Execution-time opacity control for timed automata

GT SCALP / Vérification 2024

IRCICA

É. André[1], M. Duflot[2], **Laetitia Laversa**[3], E. Lefaucheux[2]

[1]LIPN, Université Sorbonne Paris Nord
[2]LORIA, Université de Lorraine
[3]IRIF, Université Paris Cité

Context

- Ensure security of real time systems
- Side-channel attacks: using non-algorithmic weaknesses (timing information, power consumption, electromagnetic leakage, sound...)

Context

`pwd`	b a g u e t t e
`attempt`	b a g e l

Context

pwd	b	a	g	u	e	t	t	e
attempt	b	a	g	e	l			

Context

`pwd`	`b`	`a`	`g`	`u`	`e`	`t`	`t`	`e`
`attempt`	`b`	`a`	`g`	`e`	`l`			

Context

`pwd`	b	a	g	u	e	t	t	e
`attempt`	b	a	g	e	l			

Context

pwd	b	a	g	u	e	t	t	e
attempt	b	a	g	e	l			

Context

`pwd`	b	a	g	u	e	t	t	e
`attempt`	b	a	g	e	l			

→ Execution time is proportional to the number of consecutive correct characters.

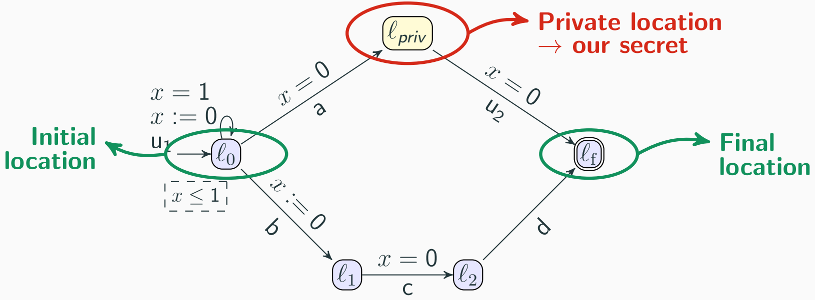
Context

- Ensure security of real time systems
- Side-channel attacks: using non-algorithmic weaknesses (timing information, power consumption, electromagnetic leakage, sound...)
- The attacker: external observer who only knows execution time
- Our objective: keep a secret

Model & Problem

Timed Automaton (TA)

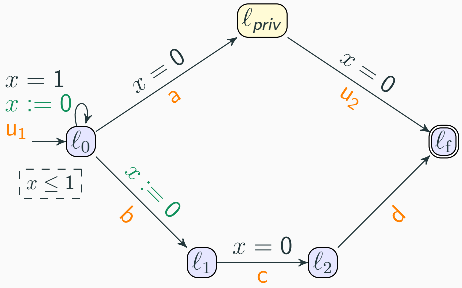
Timed automaton : finite automaton with clocks



Locations

Timed Automaton (TA)

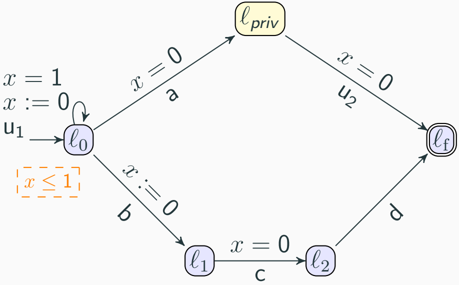
Timed automaton : finite automaton with clocks



Transitions: actions and reset

Timed Automaton (TA)

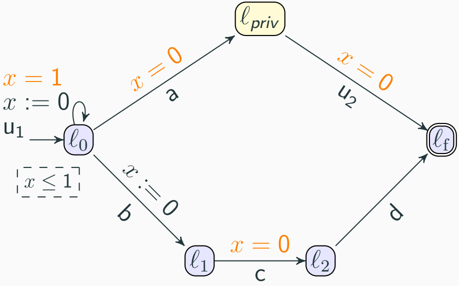
Timed automaton : finite automaton with clocks



Invariants

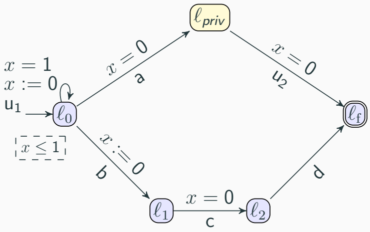
Timed Automaton (TA)

Timed automaton : finite automaton with clocks

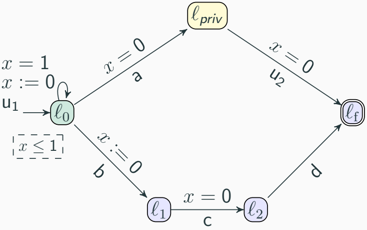


Guards

Timed automata and runs



Timed automata and runs



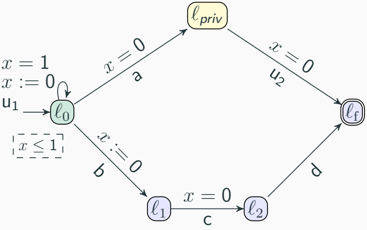
ℓ_0

$x = 0$

$t = 0$

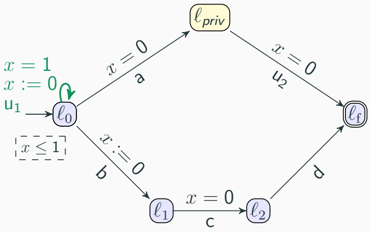
$$\rho_1 \quad = \quad (\ell_0, 0)$$

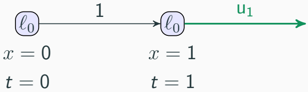
Timed automata and runs



$$\rho_1 \quad = \quad (\ell_0, 0)$$

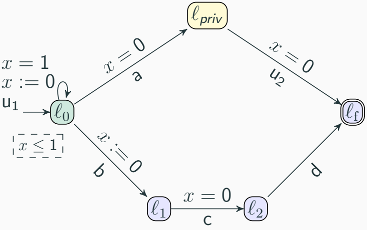
Timed automata and runs

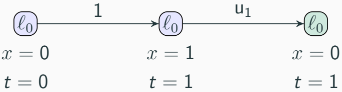




$$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1, u_1}$$

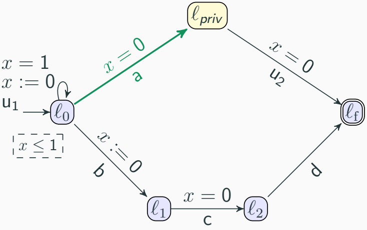
Timed automata and runs

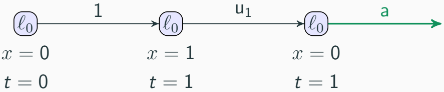




$$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1, u_1} (\ell_0, 0)$$

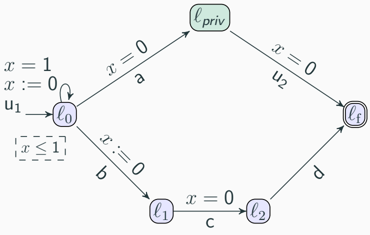
Timed automata and runs

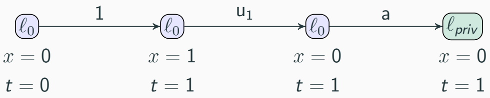




$$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1, u_1} (\ell_0, 0) \xrightarrow{0, a}$$

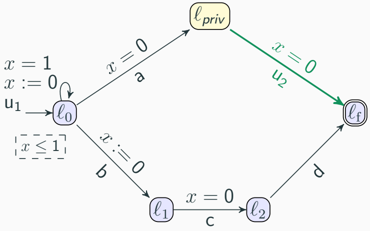
Timed automata and runs

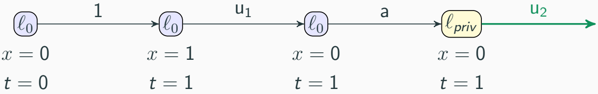




$$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1,u_1} (\ell_0, 0) \xrightarrow{0,a} (\ell_{priv}, 0)$$

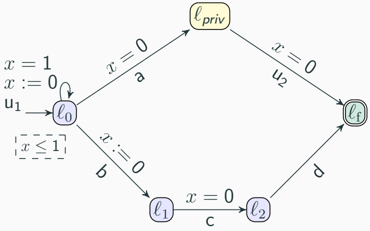
Timed automata and runs

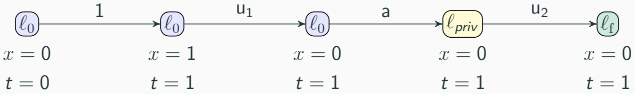




$$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1,u_1} (\ell_0, 0) \xrightarrow{0,a} (\ell_{priv}, 0) \xrightarrow{0,u_2}$$

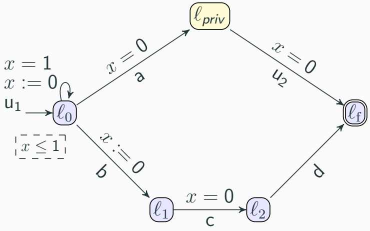
Timed automata and runs





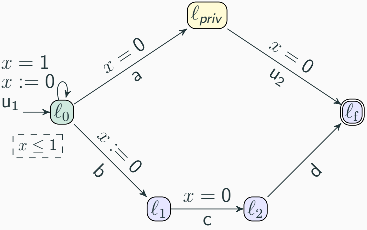
$$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1, u_1} (\ell_0, 0) \xrightarrow{0, a} (\ell_{priv}, 0) \xrightarrow{0, u_2} (\ell_f, 0) \qquad dur(\rho_1) = 1$$

Timed automata and runs



$$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1, u_1} (\ell_0, 0) \xrightarrow{0, a} (\ell_{priv}, 0) \xrightarrow{0, u_2} (\ell_f, 0) \qquad\qquad dur(\rho_1) = 1$$

Timed automata and runs



$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1,u_1} (\ell_0, 0) \xrightarrow{0,a} (\ell_{priv}, 0) \xrightarrow{0,u_2} (\ell_f, 0) \qquad dur(\rho_1) = 1$

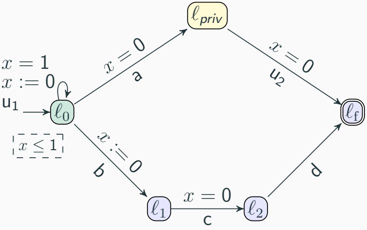
ℓ_0

$x = 0$

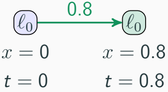
$t = 0$

$\rho_2 \quad = \quad (\ell_0, 0)$

Timed automata and runs

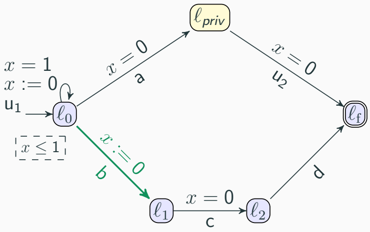


$$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1,u_1} (\ell_0, 0) \xrightarrow{0,a} (\ell_{priv}, 0) \xrightarrow{0,u_2} (\ell_f, 0) \qquad dur(\rho_1) = 1$$

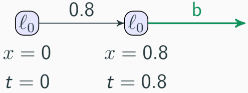


$$\rho_2 \quad = \quad (\ell_0, 0)$$

Timed automata and runs

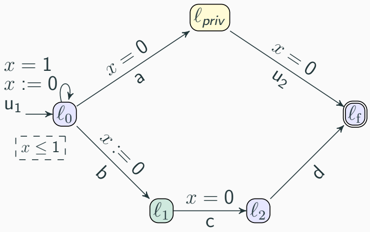


$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1,u_1} (\ell_0, 0) \xrightarrow{0,a} (\ell_{priv}, 0) \xrightarrow{0,u_2} (\ell_f, 0) \qquad dur(\rho_1) = 1$

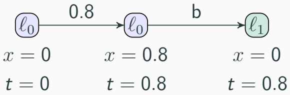


$\rho_2 \quad = \quad (\ell_0, 0) \xrightarrow{0.8,b}$

Timed automata and runs

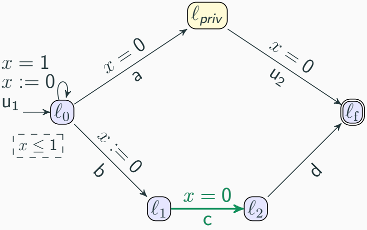


$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1, u_1} (\ell_0, 0) \xrightarrow{0, a} (\ell_{priv}, 0) \xrightarrow{0, u_2} (\ell_f, 0) \qquad dur(\rho_1) = 1$

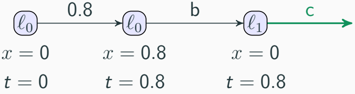


$\rho_2 \quad = \quad (\ell_0, 0) \xrightarrow{0.8, b} (\ell_1, 0)$

Timed automata and runs

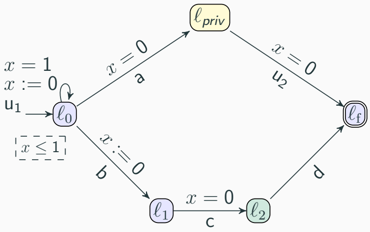


$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1, u_1} (\ell_0, 0) \xrightarrow{0, a} (\ell_{priv}, 0) \xrightarrow{0, u_2} (\ell_f, 0) \qquad dur(\rho_1) = 1$

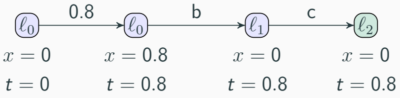


$\rho_2 \quad = \quad (\ell_0, 0) \xrightarrow{0.8, b} (\ell_1, 0) \xrightarrow{0, c}$

Timed automata and runs

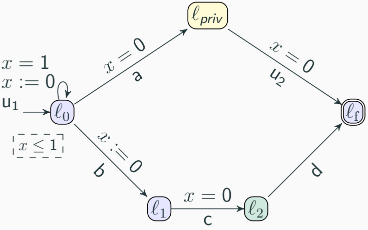


$$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1, u_1} (\ell_0, 0) \xrightarrow{0, a} (\ell_{priv}, 0) \xrightarrow{0, u_2} (\ell_f, 0) \qquad dur(\rho_1) = 1$$

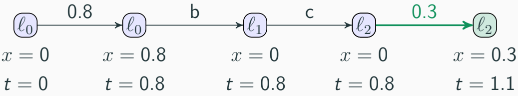


$$\rho_2 \quad = \quad (\ell_0, 0) \xrightarrow{0.8, b} (\ell_1, 0) \xrightarrow{0, c} (\ell_2, 0)$$

Timed automata and runs

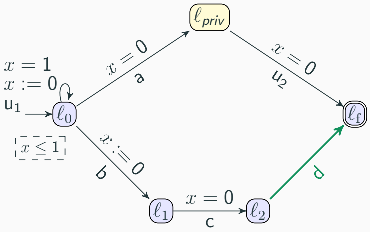


$$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1,u_1} (\ell_0, 0) \xrightarrow{0,a} (\ell_{priv}, 0) \xrightarrow{0,u_2} (\ell_f, 0) \qquad dur(\rho_1) = 1$$



$$\rho_2 \quad = \quad (\ell_0, 0) \xrightarrow{0.8,b} (\ell_1, 0) \xrightarrow{0,c} (\ell_2, 0)$$

Timed automata and runs



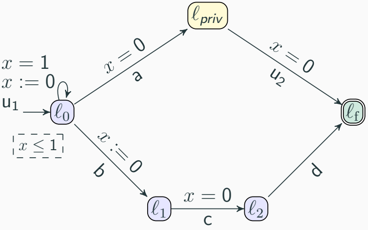
$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1, u_1} (\ell_0, 0) \xrightarrow{0, a} (\ell_{priv}, 0) \xrightarrow{0, u_2} (\ell_f, 0) \qquad dur(\rho_1) = 1$

$$\ell_0 \xrightarrow{0.8} \ell_0 \xrightarrow{b} \ell_1 \xrightarrow{c} \ell_2 \xrightarrow{0.3} \ell_2 \xrightarrow{d}$$

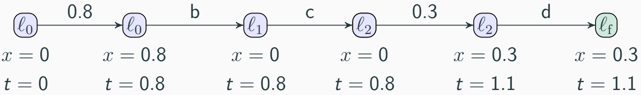
$x = 0$	$x = 0.8$	$x = 0$	$x = 0$	$x = 0.3$
$t = 0$	$t = 0.8$	$t = 0.8$	$t = 0.8$	$t = 1.1$

$\rho_2 \quad = \quad (\ell_0, 0) \xrightarrow{0.8, b} (\ell_1, 0) \xrightarrow{0, c} (\ell_2, 0) \xrightarrow{0.3, d}$

Timed automata and runs

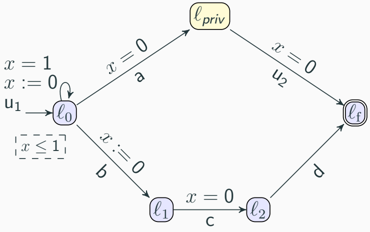


$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1, u_1} (\ell_0, 0) \xrightarrow{0, a} (\ell_{priv}, 0) \xrightarrow{0, u_2} (\ell_f, 0) \qquad dur(\rho_1) = 1$

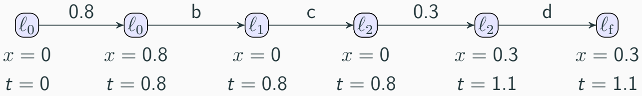


$\rho_2 \quad = \quad (\ell_0, 0) \xrightarrow{0.8, b} (\ell_1, 0) \xrightarrow{0, c} (\ell_2, 0) \xrightarrow{0.3, d} (\ell_f, 0.3)$

Timed automata and runs

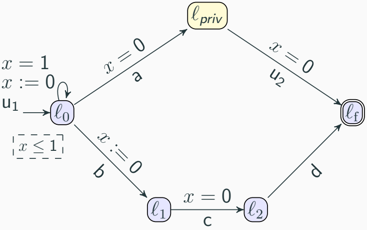


$$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1, u_1} (\ell_0, 0) \xrightarrow{0, a} (\ell_{priv}, 0) \xrightarrow{0, u_2} (\ell_f, 0) \qquad dur(\rho_1) = 1$$



$$\rho_2 \quad = \quad (\ell_0, 0) \xrightarrow{0.8, b} (\ell_1, 0) \xrightarrow{0, c} (\ell_2, 0) \xrightarrow{0.3, d} (\ell_f, 0.3) \qquad dur(\rho_2) = 1.1$$

Timed automata and runs



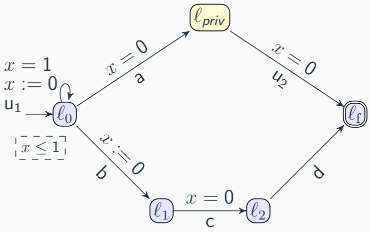
$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1,u_1} (\ell_0, 0) \xrightarrow{0,a} (\ell_{priv}, 0) \xrightarrow{0,u_2} (\ell_f, 0) \qquad dur(\rho_1) = 1$

Private run

$\rho_2 \quad = \quad (\ell_0, 0) \xrightarrow{0.8,b} (\ell_1, 0) \xrightarrow{0,c} (\ell_2, 0) \xrightarrow{0.3,d} (\ell_f, 0.3) \qquad dur(\rho_2) = 1.1$

Public run

Timed automata and runs



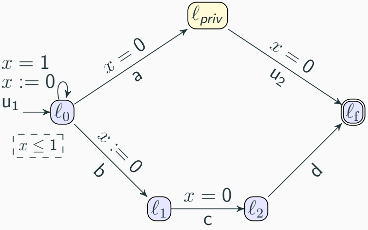
$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1,u_1} (\ell_0, 0) \xrightarrow{0,a} (\ell_{priv}, 0) \xrightarrow{0,u_2} (\ell_f, 0) \qquad dur(\rho_1) = 1$

Private run (visiting ℓ_{priv})

$\rho_2 \quad = \quad (\ell_0, 0) \xrightarrow{0.8,b} (\ell_1, 0) \xrightarrow{0,c} (\ell_2, 0) \xrightarrow{0.3,d} (\ell_f, 0.3) \qquad dur(\rho_2) = 1.1$

Public run (avoiding ℓ_{priv})

Timed automata and runs



$\rho_1 \quad = \quad (\ell_0, 0) \xrightarrow{1, u_1} (\ell_0, 0) \xrightarrow{0, a} (\ell_{priv}, 0) \xrightarrow{0, u_2} (\ell_f, 0)$ $\quad dur(\rho_1) = 1$

Private run (visiting ℓ_{priv})

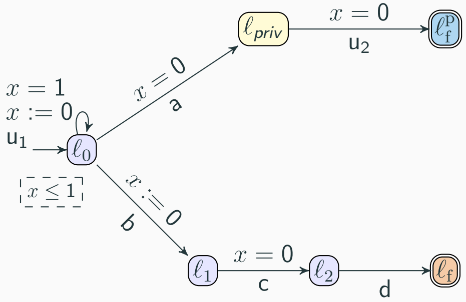
Private duration

$\rho_2 \quad = \quad (\ell_0, 0) \xrightarrow{0.8, b} (\ell_1, 0) \xrightarrow{0, c} (\ell_2, 0) \xrightarrow{0.3, d} (\ell_f, 0.3)$ $\quad dur(\rho_2) = 1.1$

Public run (avoiding ℓ_{priv})

Public duration

Duplicated Timed Automaton



Last location is sufficient to discriminate private and public runs.

Execution-time opacity

Private durations	=	Public durations

Execution-time opacity

Private durations = **Public durations**

Is a given system opaque? Decidable[1]

[1] *Configuring Timing Parameters to Ensure Execution-Time Opacity in Timed Automata*, André *et al.*, TiCSA 2023

Execution-time opacity control

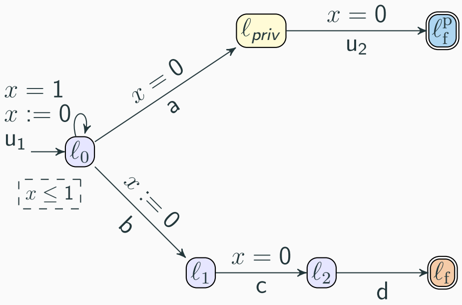
Private durations	=	Public durations

Is a given system opaque? Decidable[1]

→ **Can we make a given system opaque?**

[1] *Configuring Timing Parameters to Ensure Execution-Time Opacity in Timed Automata*, André *et al.*, TiCSA 2023

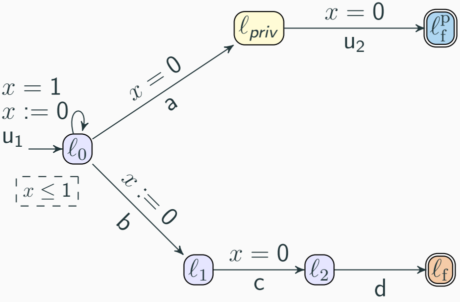
A strategy to make it opaque



Private durations

$\mathbb{N}$

A strategy to make it opaque



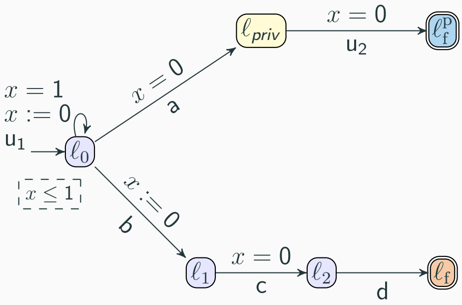
Private durations

$\mathbb{N}$

Public durations

$\mathbb{R}^+$

A strategy to make it opaque



Private durations

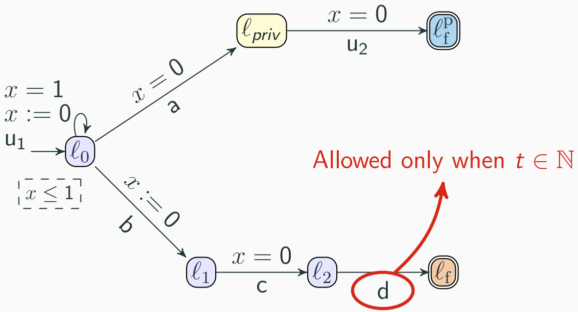
$\mathbb{N}$

Non-opaque

Public durations

$\mathbb{R}^+$

A strategy to make it opaque



Private durations

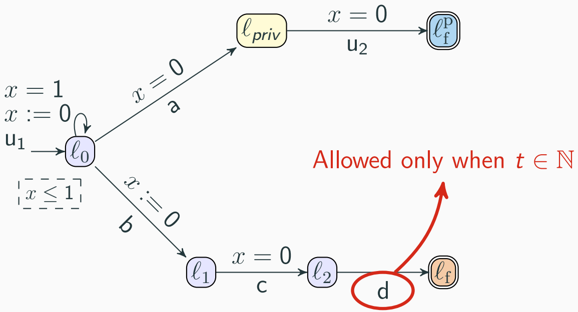
$\mathbb{N}$

Non-opaque

Public durations

$\mathbb{R}^+$

A strategy to make it opaque



Private durations

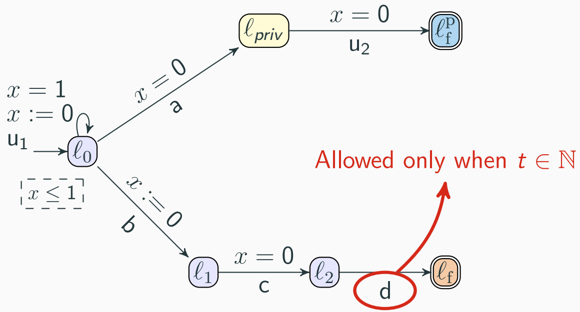
$\mathbb{N}$

Non-opaque

Public durations

~~$\mathbb{R}^+$~~ $\mathbb{N}$

A strategy to make it opaque



Private durations

$\mathbb{N}$

Opaque :-)

Public durations

~~$\mathbb{R}^+$~~ $\mathbb{N}$

Controller

Controllable / uncontrollable actions

In actions set:

- controllable actions:
  can be enabled and disabled at runtime
- uncontrollable actions: always available

Strategy

A function allowing at each time a set of possible actions

$$\sigma : \mathbb{R}_{\geq 0} \rightarrow 2^{\Sigma_c}$$

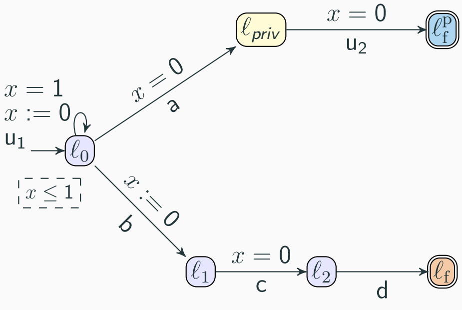
Controller

Actions

$\Sigma = \Sigma_c \uplus \Sigma_u$

$\Sigma_u = \{\mathsf{u}_1, \mathsf{u}_2\}$

$\Sigma_c = \{\mathsf{a},\ \mathsf{b},\ \mathsf{c},\ \mathsf{d}\}$



Strategy:

$$\sigma(\tau) = \begin{cases} \{\mathsf{a},\ \mathsf{b},\ \mathsf{c},\ \mathsf{d}\} & \text{for } \tau \in \mathbb{N} \\ \{\mathsf{a},\ \mathsf{b},\ \mathsf{c}\} & \text{for } \tau \in \mathbb{R} \setminus \mathbb{N} \end{cases}$$

Our approach

Our approach

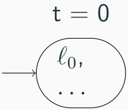
Intuition

Build an automaton where each state represents a set of reachable states at a given time.

Our approach

Intuition

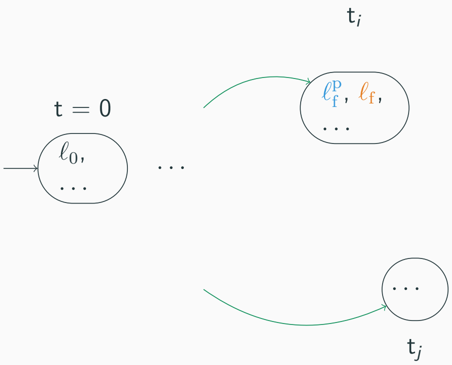
Build an automaton where each state represents a set of reachable states at a given time.



Our approach

Intuition

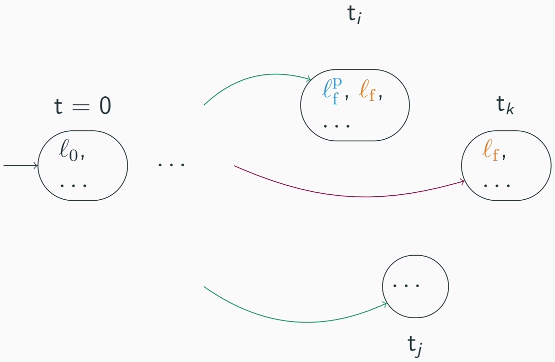
Build an automaton where each state represents a set of reachable states at a given time.



Our approach

Intuition

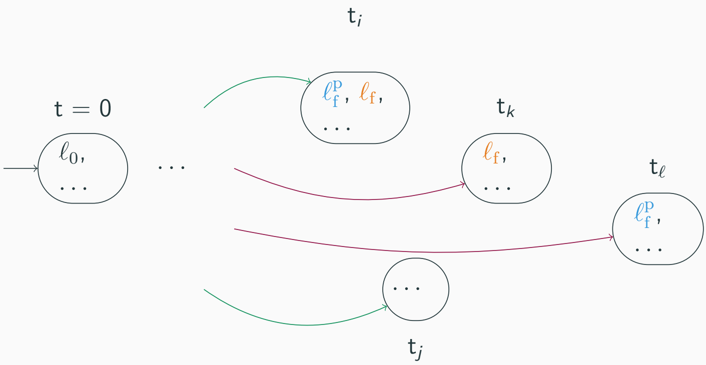
Build an automaton where each state represents a set of reachable states at a given time.



Our approach

Intuition

Build an automaton where each state represents a set of reachable states at a given time.

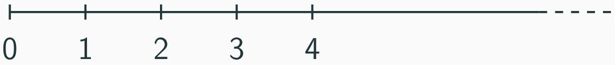


Region abstraction

Problem

Continuous time → Infinite number of configurations

Discretize the time



Region abstraction

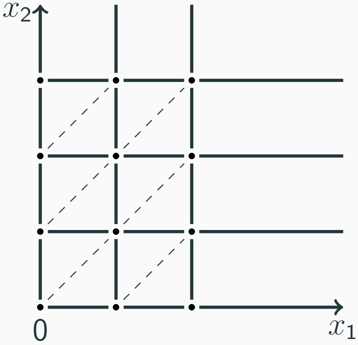
Problem

Continuous time $\rightarrow$ Infinite number of configurations

Discretize the time

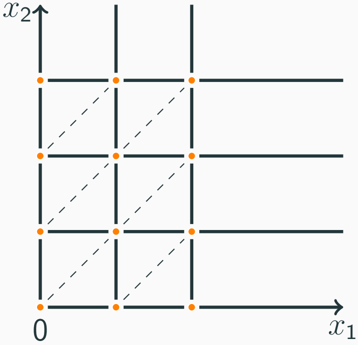
Region abstraction

With 2 clocks:



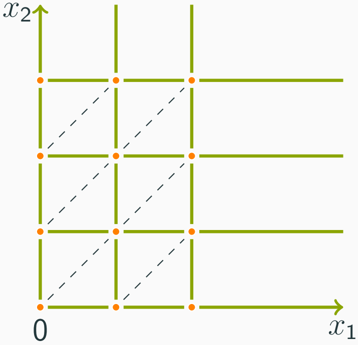
Region abstraction

With 2 clocks:



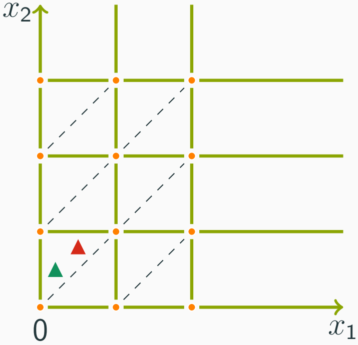
Region abstraction

With 2 clocks:



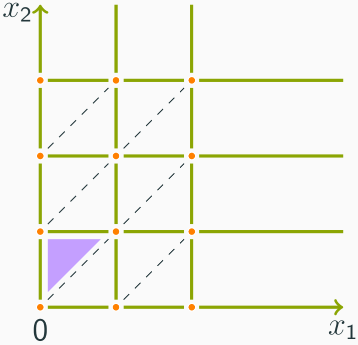
Region abstraction

With 2 clocks:



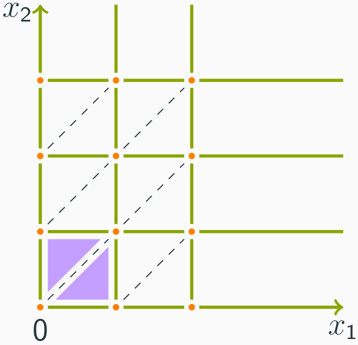
Region abstraction

With 2 clocks:



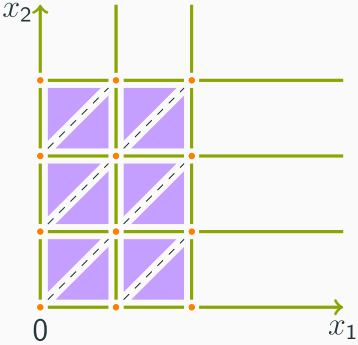
Region abstraction

With 2 clocks:



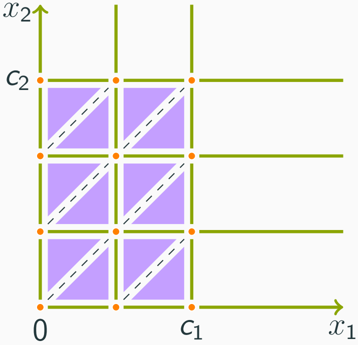
Region abstraction

With 2 clocks:



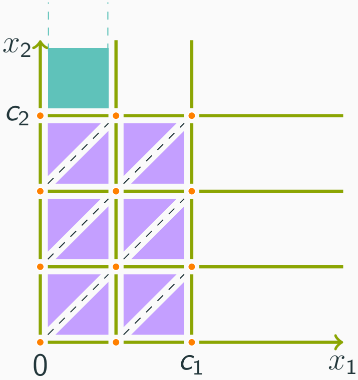
Region abstraction

With 2 clocks:



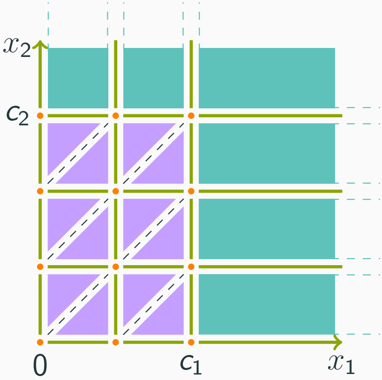
Region abstraction

With 2 clocks:



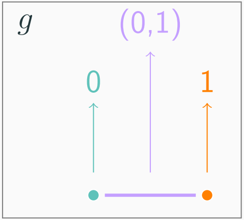
Region abstraction

With 2 clocks:



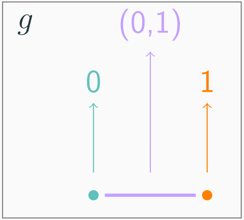
Abstraction of elapsed time

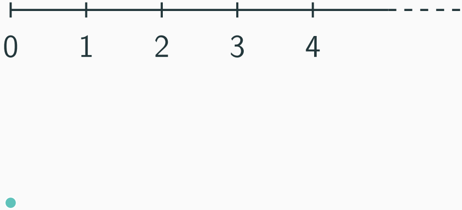
Add clock g that represents the global time.



Abstraction of elapsed time

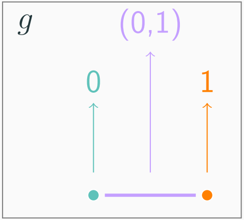
Add clock g that represents the global time.





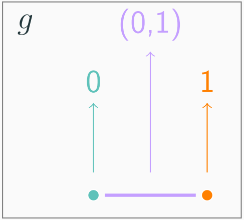
Abstraction of elapsed time

Add clock g that represents the global time.



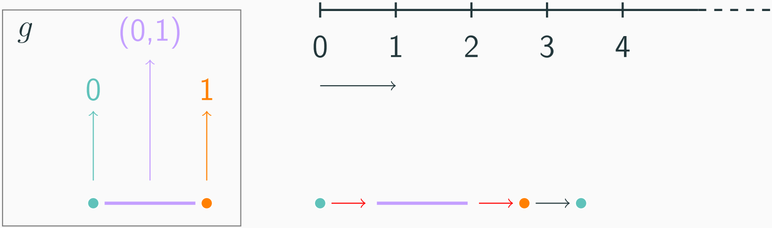
Abstraction of elapsed time

Add clock g that represents the global time.



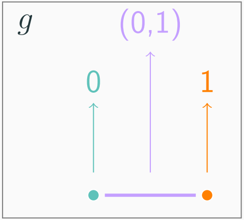
Abstraction of elapsed time

Add clock g that represents the global time.



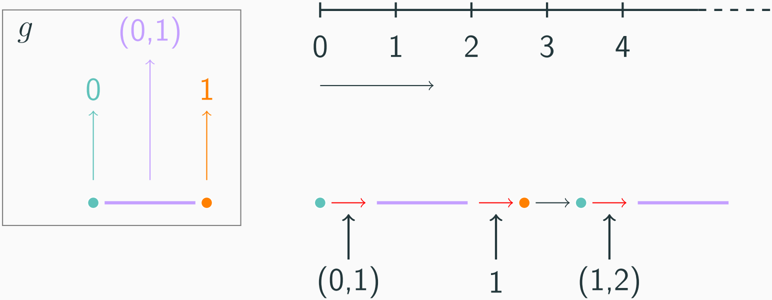
Abstraction of elapsed time

Add clock g that represents the global time.



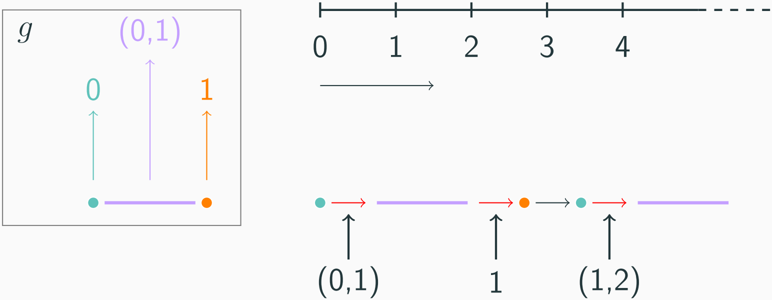
Abstraction of elapsed time

Add clock g that represents the global time.



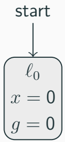
Abstraction of elapsed time

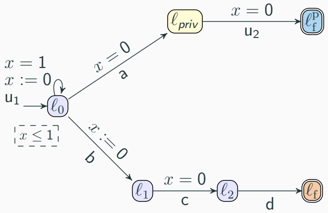
Add clock g that represents the global time.



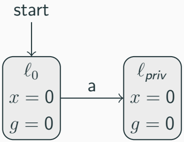
$\color{red}{\rightarrow\rightarrow}$ = 1 time unit

Region automaton with global time

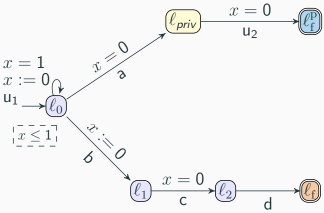




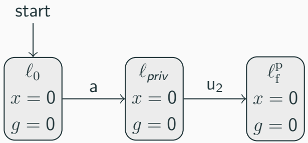
Region automaton with global time



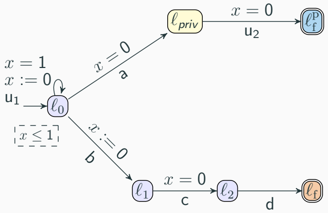
$\rightarrow$ no time



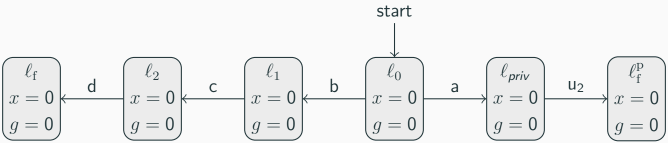
Region automaton with global time



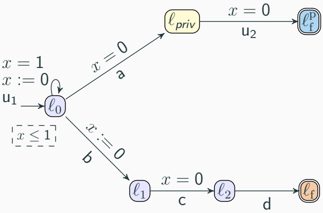
$\rightarrow$ no time



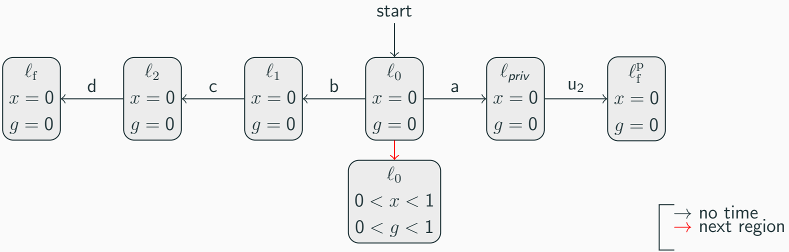
Region automaton with global time

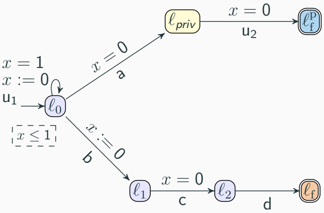


$\rightarrow$ no time

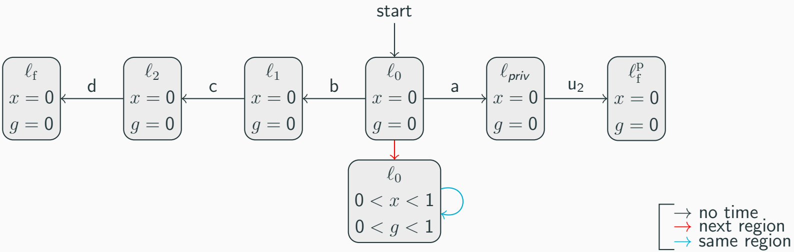


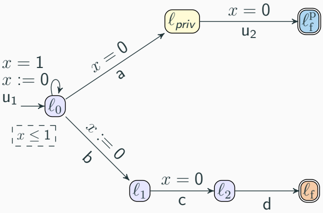
Region automaton with global time



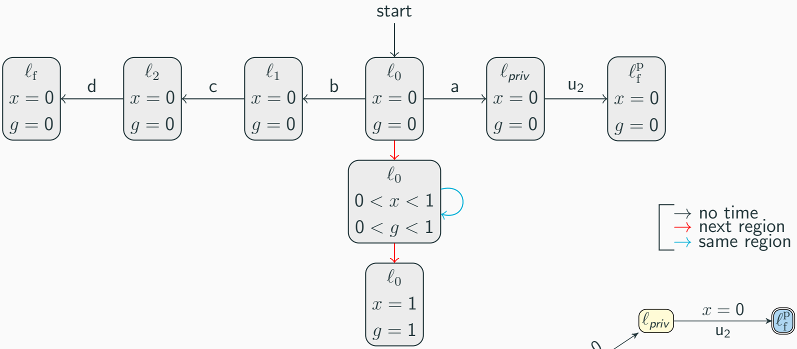


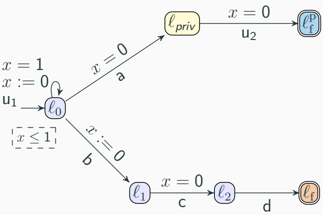
Region automaton with global time



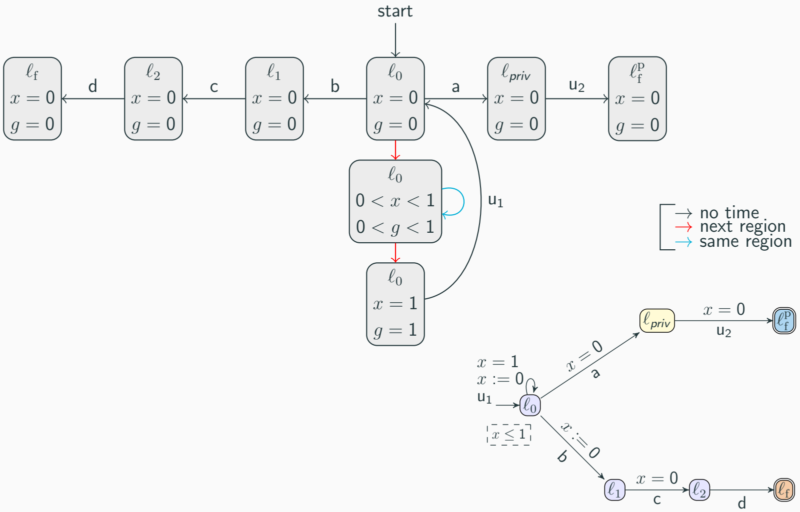


Region automaton with global time





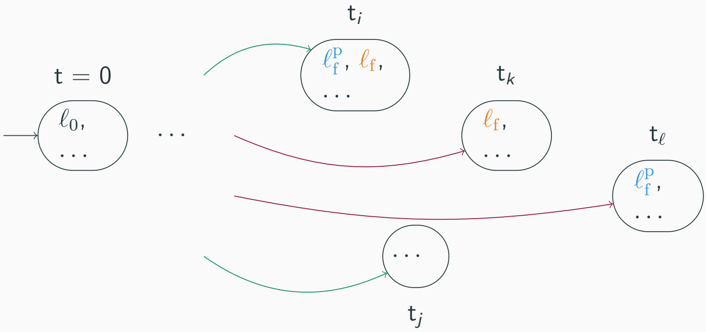
Region automaton with global time



Our approach

Intuition

Build an automaton where each **belief** represents a set of reachable states for a given time.



Beliefs

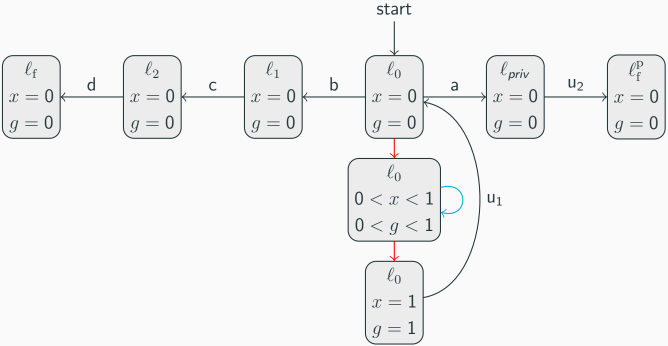
Belief

A belief is a set of regions.

Bad belief for opacity

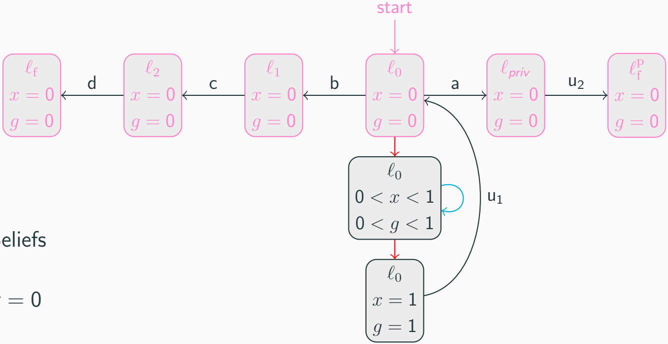
$\{\ell_{\mathrm{f}}, \ldots\}$ $\qquad$ $\{\ell_{\mathrm{f}}^{\mathrm{p}}, \ldots\}$

Beliefs



start
ℓ_f
$x = 0$
$g = 0$
d
ℓ_2
$x = 0$
$g = 0$
c
ℓ_1
$x = 0$
$g = 0$
b
ℓ_0
$x = 0$
$g = 0$
a
ℓ_{priv}
$x = 0$
$g = 0$
u_2
ℓ_f^p
$x = 0$
$g = 0$
ℓ_0
$0 < x < 1$
$0 < g < 1$
u_1
ℓ_0
$x = 1$
$g = 1$

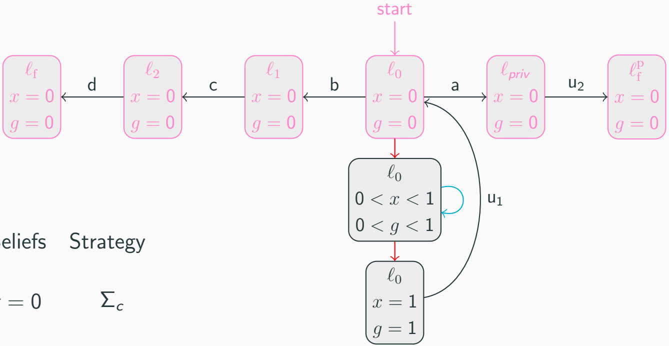
Beliefs



Beliefs

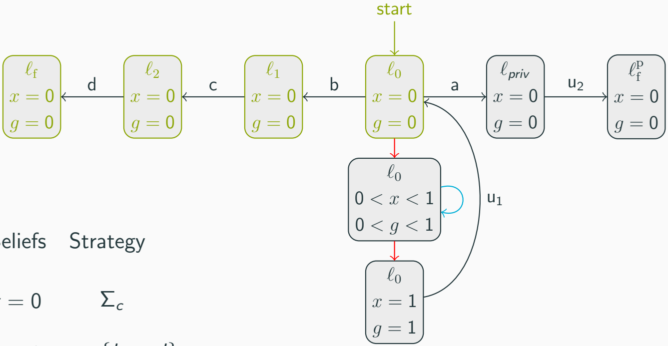
B_0 $\quad t = 0$

Beliefs



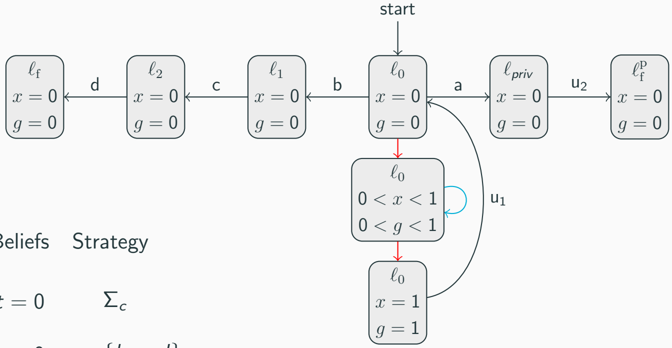
	Beliefs	Strategy
${B_0}^{\Sigma_c}$	$t=0$	Σ_c

Beliefs



	Beliefs	Strategy
${B_0}^{\Sigma_c}$	$t = 0$	Σ_c
$B_0^{\{b,c,d\}}$	$t = 0$	$\{b, c, d\}$

Beliefs



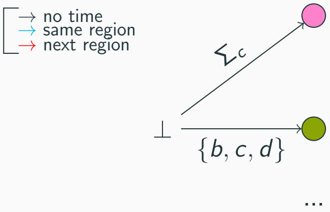
	Beliefs	Strategy
$B_0^{\Sigma_c}$	$t = 0$	Σ_c
$B_0^{\{b,c,d\}}$	$t = 0$	$\{b, c, d\}$
	...	

Beliefs depend on the available actions and the past.

Automaton of beliefs

An automaton where:

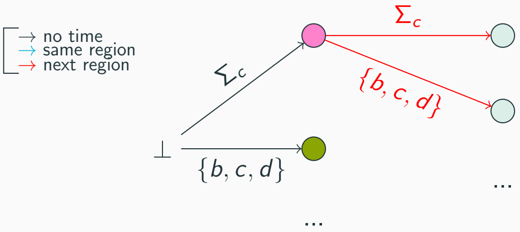
- each *state*: a belief
- each *transition*: a strategy and an elapsed time



Automaton of beliefs

An automaton where:

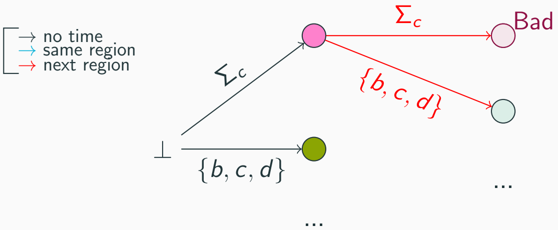
- each *state*: a belief
- each *transition*: a strategy and an elapsed time



Automaton of beliefs

An automaton where:

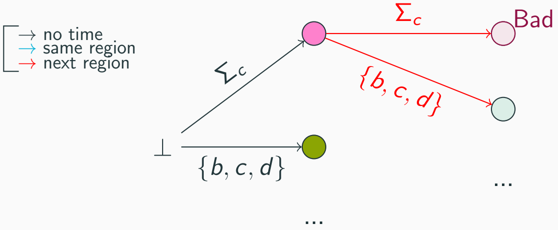
- each *state*: a belief
- each *transition*: a strategy and an elapsed time



Find a b-strategy

b-strategy γ

For a sequence of transitions in the automaton of beliefs, a b-strategy returns the next transition to take.

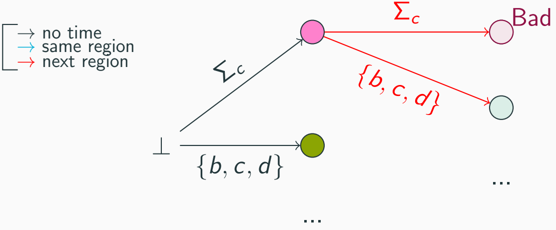


$\gamma(\varepsilon) = \xrightarrow{\Sigma_c}$

Find a b-strategy

b-strategy γ

For a sequence of transitions in the automaton of beliefs, a b-strategy returns the next transition to take.



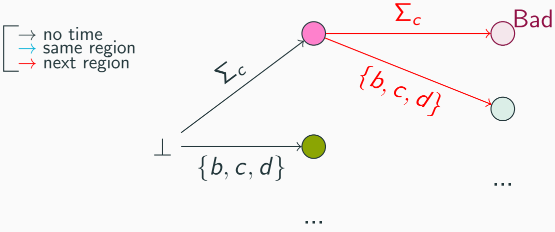
$$\gamma(\varepsilon) = \xrightarrow{\Sigma_c}$$

$$\gamma(\xrightarrow{\Sigma_c}) = \xrightarrow{\{b,c,d\}}$$

Find a b-strategy

b-strategy γ

For a sequence of transitions in the automaton of beliefs, a b-strategy returns the next transition to take.



$$\gamma(\varepsilon) = \xrightarrow{\Sigma_c}$$

$$\gamma(\xrightarrow{\Sigma_c}) = \xrightarrow{\{b,c,d\}}$$

$$\gamma(\xrightarrow{\Sigma_c}\xrightarrow{\{b,c,d\}}) = \xrightarrow{\{a,b\}}$$

...

Results

There is a strategy[1] to make a TA opaque

$\Leftrightarrow$

There is a b-strategy on the automaton of beliefs

[1] a finitely-varying strategy

Results

There is a strategy[1] to make a TA opaque

$\Leftrightarrow$

There is a b-strategy on the automaton of beliefs

Building a controller for opacity

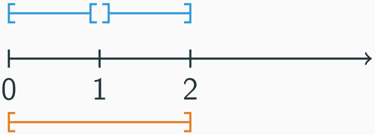
$\Leftrightarrow$

Solving a one-player safety game on a finite arena

[1] a finitely-varying strategy

So accurate?

Private durations



Public durations

Can the attacker really see this violation?

→ Other opacities allowing different types of *ponctual* violations.

Conclusion & Perspectives

- Variants of opacity:
    - Full, weak and existential opacities
    - Robust opacities
    - others?

Conclusion & Perspectives

- Variants of opacity:
  - Full, weak and existential opacities
  - Robust opacities
  - others?
- Non finetely-varying strategies

Conclusion & Perspectives

- Variants of opacity:
    - Full, weak and existential opacities
    - Robust opacities
    - others?
- Non finetely-varying strategies
- Quantified opacity

Conclusion & Perspectives

- Variants of opacity:
  - Full, weak and existential opacities
  - Robust opacities
  - others?
- Non finetely-varying strategies
- Quantified opacity
- High complexity, but implementation?

Thank you!