Making Timed Automata Robust
(Work in progress)

Patricia Bouyer-Decitre[1] Nicolas Markey[1] Ocan Sankur[1]
Claus Thrane[2]

[1]LSV, CNRS & ENS Cachan, France.
{bouyer,markey,sankur}@lsv.ens-cachan.fr

[2]Dept.of Computer Science, AAU, Denmark.
crt@cs.aau.dk

DOTS, Sept. 4th 2010

From Quantitative analysis to robustness

From Quantitative analysis to robustness

Quantitative Analysis (i.e. real-valued)

Model-checking, Simulation-, Language inclusion- checking ...

From Quantitative analysis to robustness

Quantitative Analysis (i.e. real-valued)

Model-checking, Simulation-, Language inclusion- checking ...

Robust verification

Implementability of timed automata

Quantitative Analysis

Timed Transition System $(S, \rightarrow)$

A set S of states, and $\rightarrow \subseteq S \times (\Sigma \cup \mathbb{R}_{\leq 0}) \times S$ of transitions.

Timed simulation distance

A binary relation R_ϵ on the set S a *timed simulation distance*, provided that if $s \, R_\epsilon \, t$, then for all $a \in \Sigma$ and $d \in \mathbb{R}_{\leq 0}$:

if $s \xrightarrow{a} s'$ then $t \xrightarrow{a} t'$ s.t. $s' \, R_\epsilon \, t'$

if $s \xrightarrow{d} s'$ then $t \xrightarrow{d'} t'$ s.t. $s' \, R \, t'$ and $|d - d'| \leq \epsilon$

- $s \leq_\epsilon t$ means (s, t) is in some timed simulation distance.
- $s \sim_\epsilon t$ means (s, t) is in some timed bisimulation distance.

Quantitative analysis — Other flavors

Definition: Distances (values in $\mathbb{R} \cup \{\infty\}$)

point-wise	**accumulating**
$d_L^{\bullet}(\sigma, \tau) = \sup_i \lambda^i \lvert\sigma_i - \tau_i\rvert$	$d_L^{+}(\sigma, \tau) = \sum_i \lambda^i \lvert\sigma_i - \tau_i\rvert$

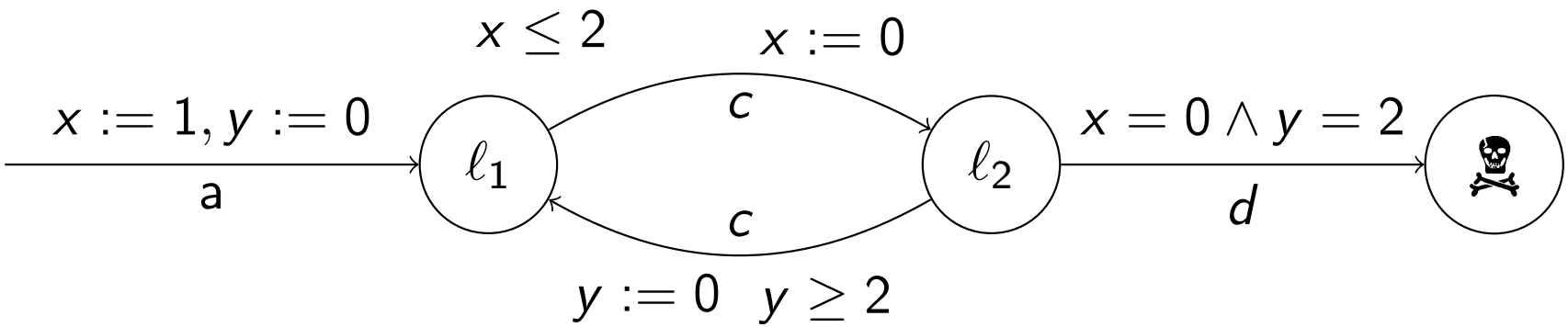
trace distance $\sigma \in (\Sigma \times \mathbb{R}_{\leq 0})^*$

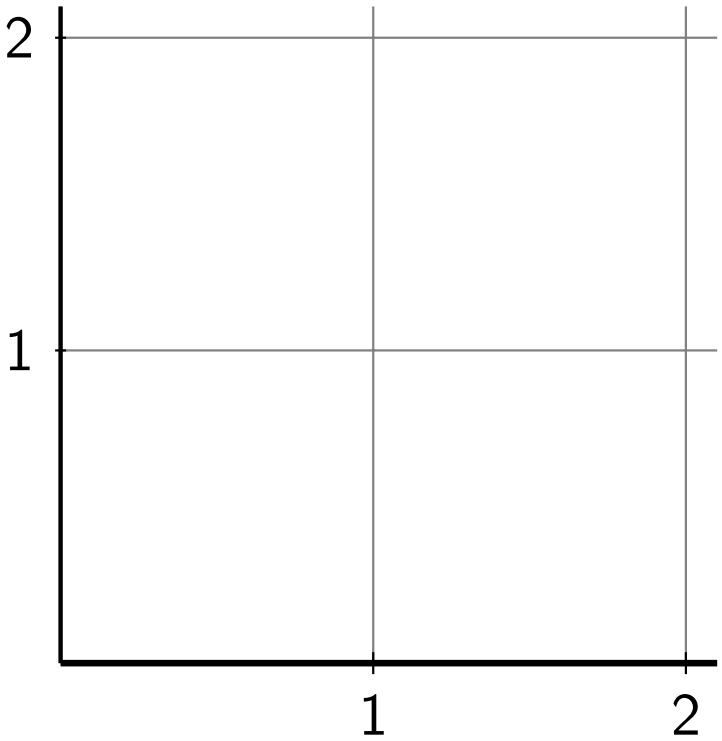
- $|\sigma, \sigma'| = \sup_i |t(\sigma)_i - t(\sigma')_i|$ whenever $u(\sigma) = u(\sigma')$
- $|s, s'| = \sup_{\sigma \in \mathsf{Tr}(s)} \inf_{\sigma' \in \mathsf{Tr}(s')} |\sigma, \sigma'|$

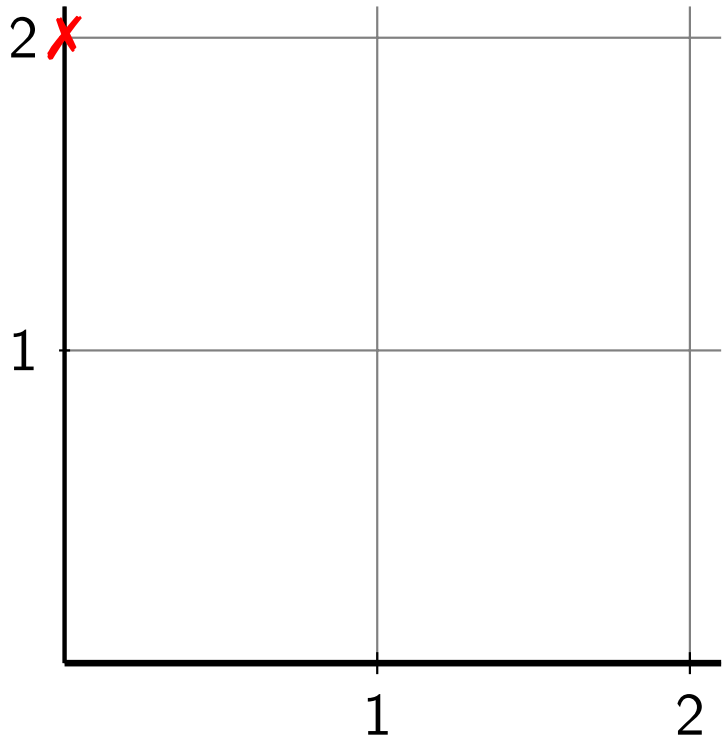
Weak transitions

$s_1 \stackrel{a,d}{\Longrightarrow} s_2$ iff $s_1 \xrightarrow{d'} s_3 \xrightarrow{a} s_4 \xrightarrow{d''} s_2$.

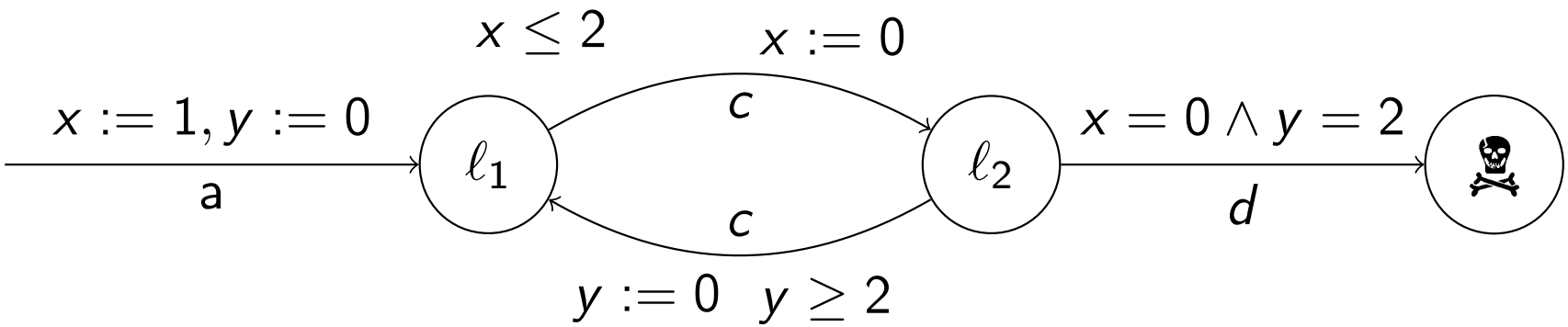
Example [Puri'98]

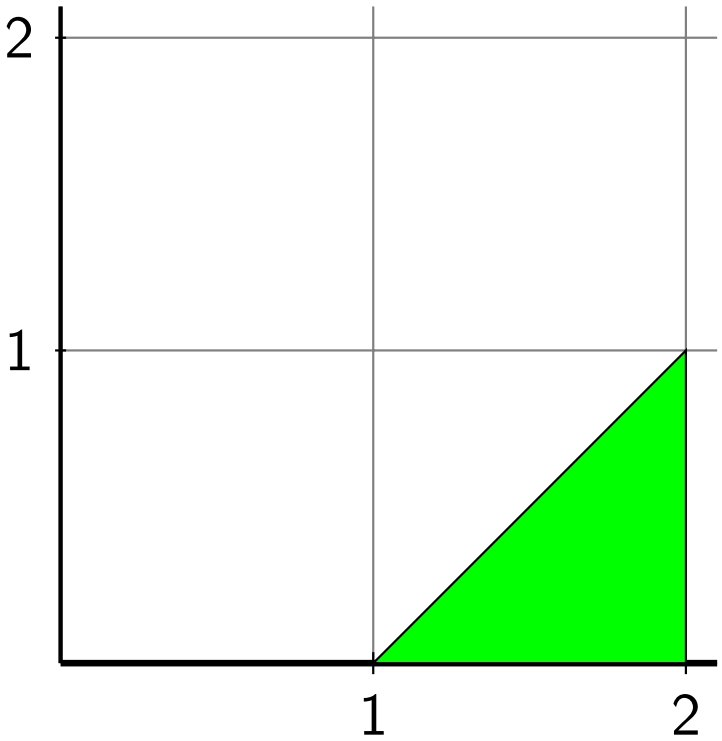


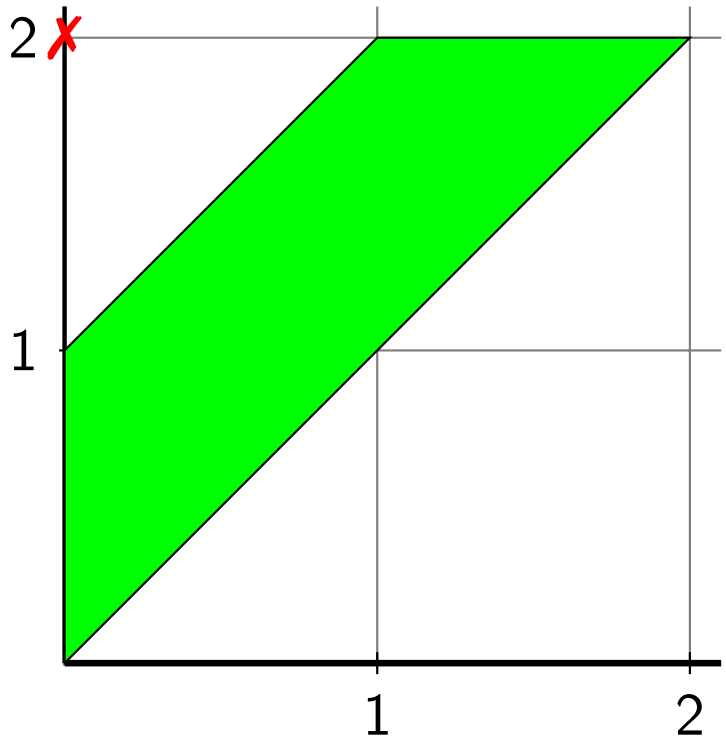




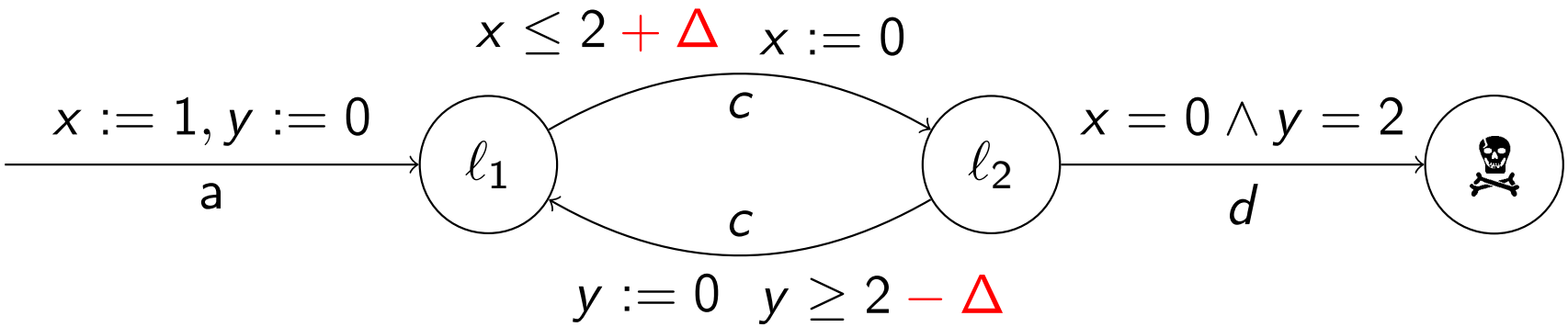
Example [Puri'98]

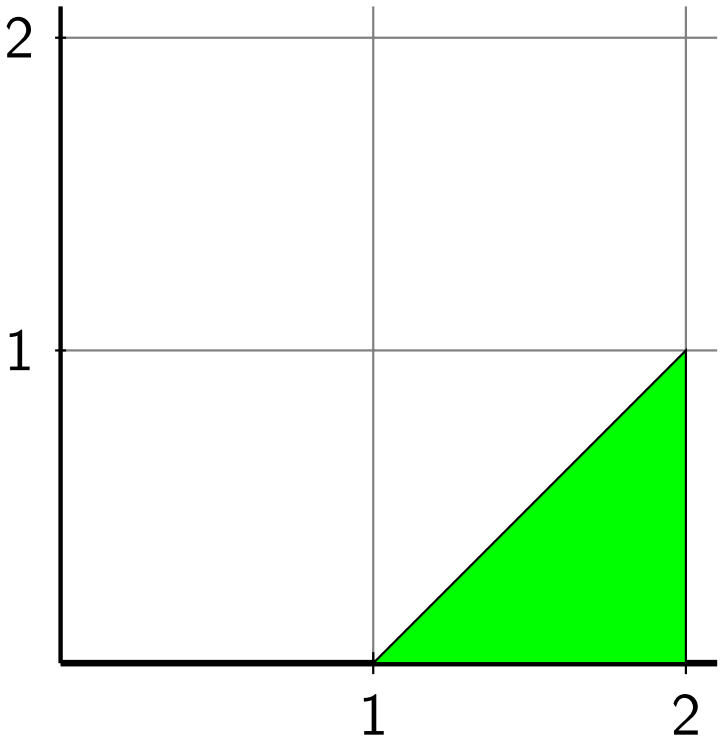


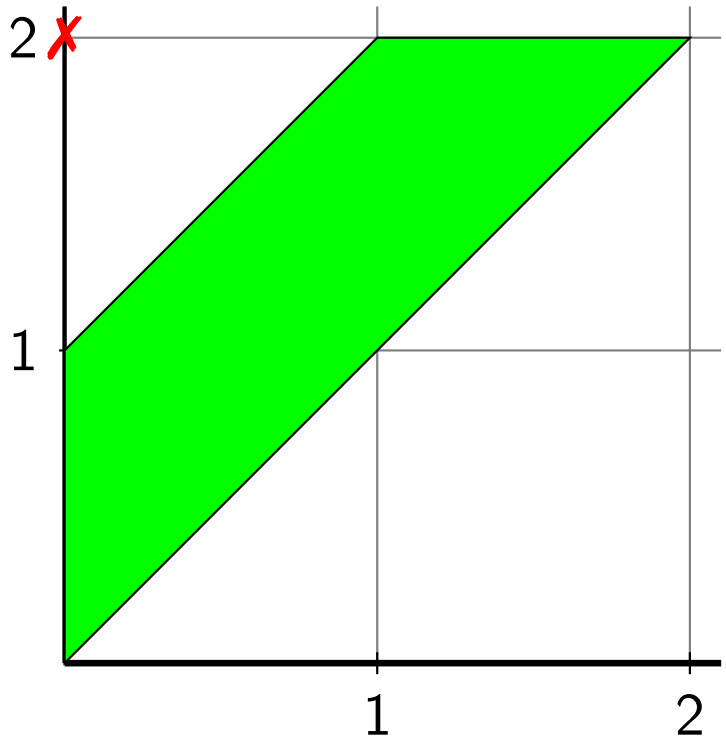




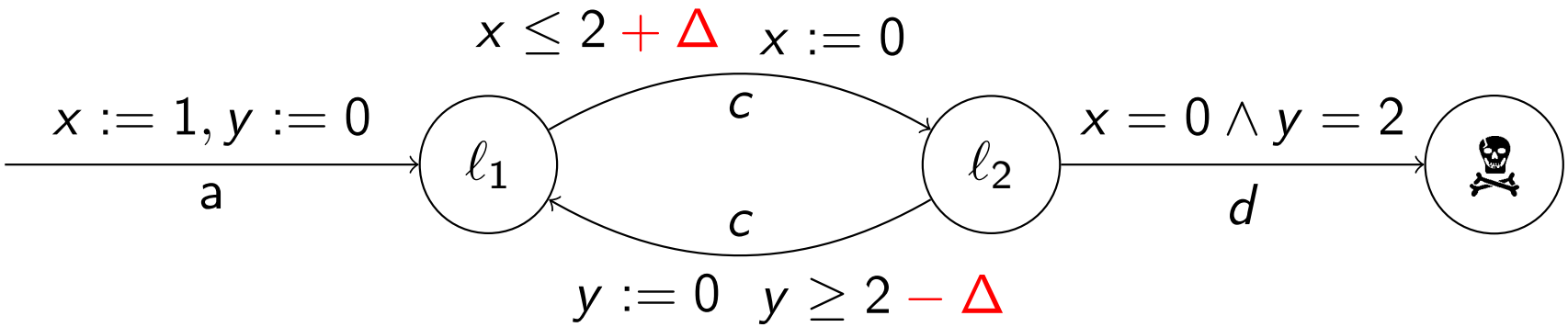
Example [Puri'98]

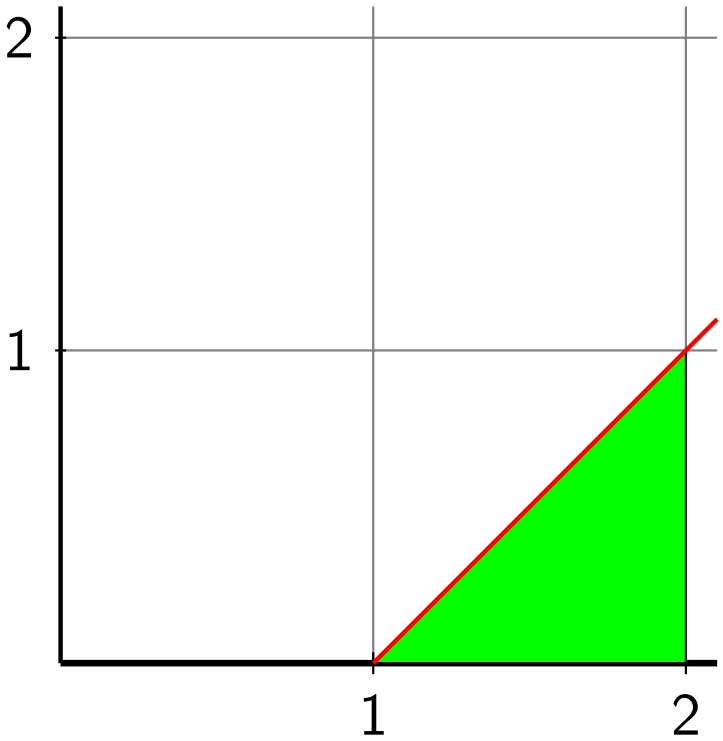


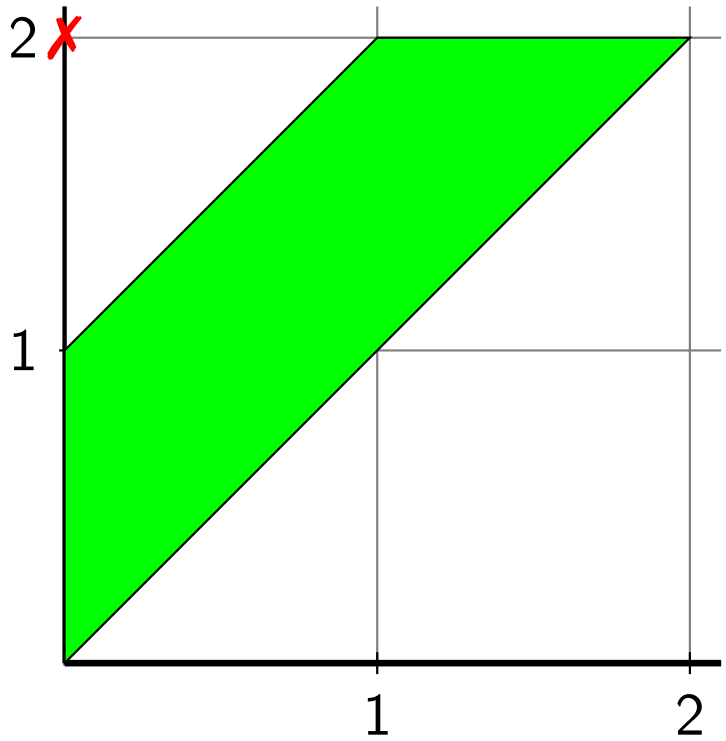




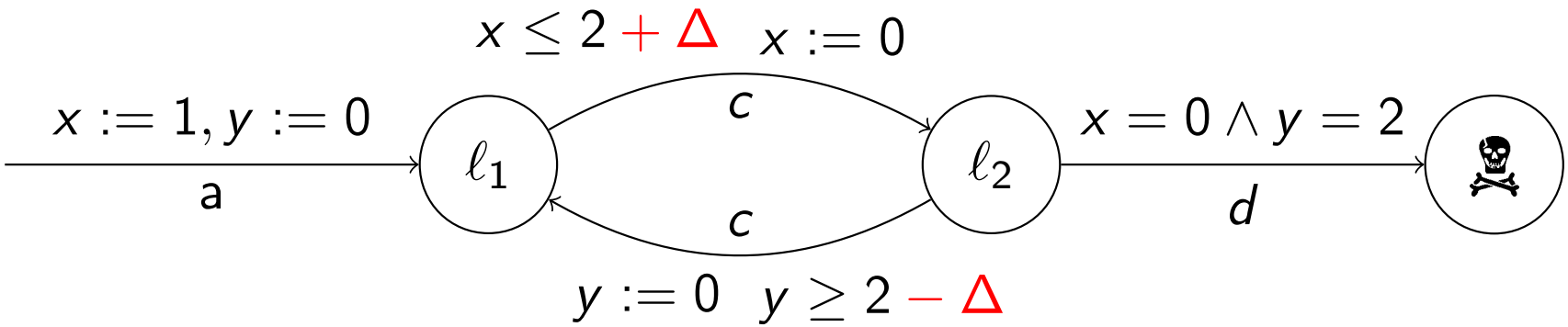
Example [Puri'98]

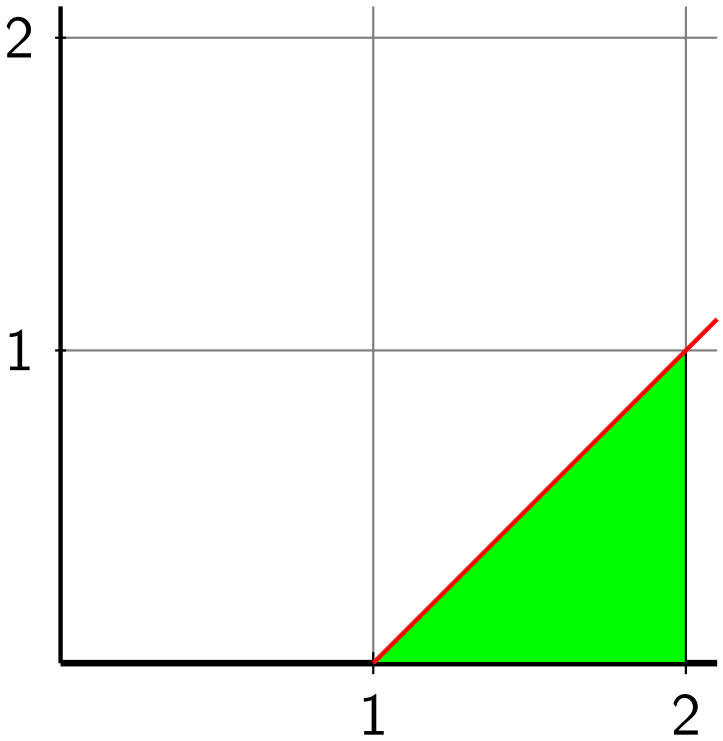


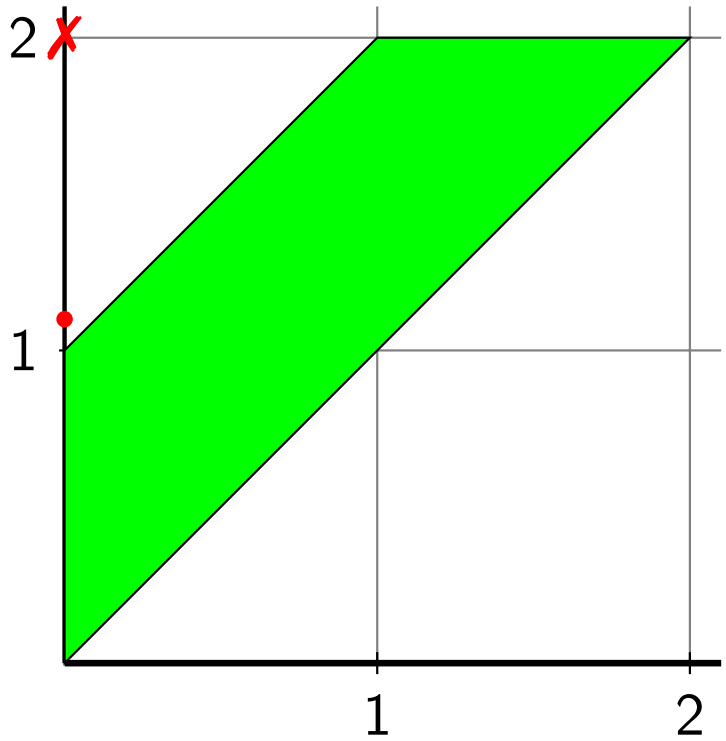




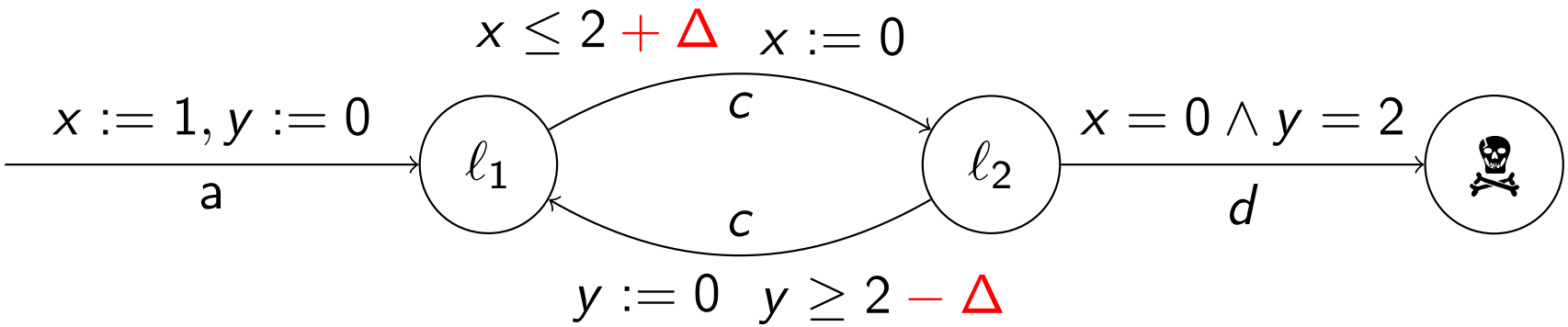
Example [Puri'98]

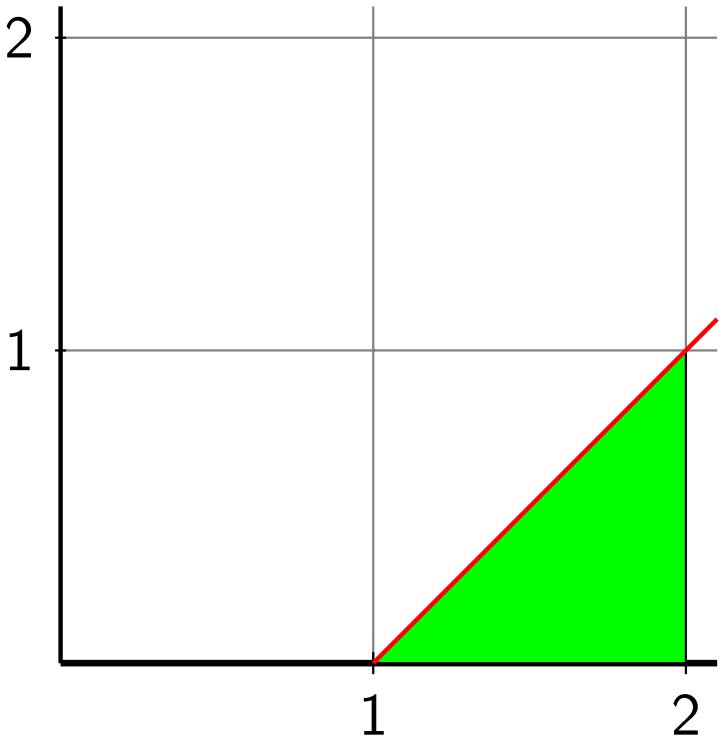


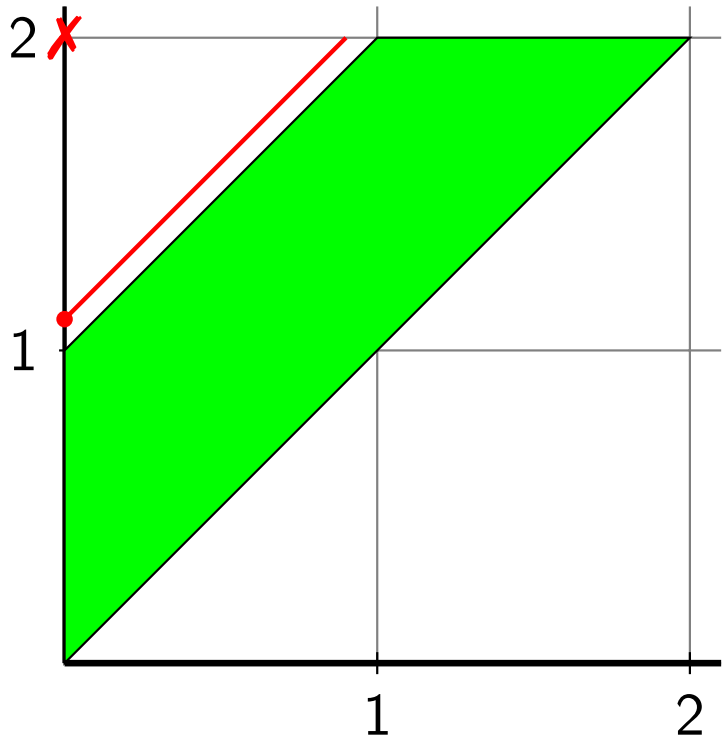




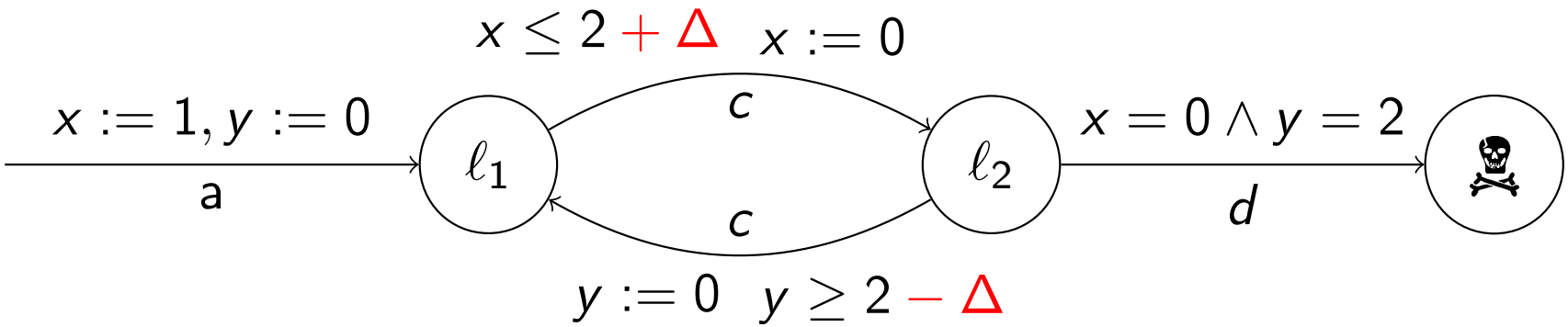
Example [Puri'98]

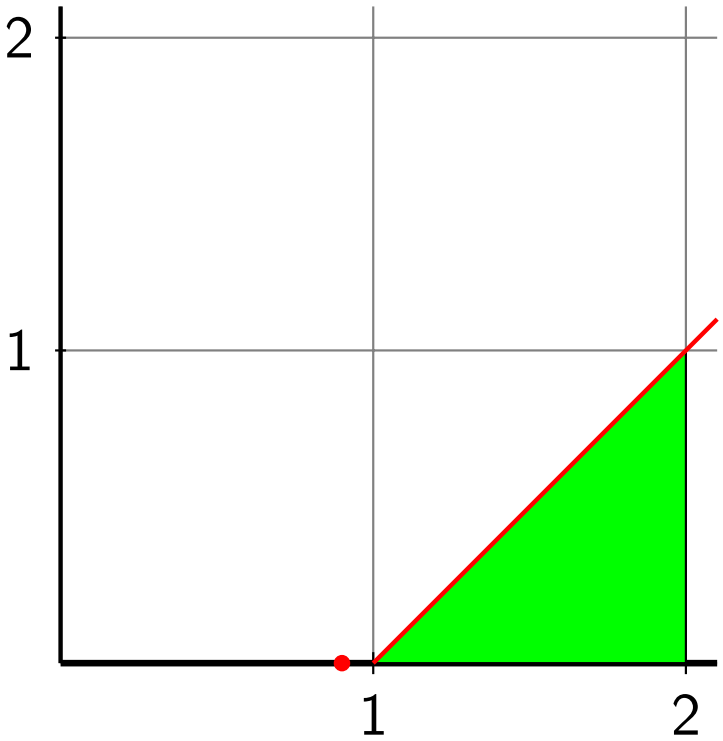


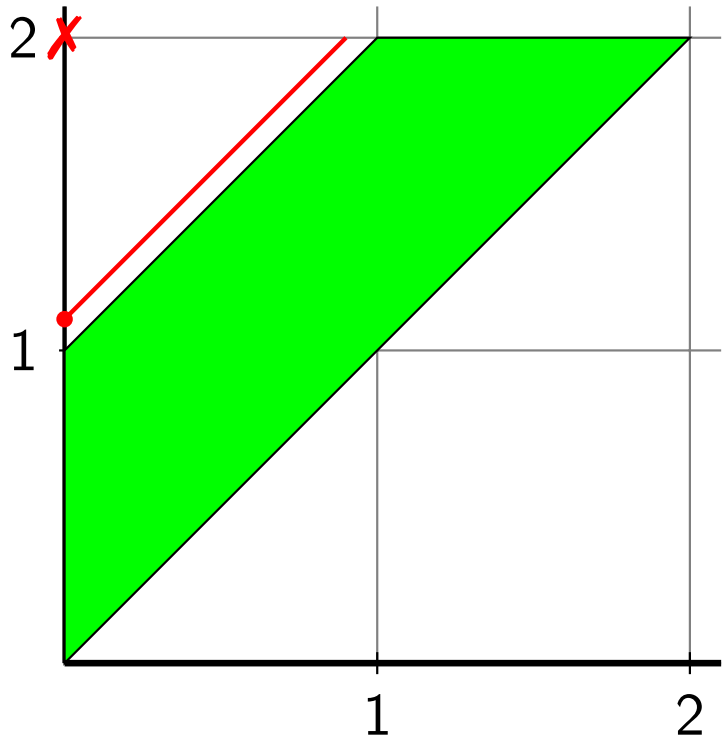




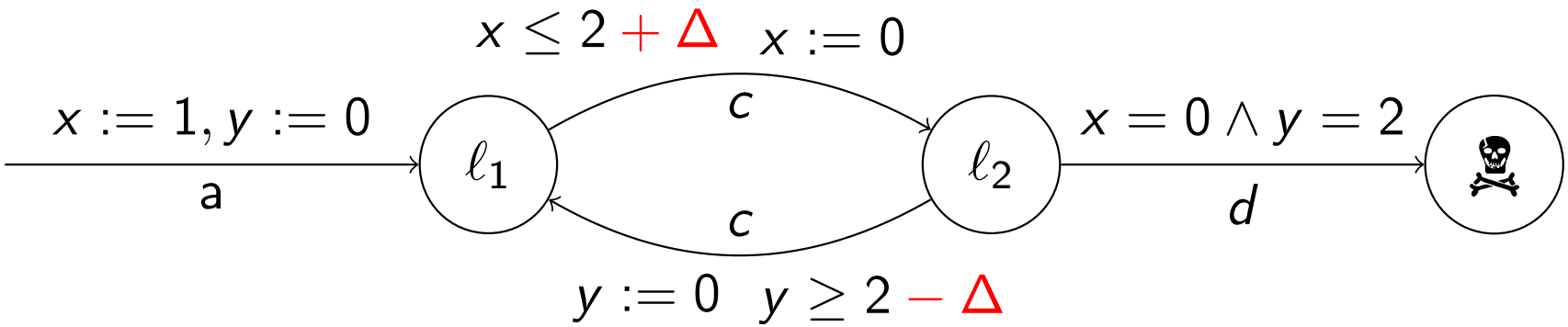
Example [Puri'98]

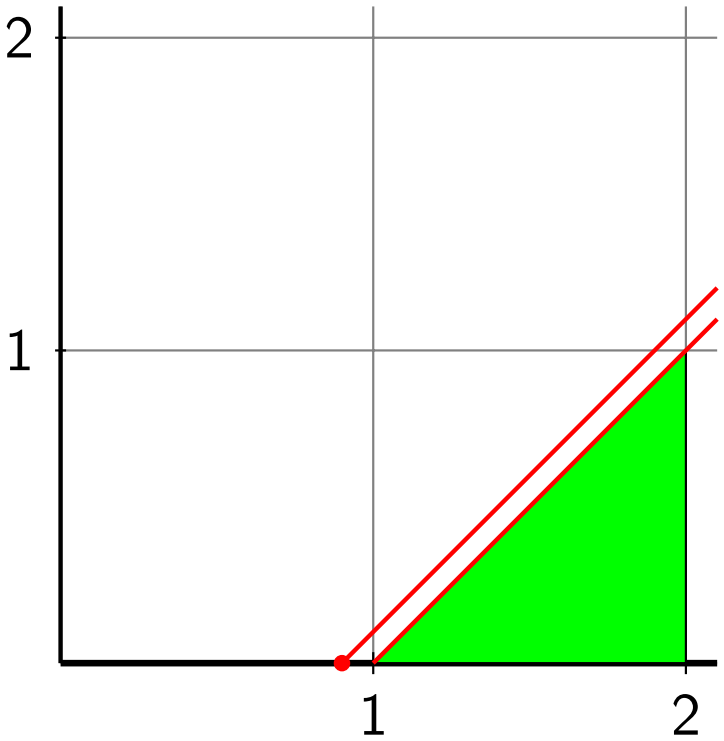


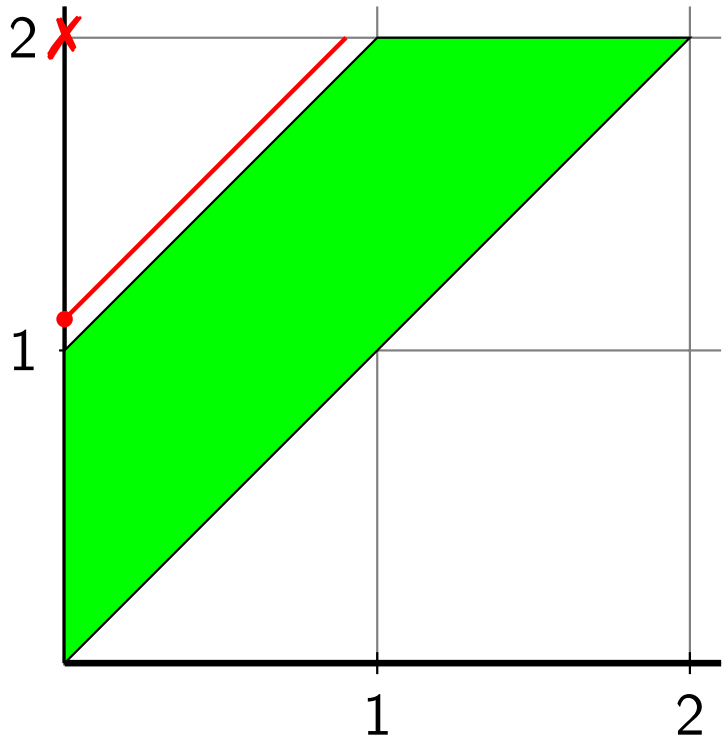




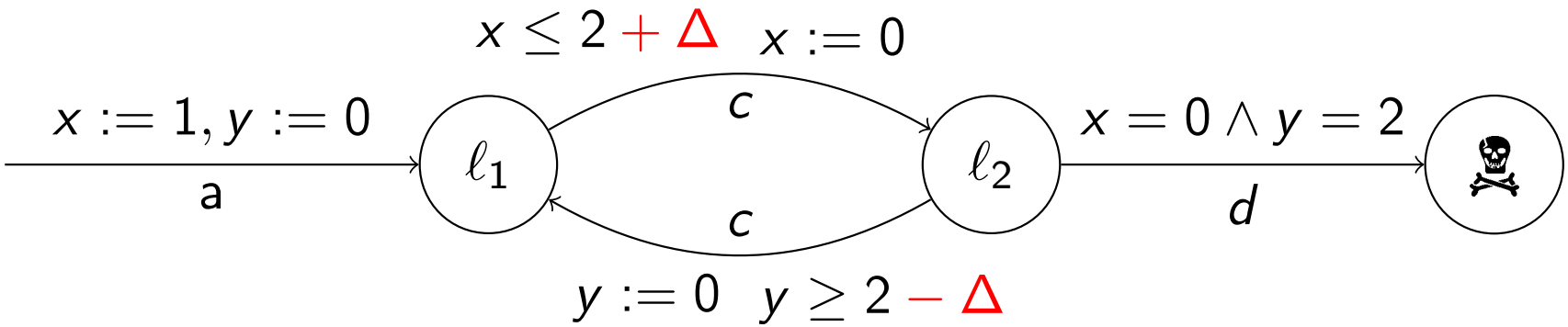
Example [Puri'98]

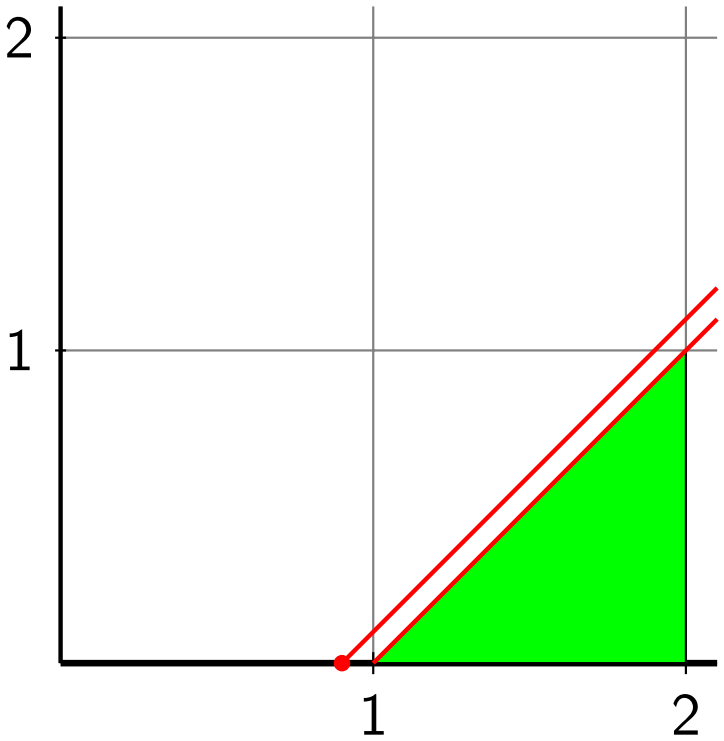


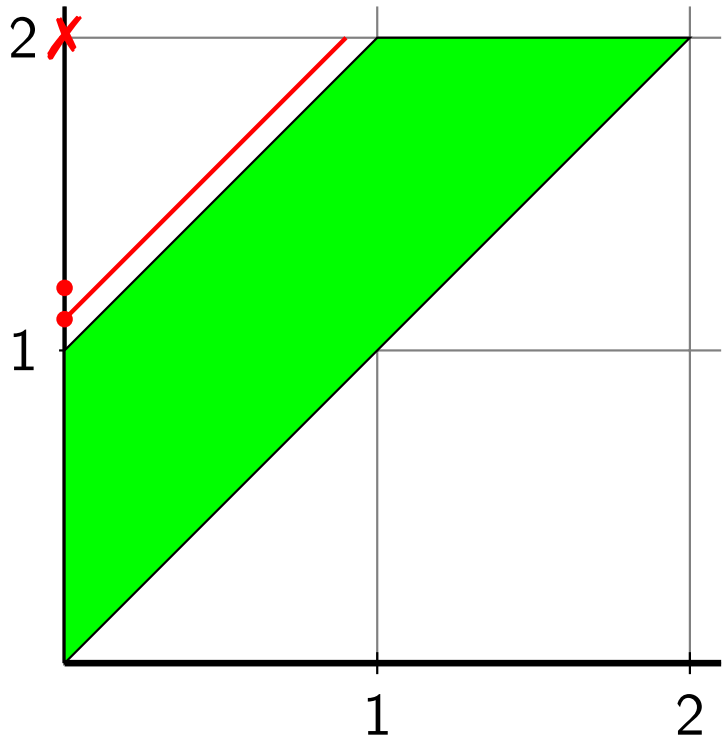




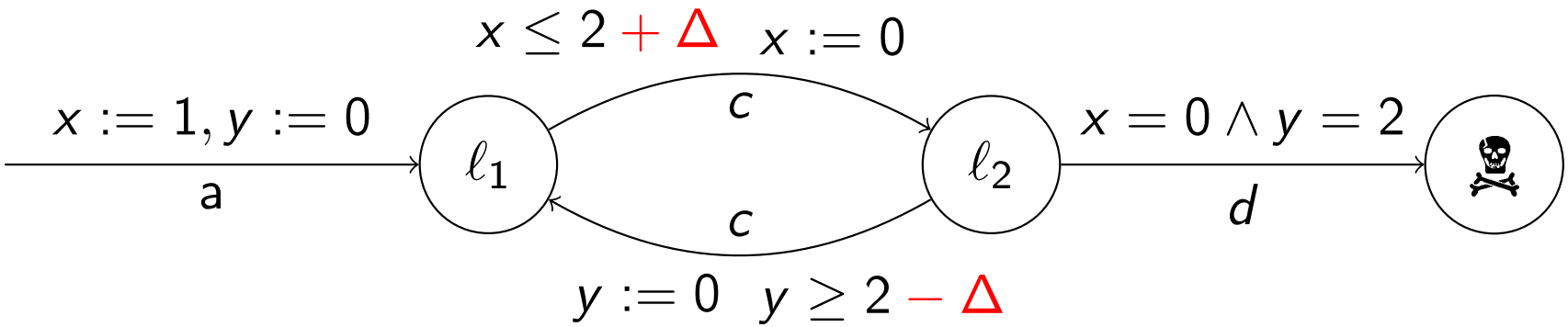
Example [Puri'98]

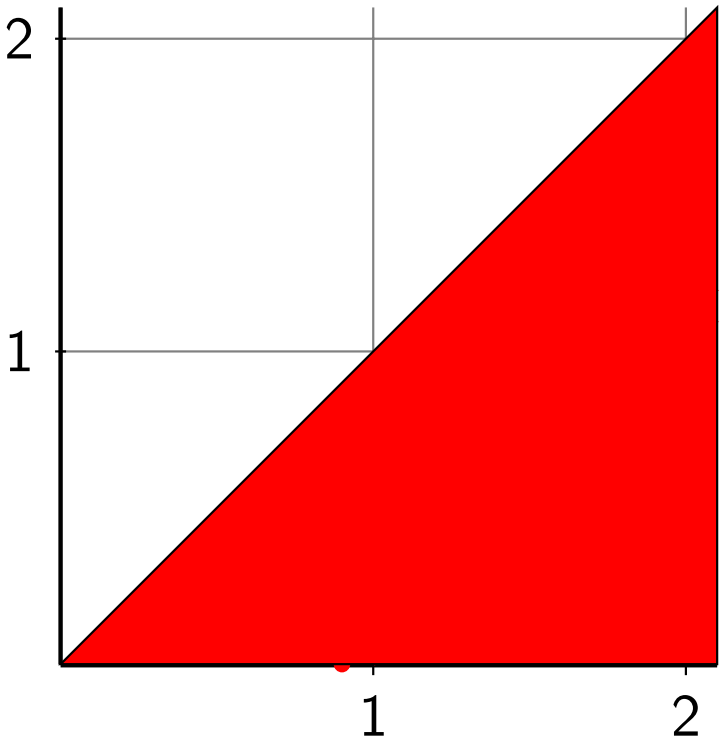


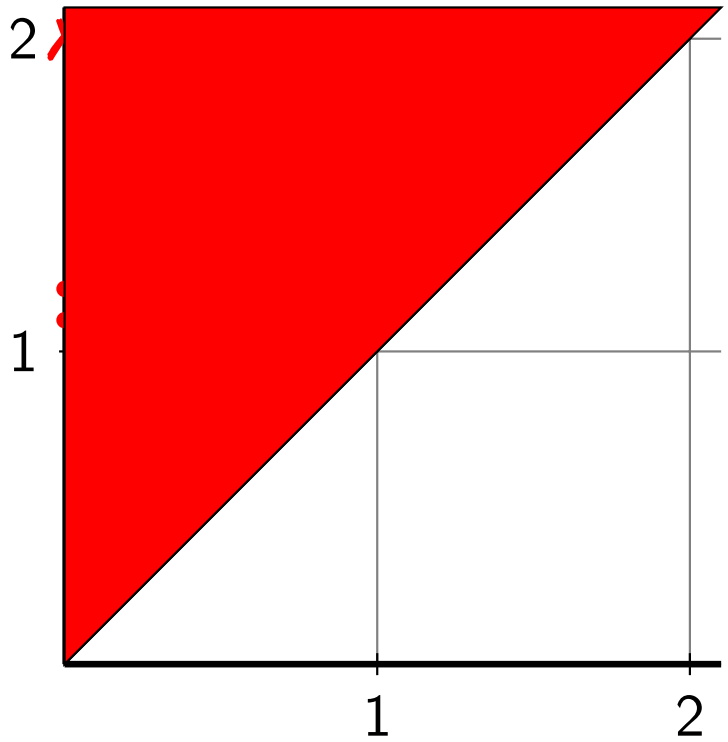




Example [Puri'98]







A_Δ formally

$$\phi_1, \phi_2 ::= x \bowtie k \mid x - y \bowtie k \mid \psi_1 \wedge \phi_2$$

where $k \in \mathbb{N}$, $x, y \in C$ *and* $\bowtie \in \{\leq \geq\}$

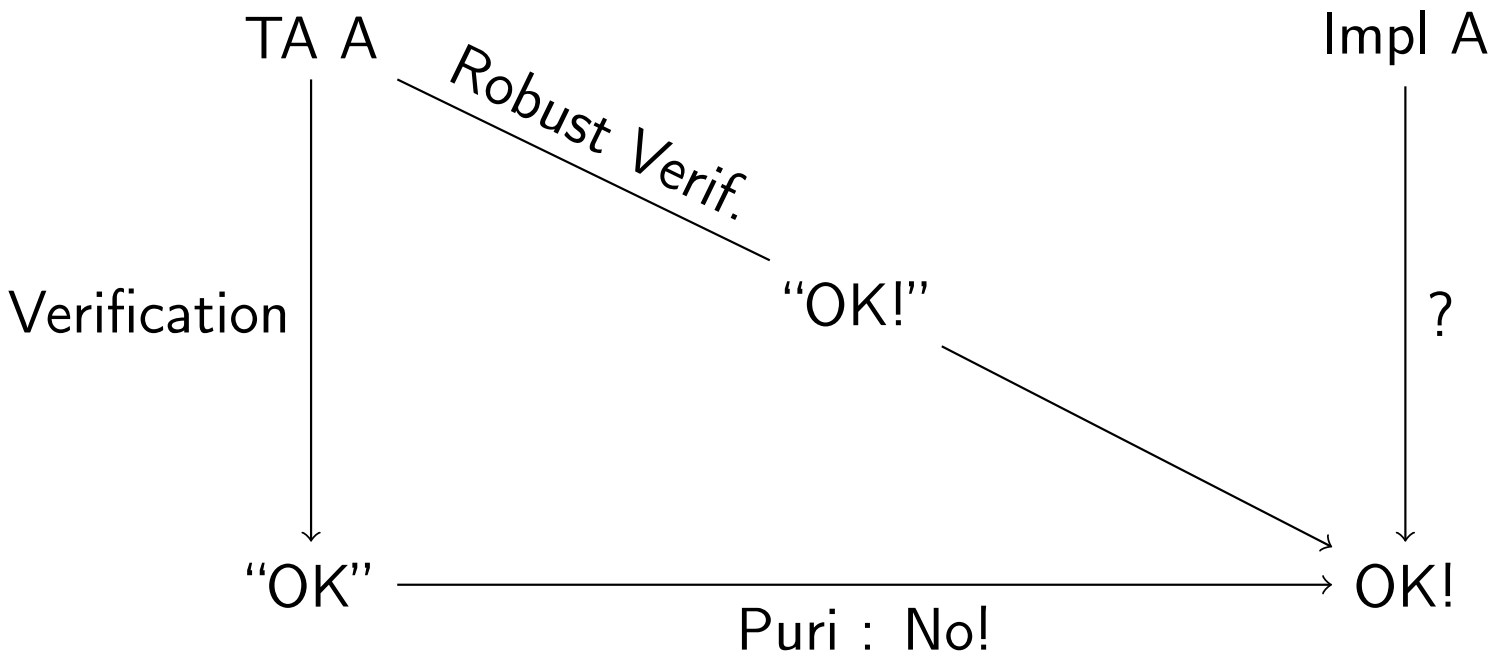
$$\begin{aligned}
[\![x \geq k]\!]_\Delta &= \{v \in \mathbb{R}^C_{\leq 0} \mid v(x) \geq k - \Delta\} \\
[\![x \leq k]\!]_\Delta &= \{v \in \mathbb{R}^C_{\leq 0} \mid v(x) \leq k + \Delta\} \\
[\![x - y \geq k]\!]_\Delta &= \{v \in \mathbb{R}^C_{\leq 0} \mid v(x) - v(y) \geq k - \Delta\} \\
[\![x - y \leq k]\!]_\Delta &= \{v \in \mathbb{R}^C_{\leq 0} \mid v(x) - v(y) \leq k + \Delta\} \\
[\![\phi_1 \wedge \phi_2]\!]_\Delta &= [\![\phi_1]\!]_\Delta \cap [\![\phi_2]\!]_\Delta
\end{aligned}$$

What is robustness?

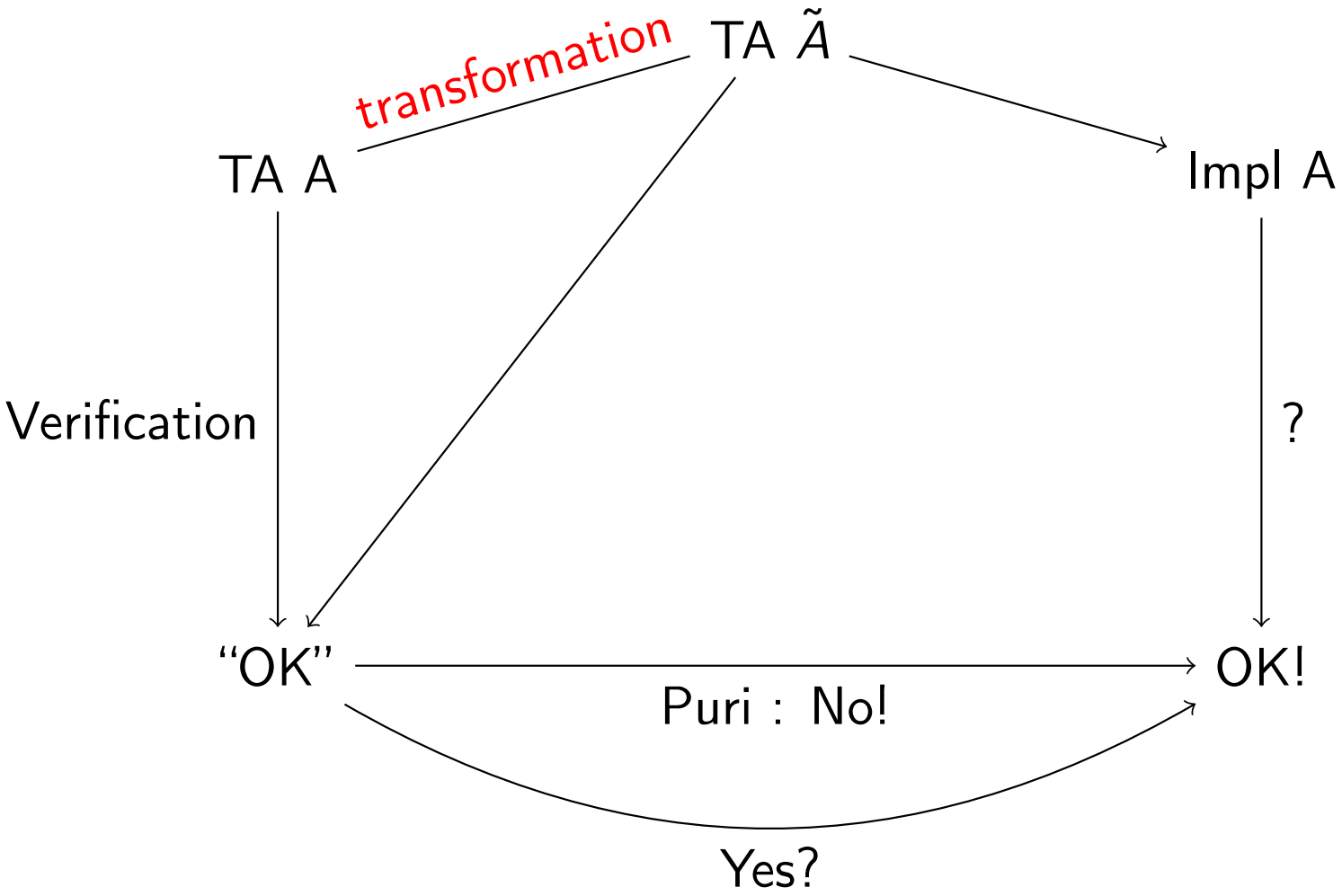
Whenever $\mathcal{A}$ is robust, does it mean $\mathcal{A} \sim_\epsilon \mathcal{A}_\Delta$ for some $\epsilon = F(\Delta)$?

Semantic robustness — vs. — syntactic robustness

Semantic robustness — vs. — syntactic robustness



Semantic robustness — vs. — syntactic robustness



1 Motivation

Robustness definitions?

A timed automaton A, is *robust* if there exist $\Delta > 0$ such that,

1. $Reach(A) = Reach(A_\Delta)$. (safety)
2. $|A, A_\Delta| \leq \epsilon$ (linear)
3. $A \sim_\epsilon A_\Delta$, (strong bisim)
4. $A \geq_\epsilon A_\Delta$, (sim)
5. $A \approx_\epsilon A_\Delta$ (weak bisim)

for some $\epsilon \geq 0$.

Proposition

Let $\mathcal{A}_s$, $\mathcal{A}_l$, $\mathcal{A}_{wb}$, and $\mathcal{A}_{sb}$ be the sets of safety, linear, weak bisim, and strong bisim - robust timed automata. Then:

- $\mathcal{A}_s \supset \mathcal{A}_l \supset \mathcal{A}_{wb} \supset \mathcal{A}_{sb}$

Construction — Border region timed automata

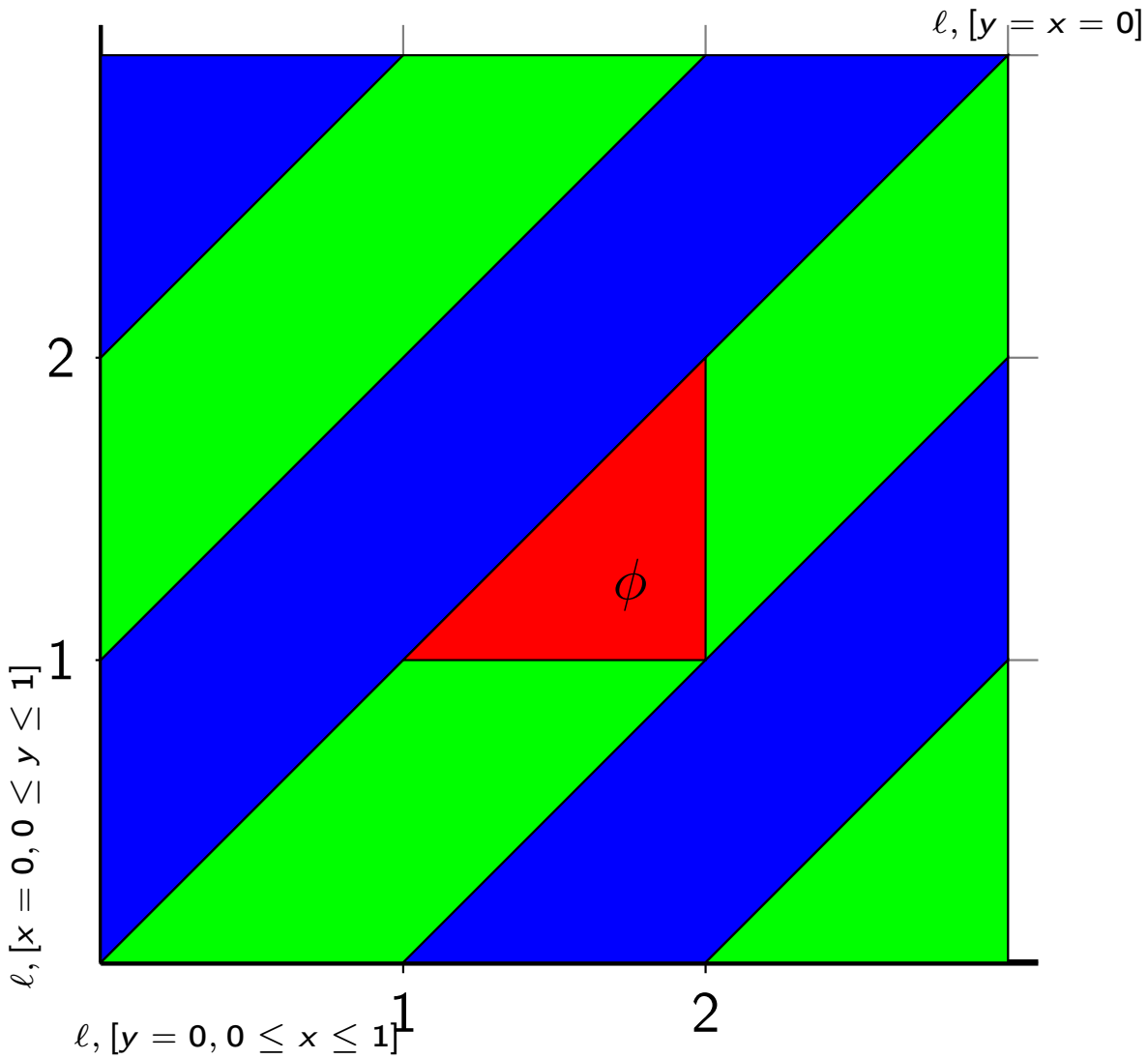
Define $B = \{ [v] \mid v \in \mathbb{R}^C_{\leq 0}, \exists c \in C : v(c) = 0\}$ of border regions.

Definition

Given $A = (C, \Gamma, L, l_0, E)$, Construct $\tilde{A} = (C, \Gamma, L', l'_0, E')$ as follows: $L' = L \times B$ and $l'_0 = l_{0_{[v_0]}}$

- $l_{[v^B]} \xrightarrow{\phi \wedge \phi_{[v]}, a, r} l'_{[v[r]^B]} \in E'$ if $l \xrightarrow{\phi, a, r} l' \in E \wedge [v] \cap [\![\phi]\!]$

For each successor $[v]$ of $[v^B]$ we add an edge if $[v] \cap [\![\phi]\!]$

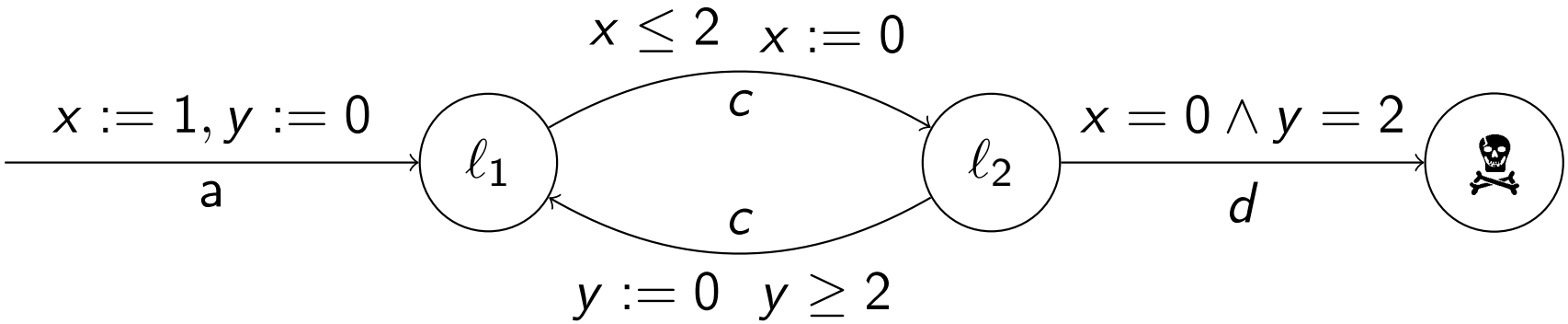

$\ell, [y = x = 0]$
2
1
ϕ
$\ell, [x = 0, 0 \leq y \leq 1]$
$\ell, [y = 0, 0 \leq x \leq 1]$
1
2

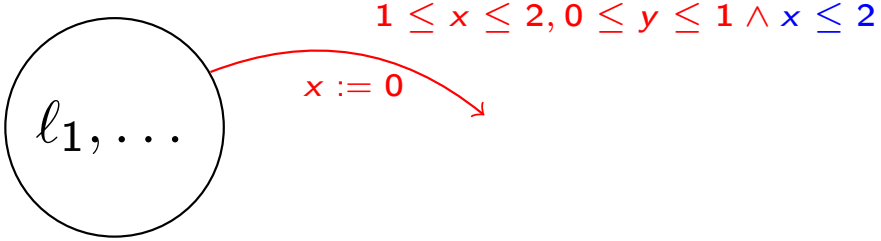
Theorem

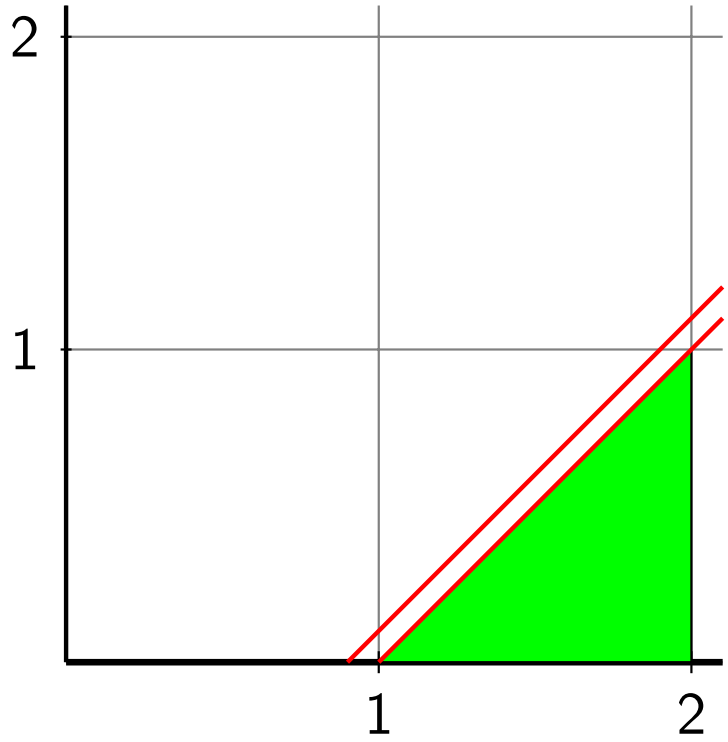
Given a timed automaton A, it holds that $A \sim_0 \tilde{A}$

Where $\tilde{A}$ is the border region timed automata of A

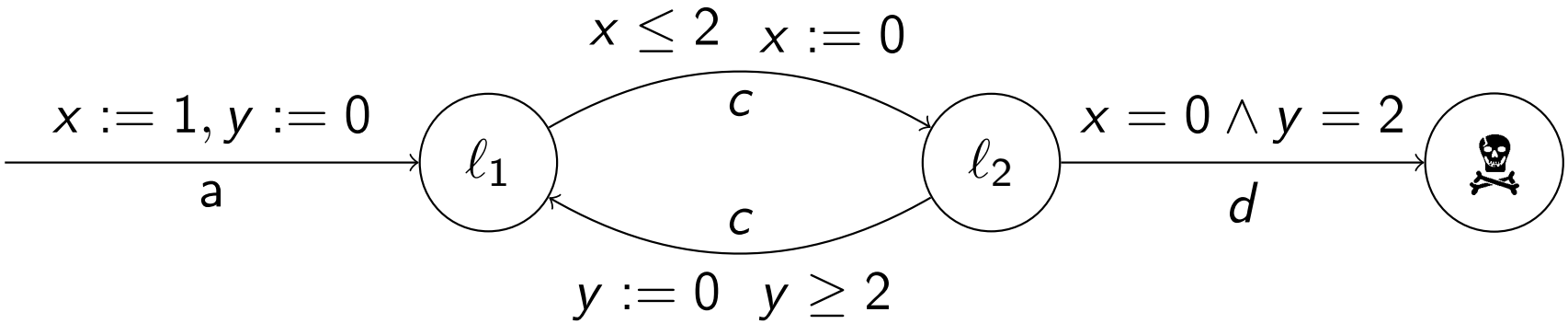
Safety robustness is obtainable

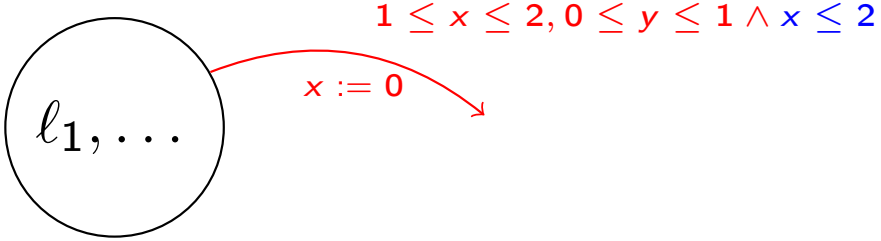


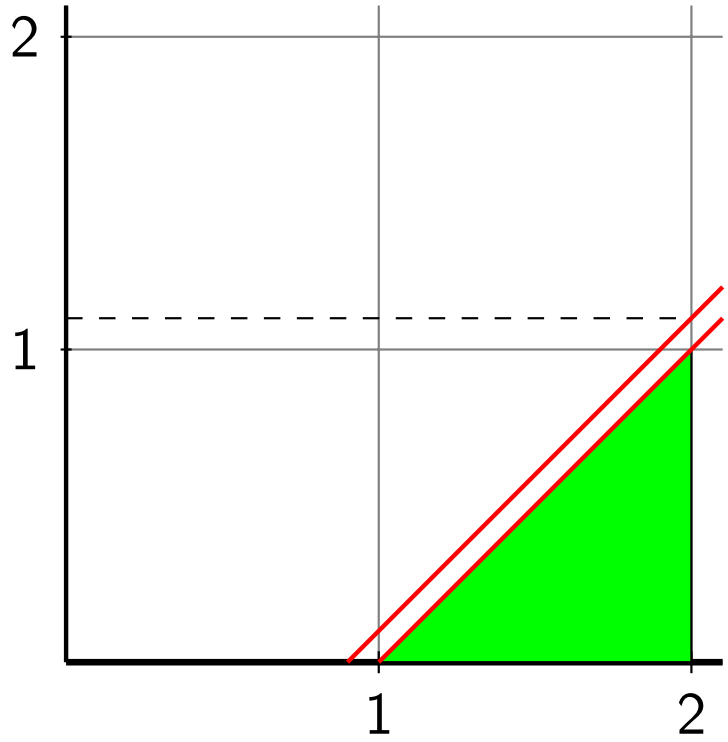


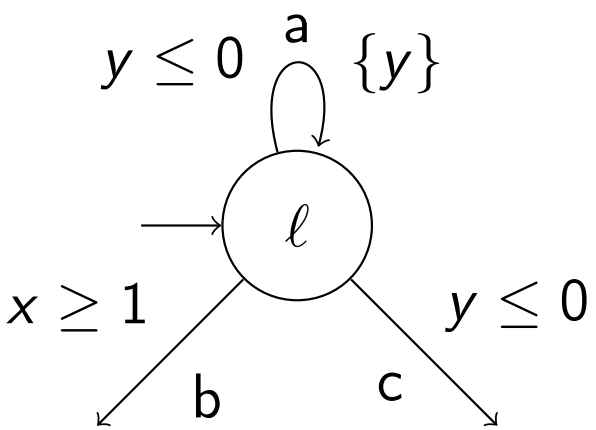


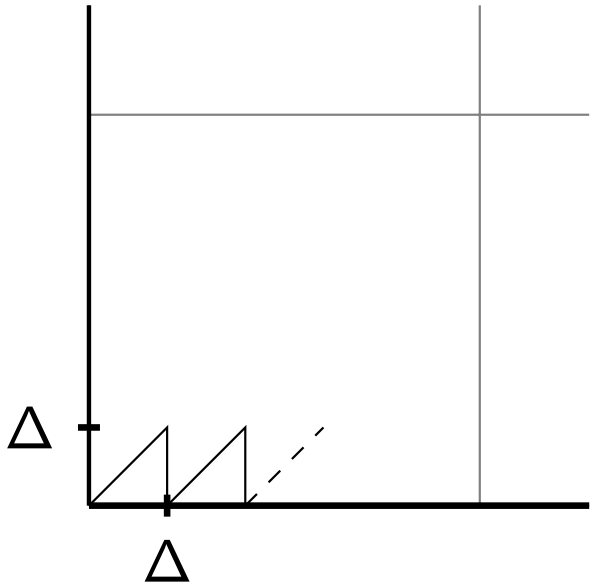
Safety robustness is obtainable











Theorem

There exist timed automata which there is no bisimulation equivalent alternative which are robust up to time abstract simulation.

Conclusion

Status

- Viable construction for safety robust
- Counter examples (proofs) for simulation/bisimulation/weak ..

Conclusion

Status

- Viable construction for safety robust
- Counter examples (proofs) for simulation/bisimulation/weak ..

The future

Other robustness definition.

Conclusion

Status

- Viable construction for safety robust
- Counter examples (proofs) for simulation/bisimulation/weak ..

The future

Other robustness definition.

Why is this so hard?

There is a great distance from syntax to semantics of TA