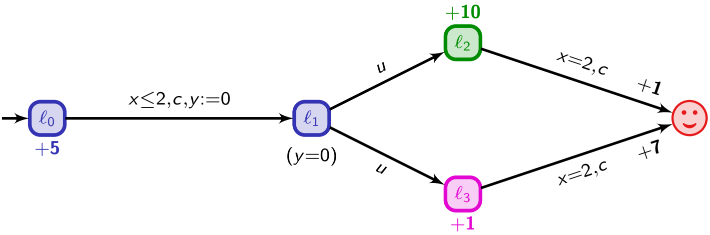
[Alur *et al*, Larsen *et al* 2001]



$$
\begin{array}{lcccccccccccc}
 & \ell_0 & \xrightarrow{1.3} & \ell_0 & \xrightarrow{c} & \ell_1 & \xrightarrow{u} & \ell_3 & \xrightarrow{0.7} & \ell_3 & \xrightarrow{c} & ☺ \\
x & 0 & & 1.3 & & 1.3 & & 1.3 & & 2 & & \\
y & 0 & & 1.3 & & 0 & & 0 & & 0.7 & & \\
\text{cost :} & & 6.5 & + & 0 & + & 0 & + & 0.7 & & &
\end{array}
$$

Timed automata with costs (or energy information)

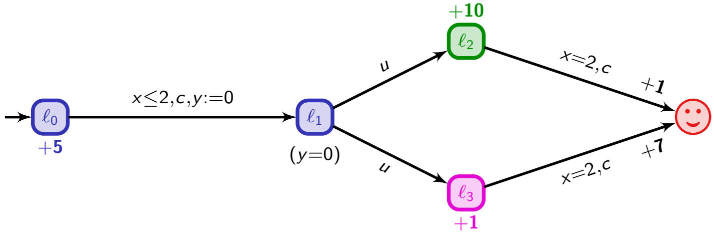
[Alur *et al*, Larsen *et al* 2001]



	ℓ_0	$\xrightarrow{1.3}$	ℓ_0	$\xrightarrow{c}$	ℓ_1	$\xrightarrow{u}$	ℓ_3	$\xrightarrow{0.7}$	ℓ_3	$\xrightarrow{c}$	☺
x	0		1.3		1.3		1.3		2		
y	0		1.3		0		0		0.7		
cost :		6.5	+	0	+	0	+	0.7	+	7	

Timed automata with costs (or energy information)

[Alur *et al*, Larsen *et al* 2001]

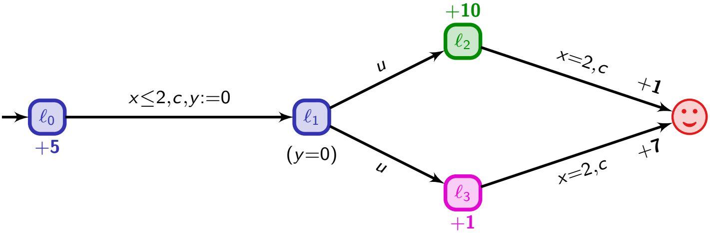


	ℓ_0	$\xrightarrow{1.3}$	ℓ_0	$\xrightarrow{c}$	ℓ_1	$\xrightarrow{u}$	ℓ_3	$\xrightarrow{0.7}$	ℓ_3	$\xrightarrow{c}$	☺
x	0		1.3		1.3		1.3		2		
y	0		1.3		0		0		0.7		

cost : $6.5 + 0 + 0 + 0.7 + 7 = 14.2$

Timed automata with costs (or energy information)

[Alur *et al*, Larsen *et al* 2001]

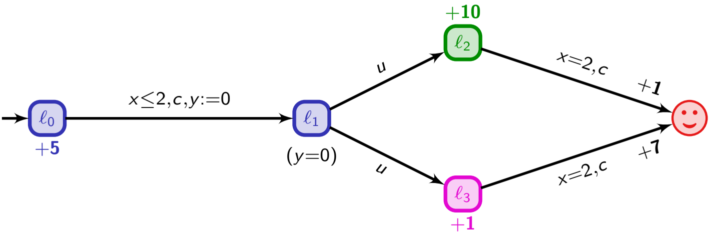


Question

What is the optimal cost for reaching ☺ ?

Timed automata with costs (or energy information)

[Alur *et al*, Larsen *et al* 2001]



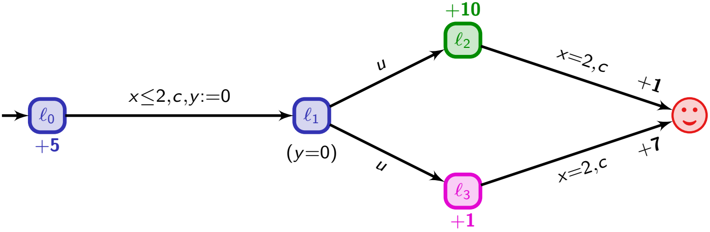
Question

What is the optimal cost for reaching 🙂?

$$5t + 10(2 - t) + 1$$

Timed automata with costs (or energy information)

[Alur *et al*, Larsen *et al* 2001]



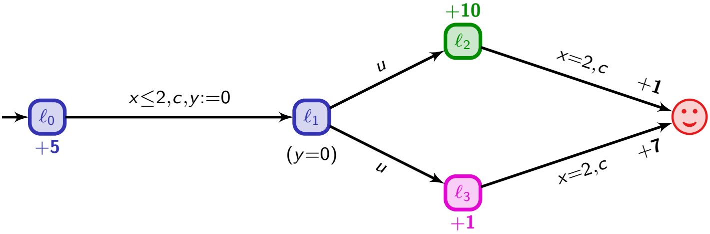
Question

What is the optimal cost for reaching 🙂?

$$5t + 10(2-t) + 1 \ , \ 5t + (2-t) + 7$$

Timed automata with costs (or energy information)

[Alur *et al*, Larsen *et al* 2001]



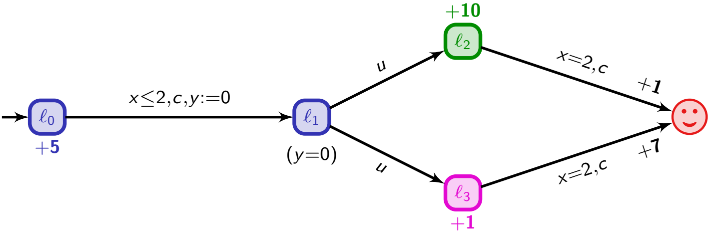
Question

What is the optimal cost for reaching ☺?

$$\min\ (\ 5t + 10(2-t) + 1\ ,\ 5t + (2-t) + 7\ )$$

Timed automata with costs (or energy information)

[Alur *et al*, Larsen *et al* 2001]



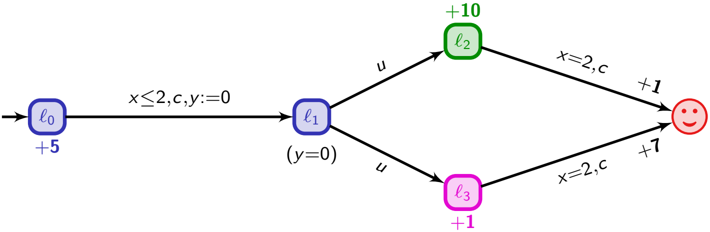
Question

What is the optimal cost for reaching 🙂 ?

$$\inf_{0 \le t \le 2} \min \left(5t + 10(2-t) + 1 \,,\; 5t + (2-t) + 7 \right) = 9$$

Timed automata with costs (or energy information)

[Alur *et al*, Larsen *et al* 2001]



Question

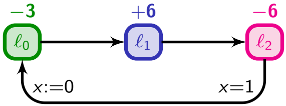
What is the optimal cost for reaching ☺?

$$\inf_{0 \leq t \leq 2} \min \left(5t + 10(2-t) + 1 \,,\; 5t + (2-t) + 7 \right) = 9$$

$\rightsquigarrow$ **strategy:** leave immediately ℓ_0, go to ℓ_3, and wait there 2 t.u.

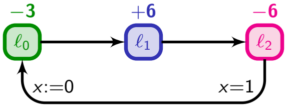
A further example with negative costs

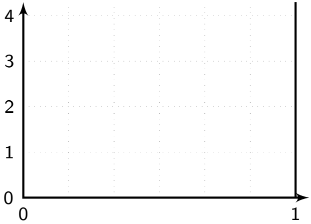
Globally $(x \leq 1)$



A further example with negative costs

Globally ($x \leq 1$)

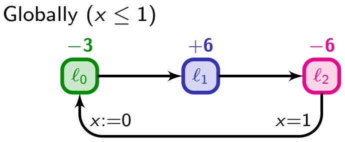


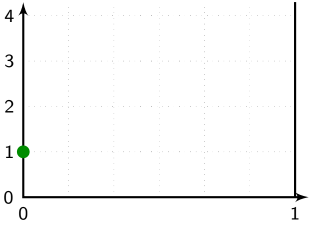


Safe bounds problems

- Lower-bound problem: can we stay above 0?

A further example with negative costs

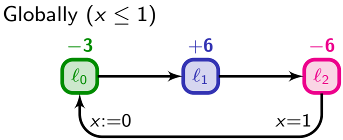


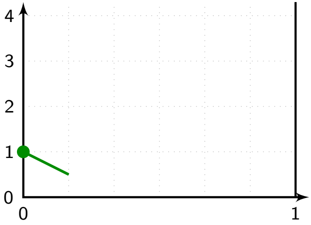


Safe bounds problems

- Lower-bound problem: can we stay above 0?

A further example with negative costs

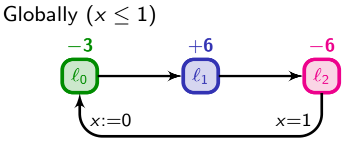


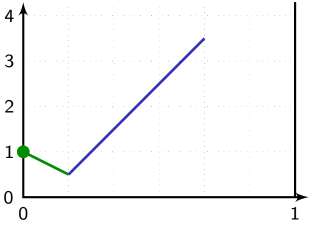


Safe bounds problems

- Lower-bound problem: can we stay above 0?

A further example with negative costs

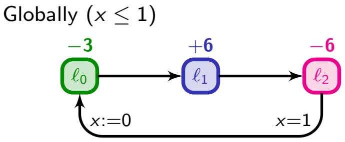


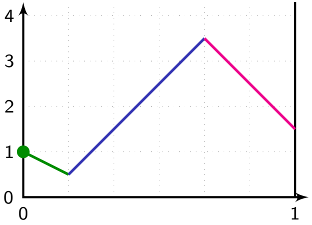


Safe bounds problems

- Lower-bound problem: can we stay above 0?

A further example with negative costs

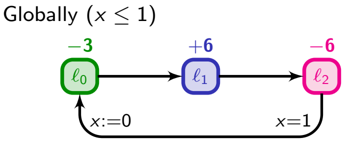


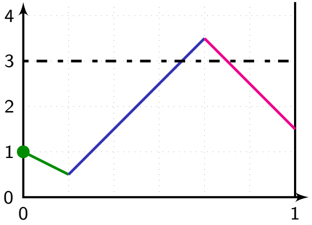


Safe bounds problems

- Lower-bound problem: can we stay above 0?

A further example with negative costs

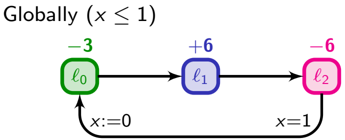


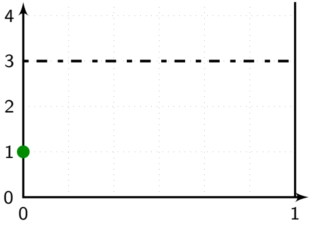


Safe bounds problems

- Lower-bound problem: can we stay above 0?

A further example with negative costs

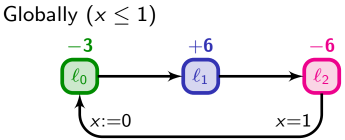


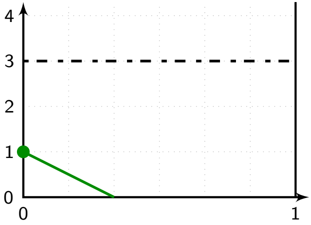


Safe bounds problems

- Lower-bound problem
- Lower-upper-bound problem: can we stay within bounds?

A further example with negative costs

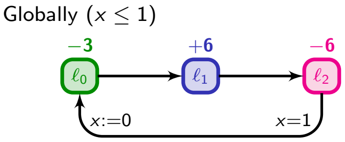


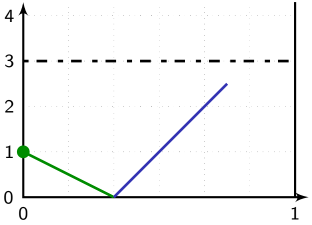


Safe bounds problems

- Lower-bound problem
- Lower-upper-bound problem: can we stay within bounds?

A further example with negative costs

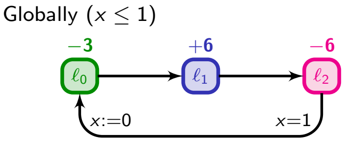


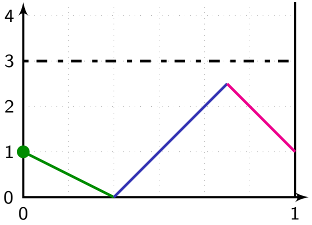


Safe bounds problems

- Lower-bound problem
- Lower-upper-bound problem: can we stay within bounds?

A further example with negative costs

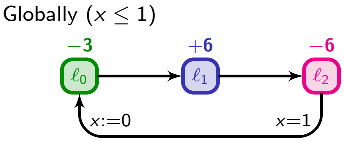


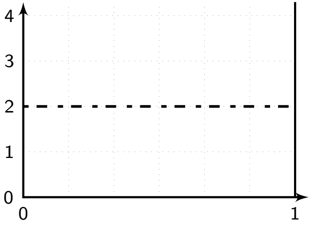


Safe bounds problems

- Lower-bound problem
- Lower-upper-bound problem: can we stay within bounds?

A further example with negative costs

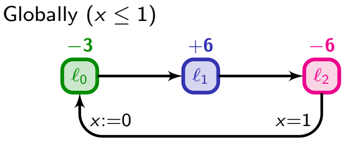


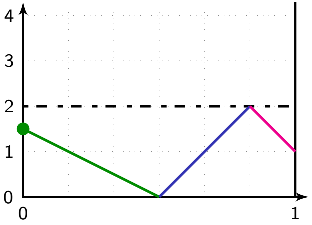


Safe bounds problems

- Lower-bound problem
- Lower-upper-bound problem: can we stay within bounds?

A further example with negative costs

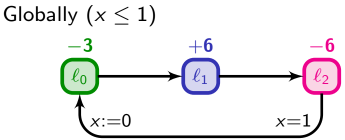


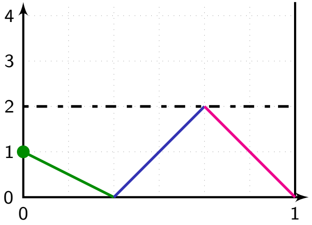


Safe bounds problems

- Lower-bound problem
- Lower-upper-bound problem: can we stay within bounds?

A further example with negative costs

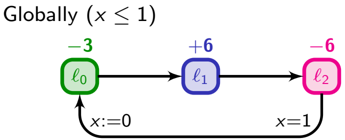


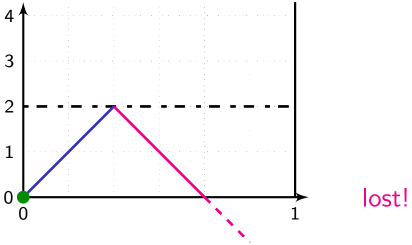


Safe bounds problems

- Lower-bound problem
- Lower-upper-bound problem: can we stay within bounds?

A further example with negative costs

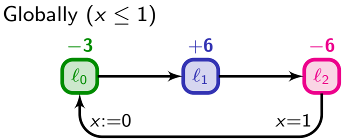


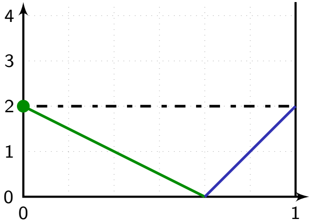


Safe bounds problems

- Lower-bound problem
- Lower-upper-bound problem: can we stay within bounds?

A further example with negative costs



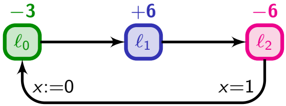


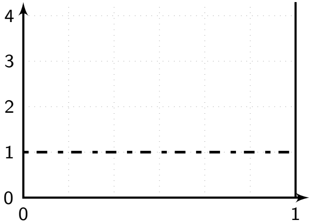
Safe bounds problems

- Lower-bound problem
- Lower-upper-bound problem: can we stay within bounds?

A further example with negative costs

Globally ($x \leq 1$)



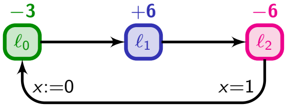


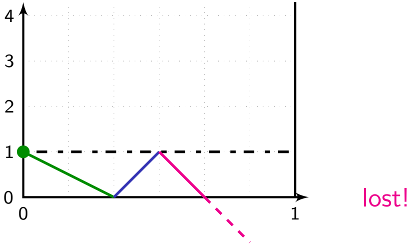
Safe bounds problems

- Lower-bound problem
- Lower-upper-bound problem: can we stay within bounds?

A further example with negative costs

Globally ($x \leq 1$)



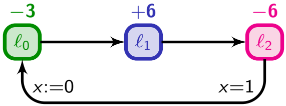


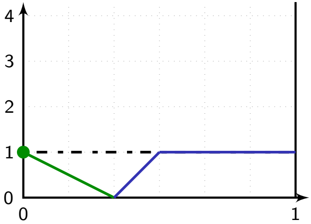
Safe bounds problems

- Lower-bound problem
- Lower-upper-bound problem: can we stay within bounds?

A further example with negative costs

Globally ($x \leq 1$)



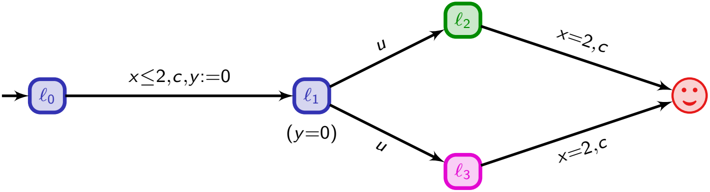


Safe bounds problems

- Lower-bound problem
- Lower-upper-bound problem
- Lower-weak-upper-bound problem: can we "weakly" stay within bounds?

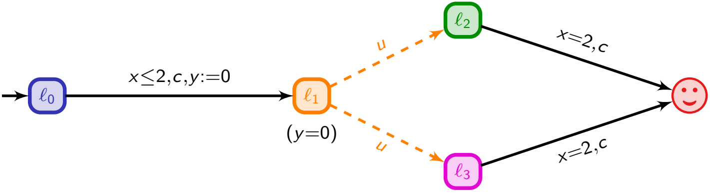
Games over timed automata

[Asarin, Maler, Pnueli, Sifakis 1998]



Games over timed automata

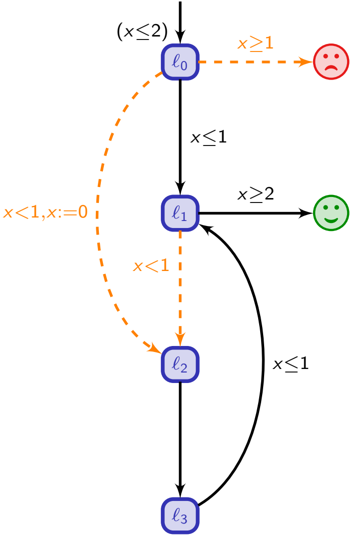
[Asarin, Maler, Pnueli, Sifakis 1998]



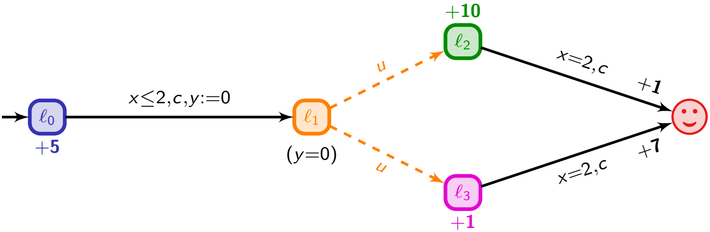
Question

Can we reach our goal whatever does the adversary?

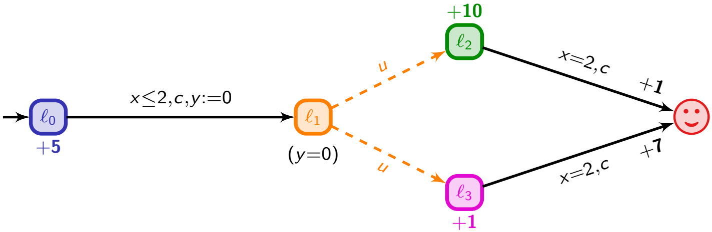
A further example



Games over timed automata with costs



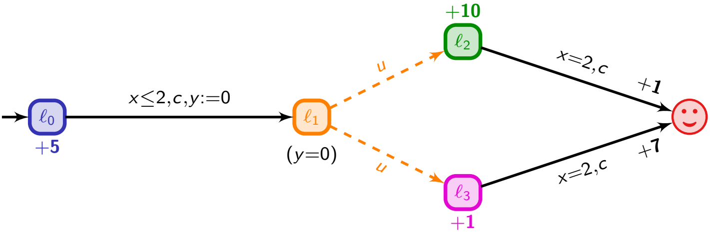
Games over timed automata with costs



Question

What is the optimal cost we can ensure from ℓ_0?

Games over timed automata with costs

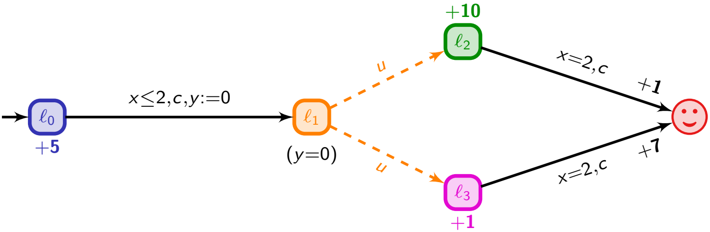


Question

What is the optimal cost we can ensure from ℓ_0?

$$5t + 10(2 - t) + 1$$

Games over timed automata with costs

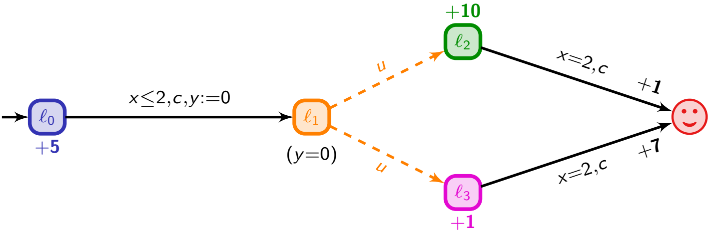


Question

What is the optimal cost we can ensure from ℓ_0?

$$5t + 10(2-t) + 1 \ , \ 5t + (2-t) + 7$$

Games over timed automata with costs

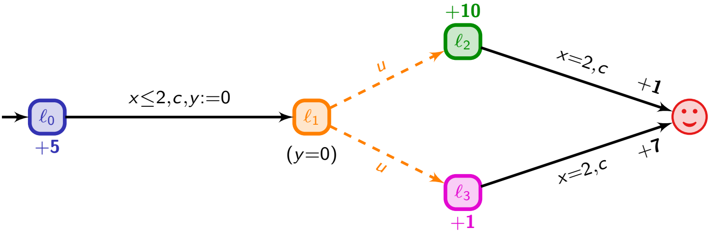


Question

What is the optimal cost we can ensure from ℓ_0?

$$\max\left(\ 5t + 10(2-t) + 1\ ,\ 5t + (2-t) + 7\ \right)$$

Games over timed automata with costs

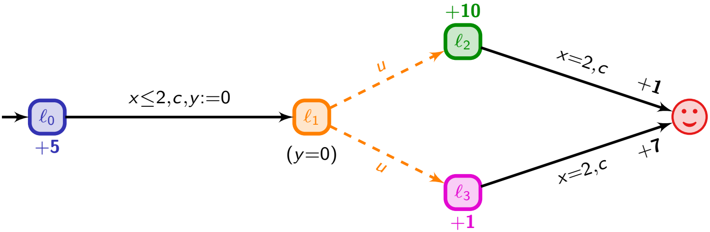


Question

What is the optimal cost we can ensure from ℓ_0?

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

Games over timed automata with costs



Question

What is the optimal cost we can ensure from ℓ_0?

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

$\rightsquigarrow$ **strategy:** wait in ℓ_0, and when $t = \frac{4}{3}$, go to ℓ_1

What can we model with those features?

- Timed automata: systems with constraints on delays between events, on durations of tasks, *etc*.

  "Is any message delivered in no more than 5 minutes?"

What can we model with those features?

- Timed automata: systems with constraints on delays between events, on durations of tasks, *etc*.

  "Is any message delivered in no more than 5 *minutes?"*

  - no real energy constraints can be expressed

What can we model with those features?

- Timed automata: systems with constraints on delays between events, on durations of tasks, *etc*.

  "Is any message delivered in no more than 5 *minutes?"*

  - no real energy constraints can be expressed

- Timed automata with costs: energy consumption, resources

  $\rightsquigarrow$ observe the quality of the system

What can we model with those features?

- Timed automata: systems with constraints on delays between events, on durations of tasks, *etc*.

  "Is any message delivered in no more than 5 minutes?"

  - no real energy constraints can be expressed

- Timed automata with costs: energy consumption, resources

  $\rightsquigarrow$ observe the quality of the system

  - Optimization questions: minimal energy consumption, mean-cost optimization, minimization of the resources

    "Can we minimize the power consumption w.r.t. the production?"

What can we model with those features?

- Timed automata: systems with constraints on delays between events, on durations of tasks, *etc*.

  "Is any message delivered in no more than 5 *minutes?"*

  - no real energy constraints can be expressed

- Timed automata with costs: energy consumption, resources

  $\rightsquigarrow$ observe the quality of the system

  - Optimization questions: minimal energy consumption, mean-cost optimization, minimization of the resources

    "Can we minimize the power consumption w.r.t. the production?"

  - Safe bounds constraints: check whether a system can stay alive with some amount of energy (that can possibly be regained)
    ex: laptop battery, autonomous robot

What can we model with those features?

- Timed automata: systems with constraints on delays between events, on durations of tasks, *etc*.

  "Is any message delivered in no more than 5 minutes?"

  - no real energy constraints can be expressed

- Timed automata with costs: energy consumption, resources

  $\rightsquigarrow$ observe the quality of the system

  - Optimization questions: minimal energy consumption, mean-cost optimization, minimization of the resources

    "Can we minimize the power consumption w.r.t. the production?"

  - Safe bounds constraints: check whether a system can stay alive with some amount of energy (that can possibly be regained)

    ex: laptop battery, autonomous robot

- Games over timed automata: interaction with an environment *(open systems)*

What can we model with those features?

- Timed automata: systems with constraints on delays between events, on durations of tasks, *etc*.

  "Is any message delivered in no more than 5 minutes?"

  - no real energy constraints can be expressed

- Timed automata with costs: energy consumption, resources

  $\rightsquigarrow$ observe the quality of the system

  - Optimization questions: minimal energy consumption, mean-cost optimization, minimization of the resources

    "Can we minimize the power consumption w.r.t. the production?"

  - Safe bounds constraints: check whether a system can stay alive with some amount of energy (that can possibly be regained)
    ex: laptop battery, autonomous robot

- Games over timed automata: interaction with an environment *(open systems)*

- Games over timed automata with costs: when the above-mentioned features are combined

Which are the results?

A taste of the results

- ☹ Adding cost (observer) variables to timed automata incredibly increases the difficulty of the problems
  - Many problems become undecidable
  - (Proofs of) algorithms become pretty much complex for restrictive decidable cases

Which are the results?

A taste of the results

- ☹ Adding cost (observer) variables to timed automata incredibly increases the difficulty of the problems
  - Many problems become undecidable
  - (Proofs of) algorithms become pretty much complex for restrictive decidable cases
- ☺ In several cases, algorithms have been developed, and case studies have been handled.

Which are the results?

A taste of the results

☹ Adding cost (observer) variables to timed automata incredibly increases the difficulty of the problems

- Many problems become undecidable
- (Proofs of) algorithms become pretty much complex for restrictive decidable cases

☺ In several cases, algorithms have been developed, and case studies have been handled.

Tools that we use

- Automata theory
- Fixpoint computation
- Game reasoning
- Abstractions
- Linear programming
- *etc*...

How does this theory apply?

Various tools are being developed

- Hybrid systems: HyTech — since 1995
- Timed automata: Uppaal — since 1995
- Timed automata with costs: Uppaal Cora — since 2001
- Games on timed automata: Uppaal Tiga — since 2005

How does this theory apply?

Various tools are being developed

- Hybrid systems: HyTech — since 1995
- Timed automata: Uppaal — since 1995
- Timed automata with costs: Uppaal Cora — since 2001
- Games on timed automata: Uppaal Tiga — since 2005

Case studies (a selection)

- Purely timed systems:
  - An audio/video protocol (Bang & Olufsen) — 1997
  - Verification of SPSMALL (STMicroelectronics) — 2008

How does this theory apply?

Various tools are being developed

- Hybrid systems: HyTech — since 1995
- Timed automata: Uppaal — since 1995
- Timed automata with costs: Uppaal Cora — since 2001
- Games on timed automata: Uppaal Tiga — since 2005

Case studies (a selection)

- Purely timed systems:
  - An audio/video protocol (Bang & Olufsen) — 1997
  - Verification of SPSMALL (STMicroelectronics) — 2008
- Games on timed automata:
  - A climate controller in a pig stable (Skov A/S) — 2007

How does this theory apply?

Various tools are being developed

- Hybrid systems: HyTech — since 1995
- Timed automata: Uppaal — since 1995
- Timed automata with costs: Uppaal Cora — since 2001
- Games on timed automata: Uppaal Tiga — since 2005

Case studies (a selection)

- Purely timed systems:
  - An audio/video protocol (Bang & Olufsen) — 1997
  - Verification of SPSMALL (STMicroelectronics) — 2008
- Games on timed automata:
  - A climate controller in a pig stable (Skov A/S) — 2007
- Timed automata with costs:
  - *Optimization questions* (EU project Ametist)
    A lacquer production planning problem (AXXOM) — 2004

How does this theory apply?

Various tools are being developed

- Hybrid systems: HyTech — since 1995
- Timed automata: Uppaal — since 1995
- Timed automata with costs: Uppaal Cora — since 2001
- Games on timed automata: Uppaal Tiga — since 2005

Case studies (a selection)

- Purely timed systems:
  - An audio/video protocol (Bang & Olufsen) — 1997
  - Verification of SPSMALL (STMicroelectronics) — 2008
- Games on timed automata:
  - A climate controller in a pig stable (Skov A/S) — 2007
- Timed automata with costs:
  - *Optimization questions* (EU project Ametist)
    A lacquer production planning problem (AXXOM) — 2004
  - *Safe bounds constraints* (EU project Quasimodo)
    A pump system (Hydac Electronic GmbH) — *theory not yet understood*