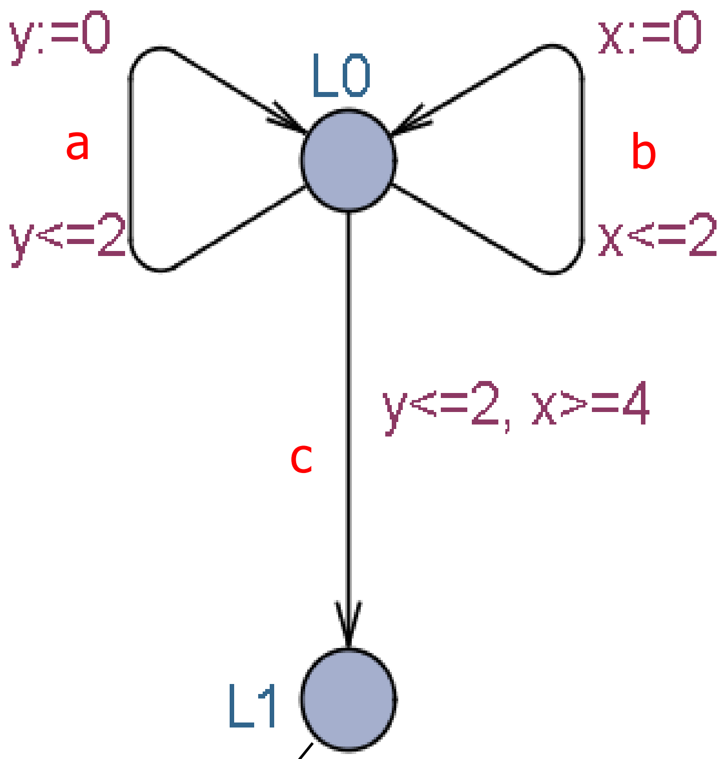
Decidability and Symbolic Verification

Kim G. Larsen
Aalborg University, DENMARK

Overview

- Decidability
  - Region Construction
  - Reachability & Bisimulation Checking
- Symbolic Verification
  - On-the-fly Exploration
  - Zones and Difference Bounded Matrices (DBM)
  - Clock Difference Diagrams (CDD)
- Verification Options

Reachability ?



Reachable from initial state (L0,x=0,y=0) ?

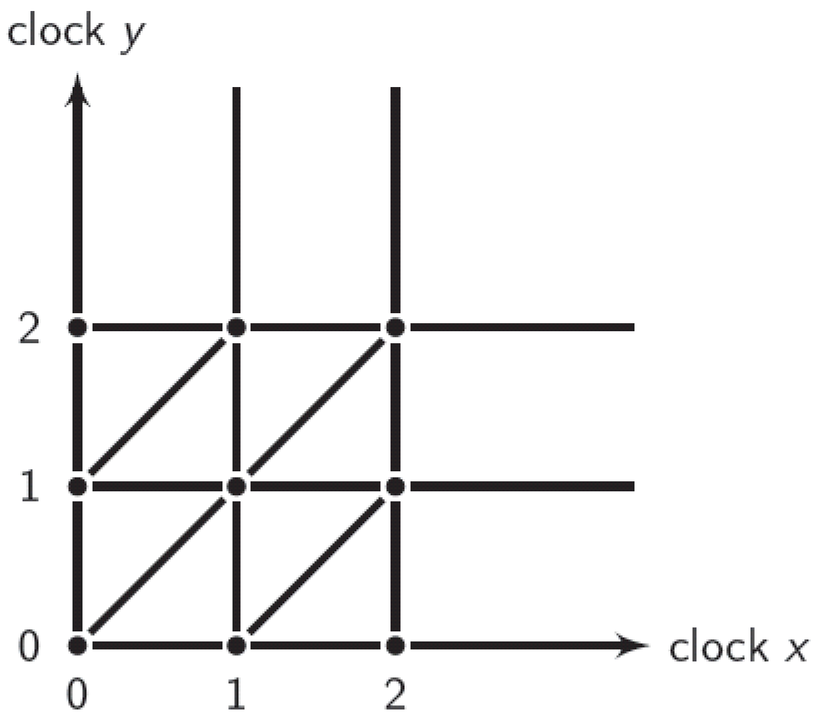
OBSTACLE:
Uncountably infinite
state space

$L \times \mathbb{R}^C$

locations

clock-valuations

The Region Abstraction

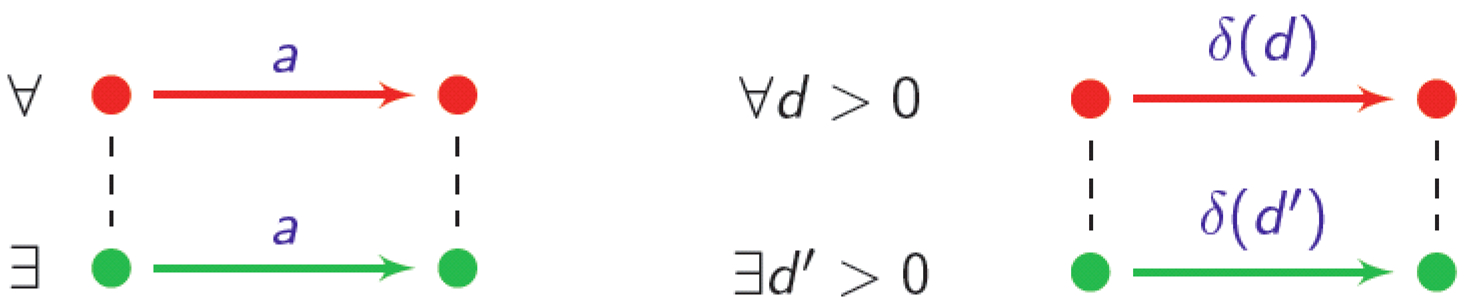


- "compatibility" between regions and constraints
- "compatibility" between regions and time elapsing

$\rightsquigarrow$ an equivalence of finite index
a time-abstract bisimulation

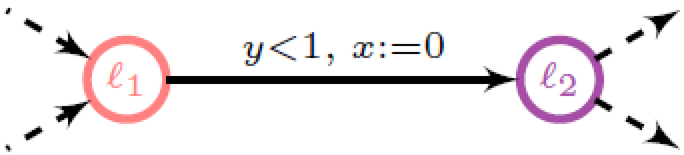
Time Abstracted Bisimulation

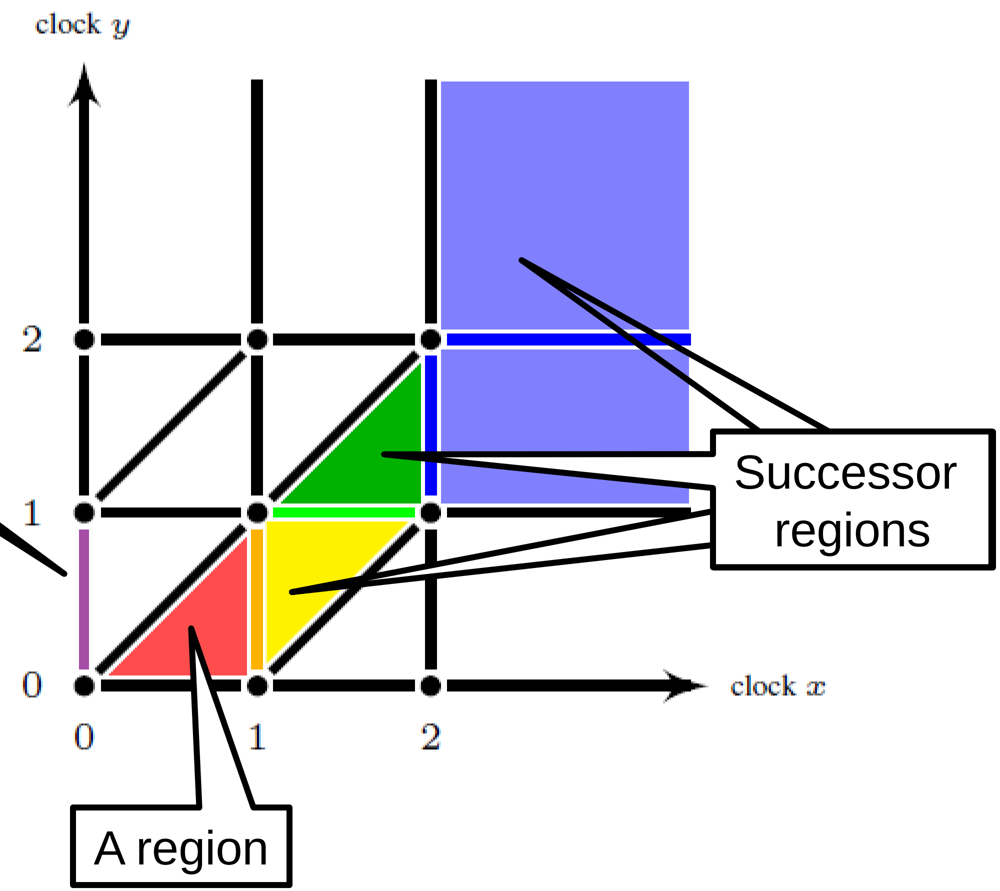
This is a relation between ● and ● such that:



… and vice-versa (swap ● and ●).

Regions – From Infinite to Finite



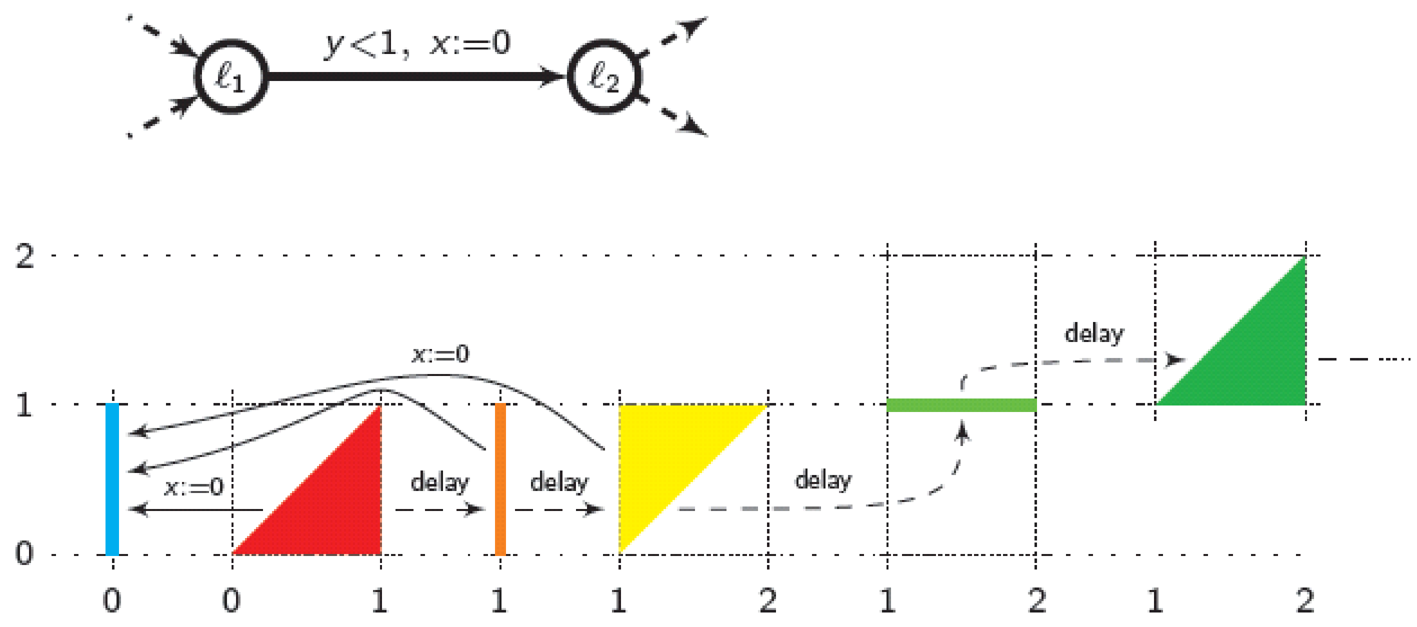


THM [AD90]
Reachability is decidable (and PSPACE-complete) for timed automata

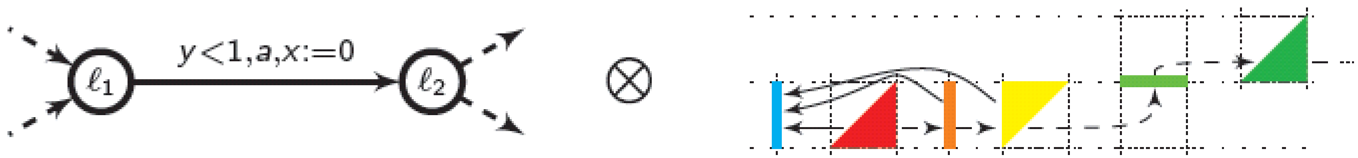
THM [CY90]
Time-optimal reachability is decidable (and PSPACE-complete) for timed automata

Region Graph

It "mimicks" the behaviours of the clocks.



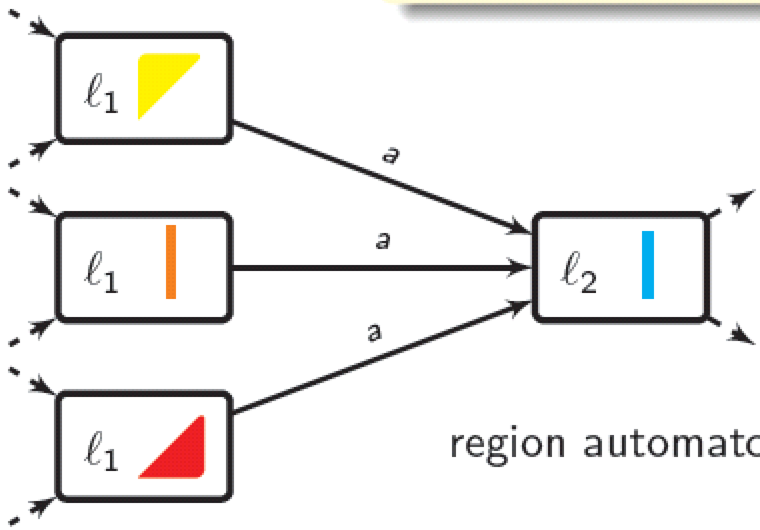
Region Automaton = Finite Bisimulation Quotiont



timed automaton

region graph

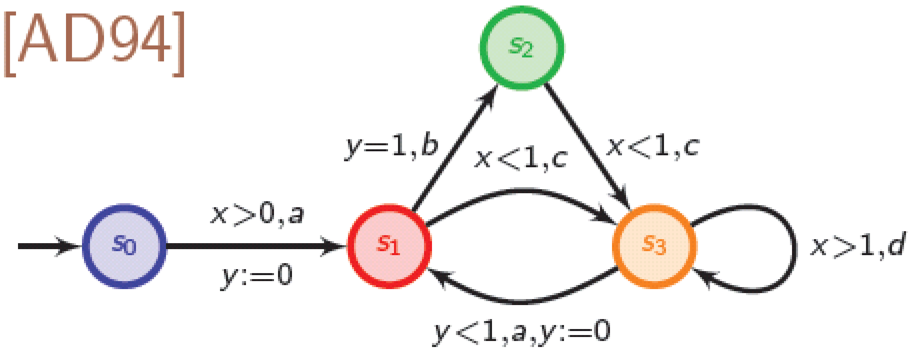
$\mathcal{L}$(reg. aut.) = UNTIME($\mathcal{L}$(timed aut.))

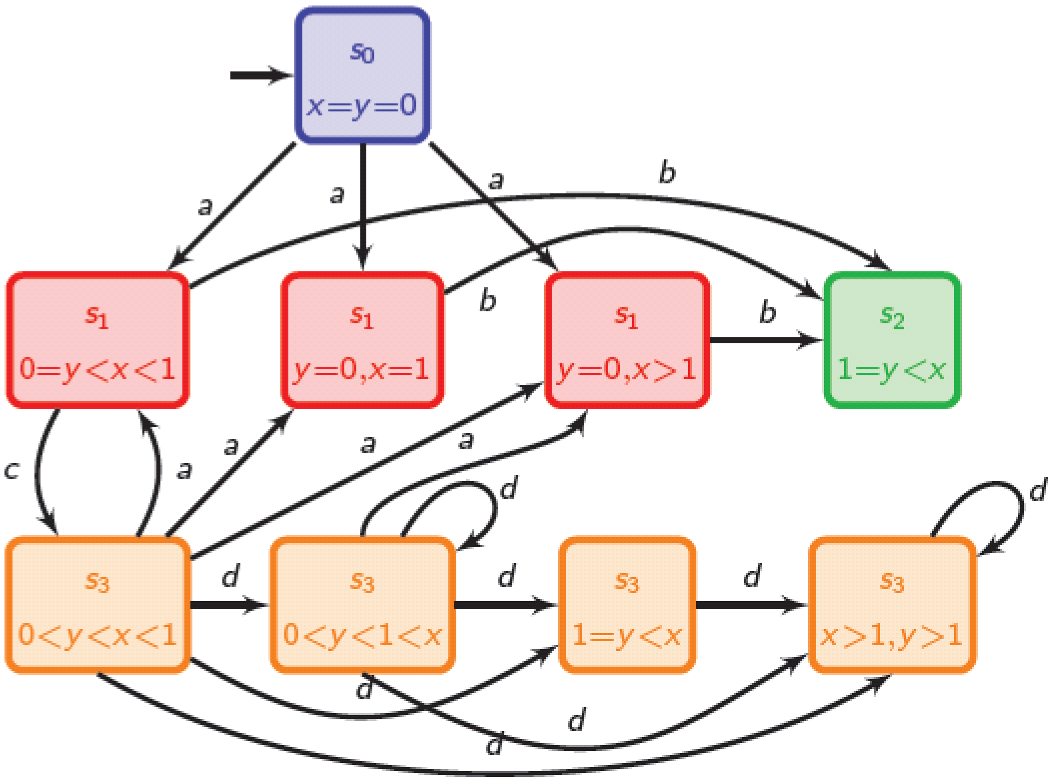


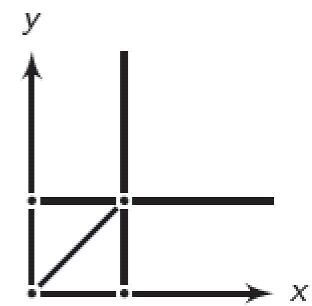
region automaton

An Example

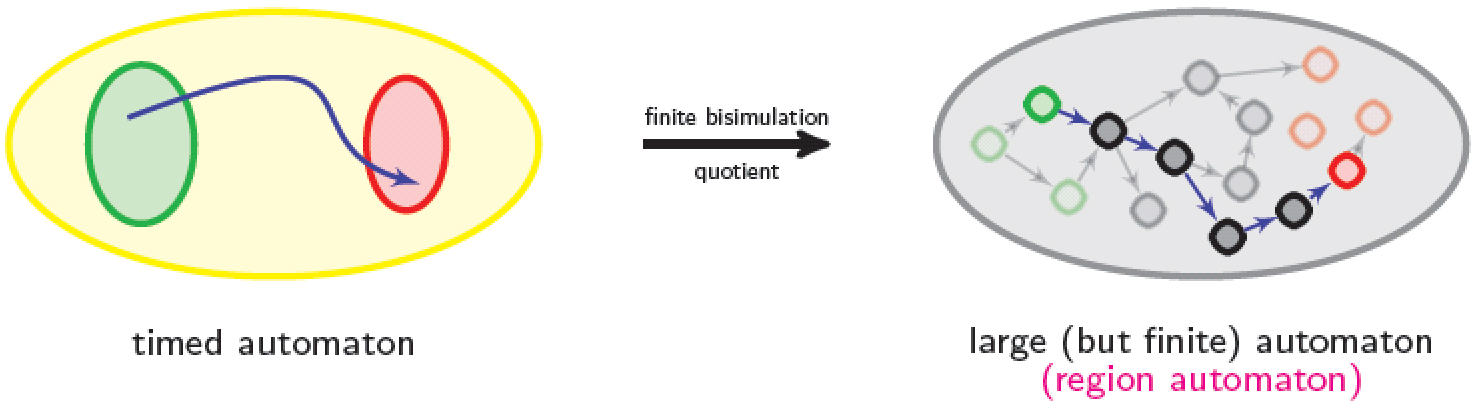
[AD94]







Region Automaton



LARGE: exponential in the number of clocks and in the constants (if encoded in binary). The number of regions is

$$\prod_{x \in X} (2M_x + 2) \cdot |X!| \cdot 2^{|X|}$$

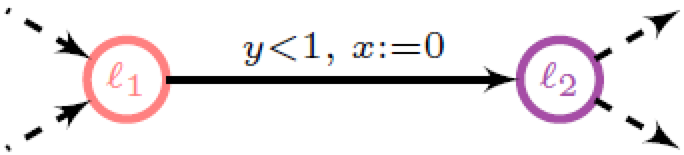
Fundamental Results

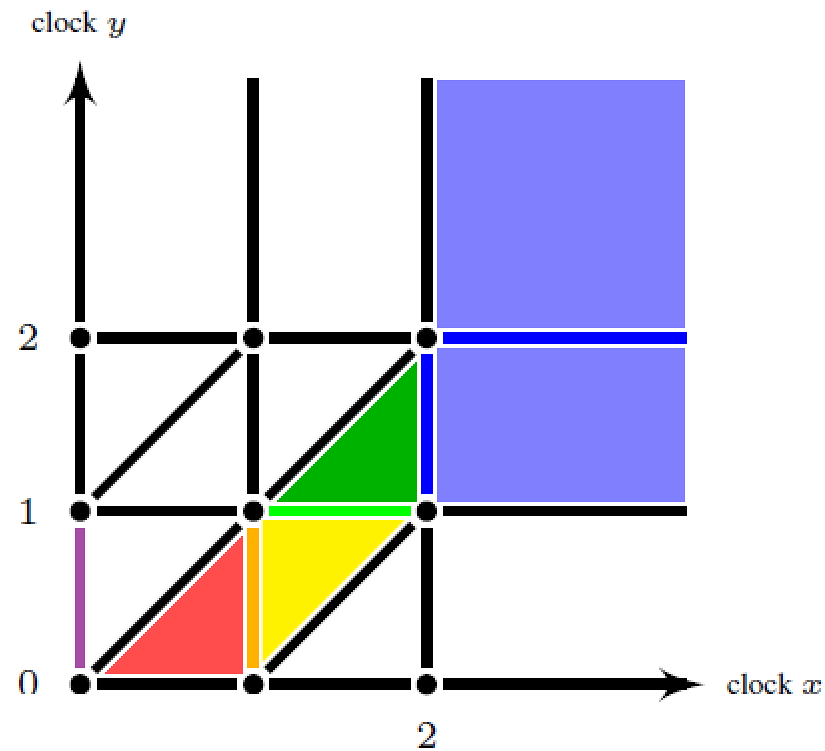
- Reachability ☺ PSPACE-c
- Model-checking
  - TCTL ☺ PSPACE-c ; MTL ☹ UNDECIDABLE ; MITL ☺ EXPSPACE-c
- Bisimulation, Simulation
  - Timed ☺ EXPTIME-c ; Untimed ☺
- Trace-inclusion
  - Timed ☹ UNDECIDABLE ; Untimed ☺ PSPACE-c

Symbolic Verification

The UPPAAL
Verification Engine

Regions – From Infinite to Finite

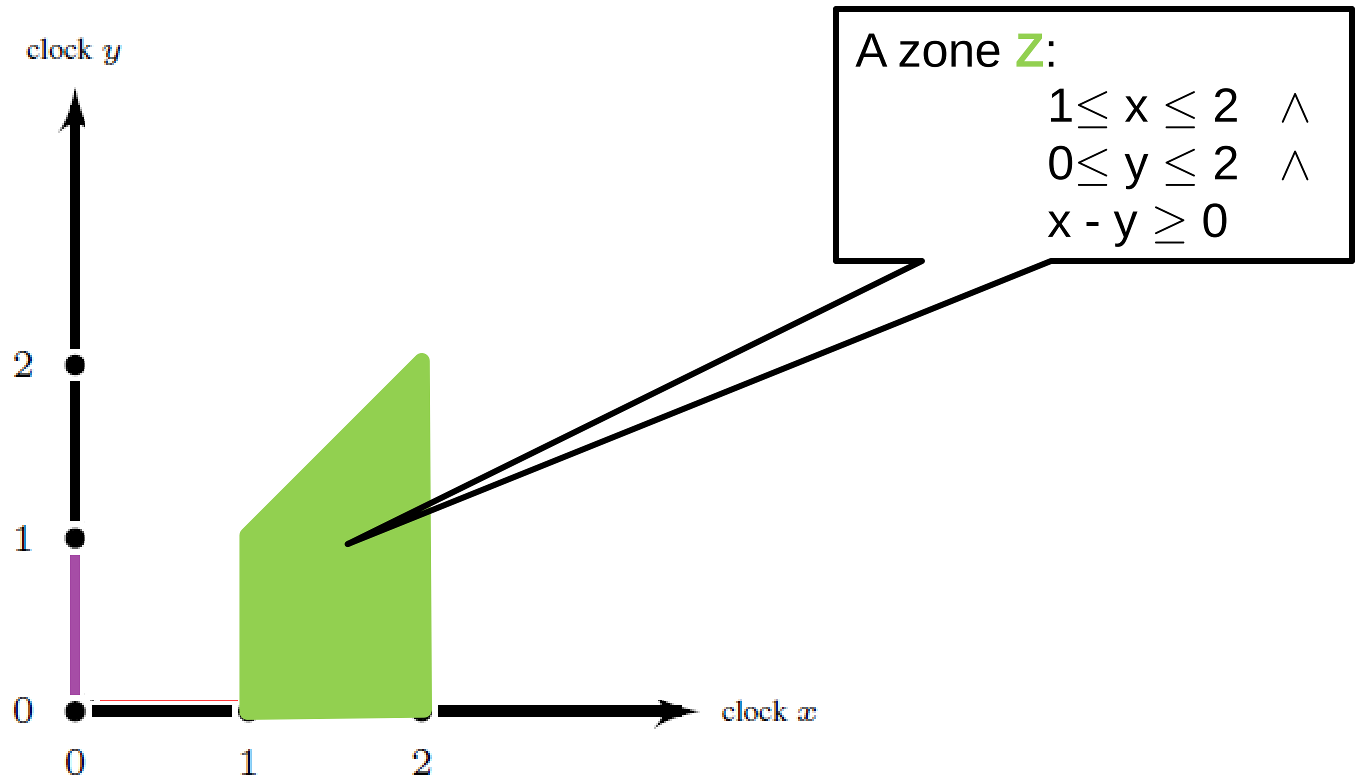




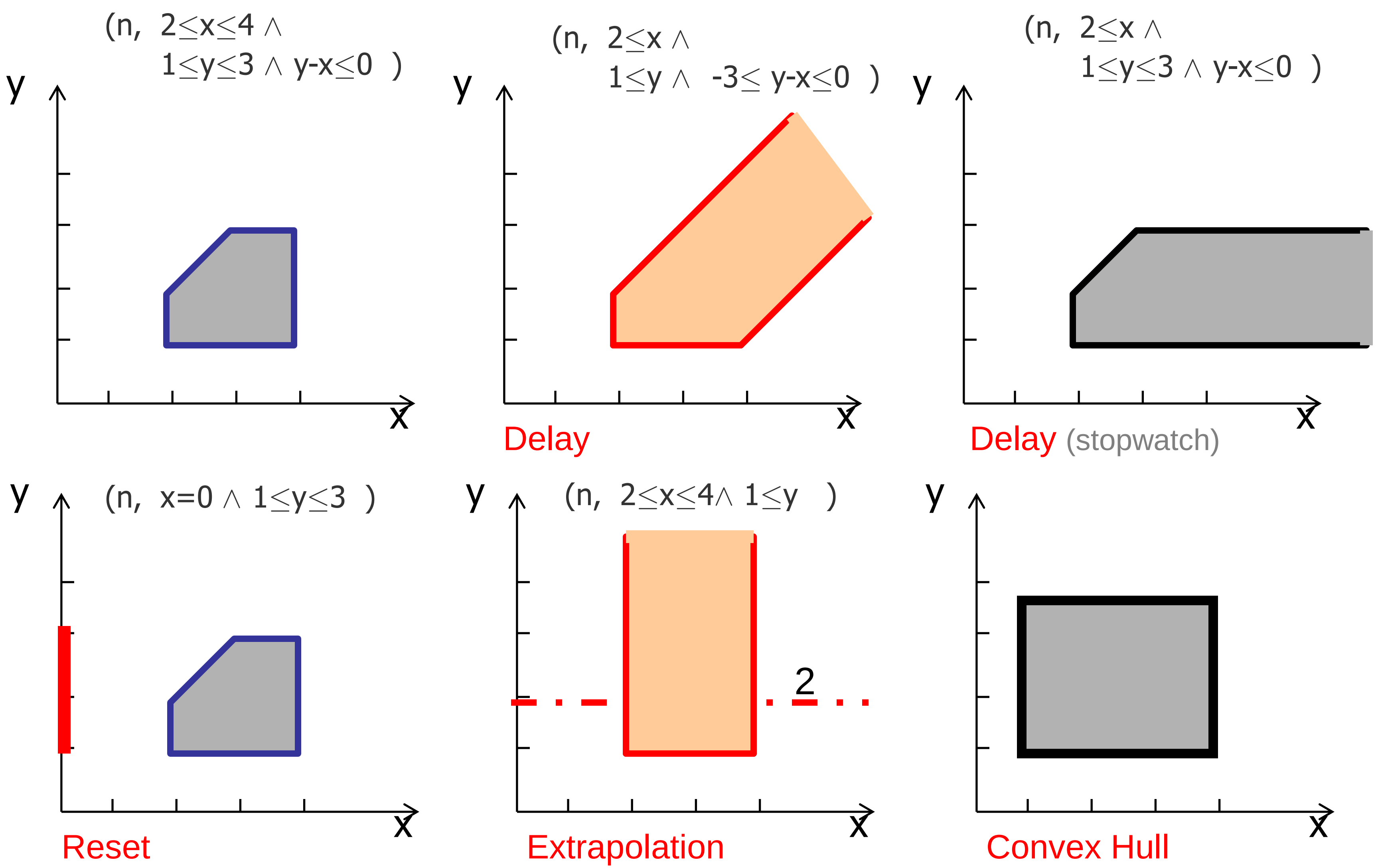
Theorem

The number of regions is $n! \cdot 2^n \cdot \prod_{x \in C}(2c_x + 2)$.

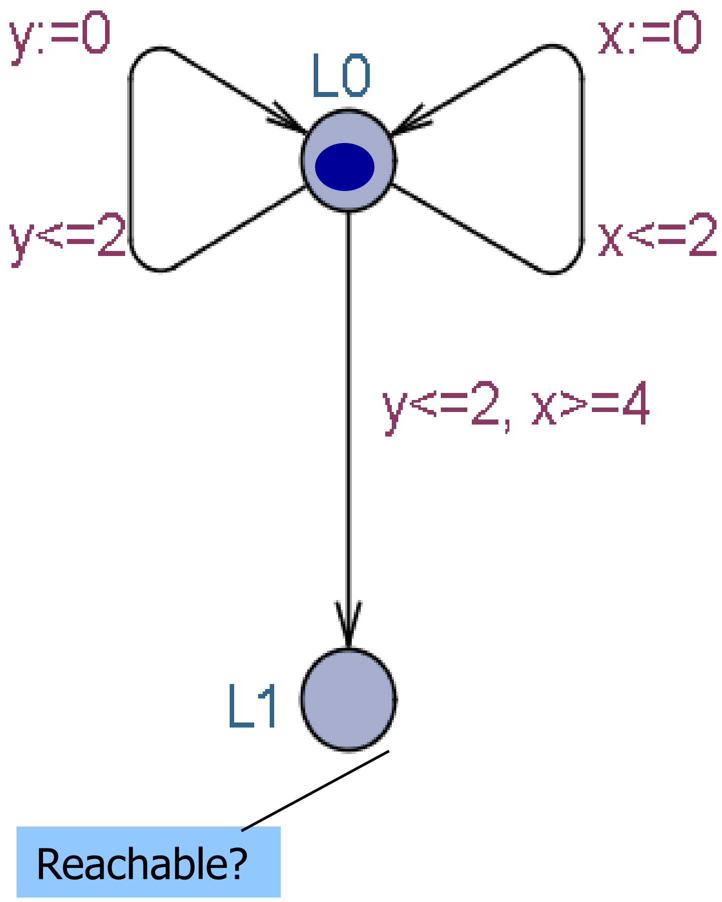
Zones – From Finite to Efficiency

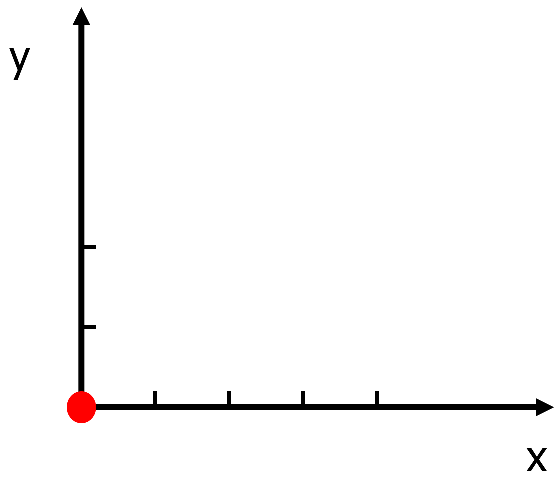


Zones – Operations

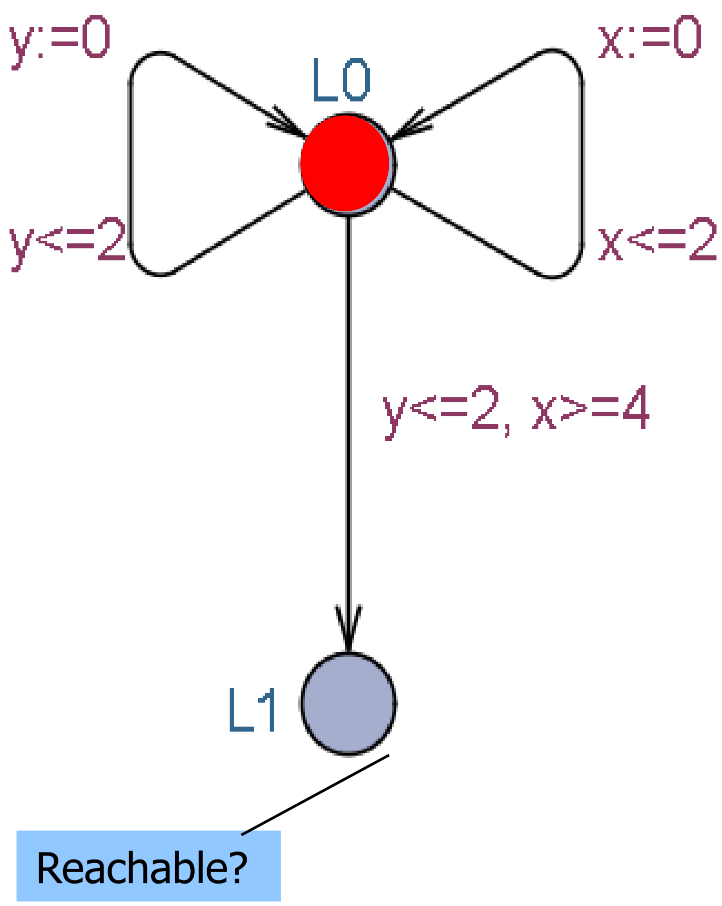


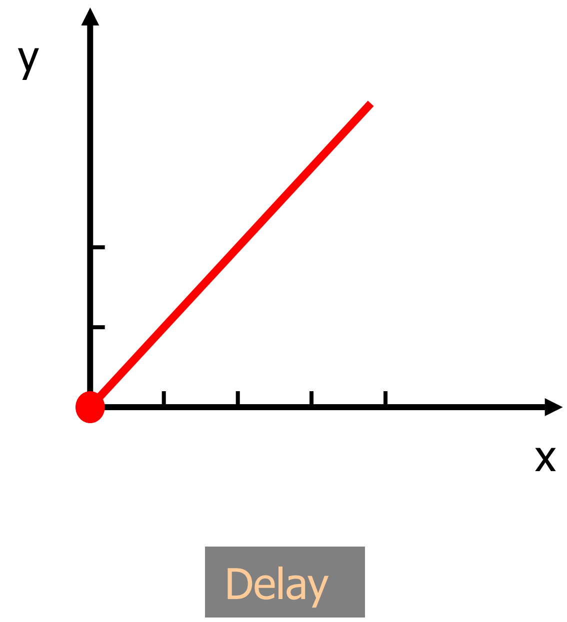
Symbolic Exploration



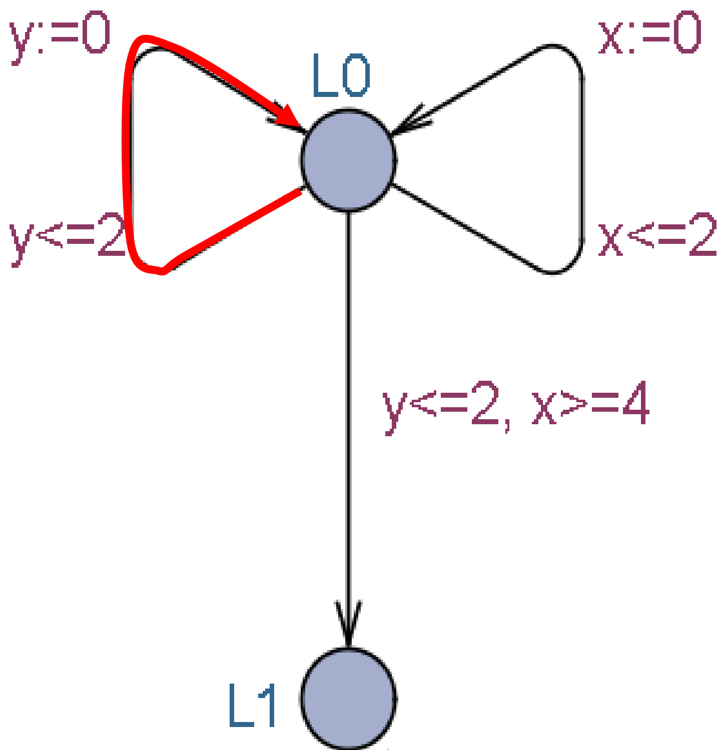


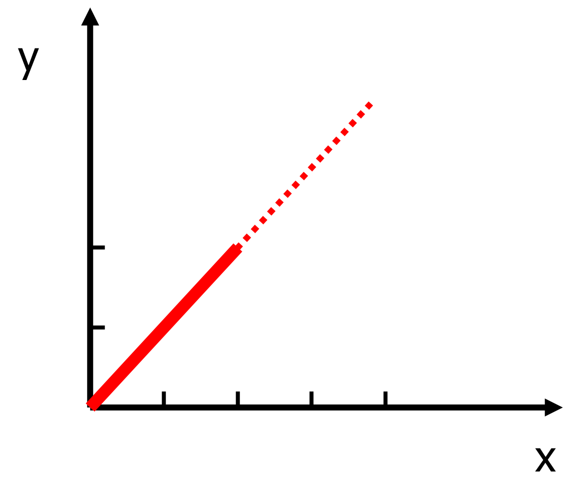
Symbolic Exploration





Symbolic Exploration

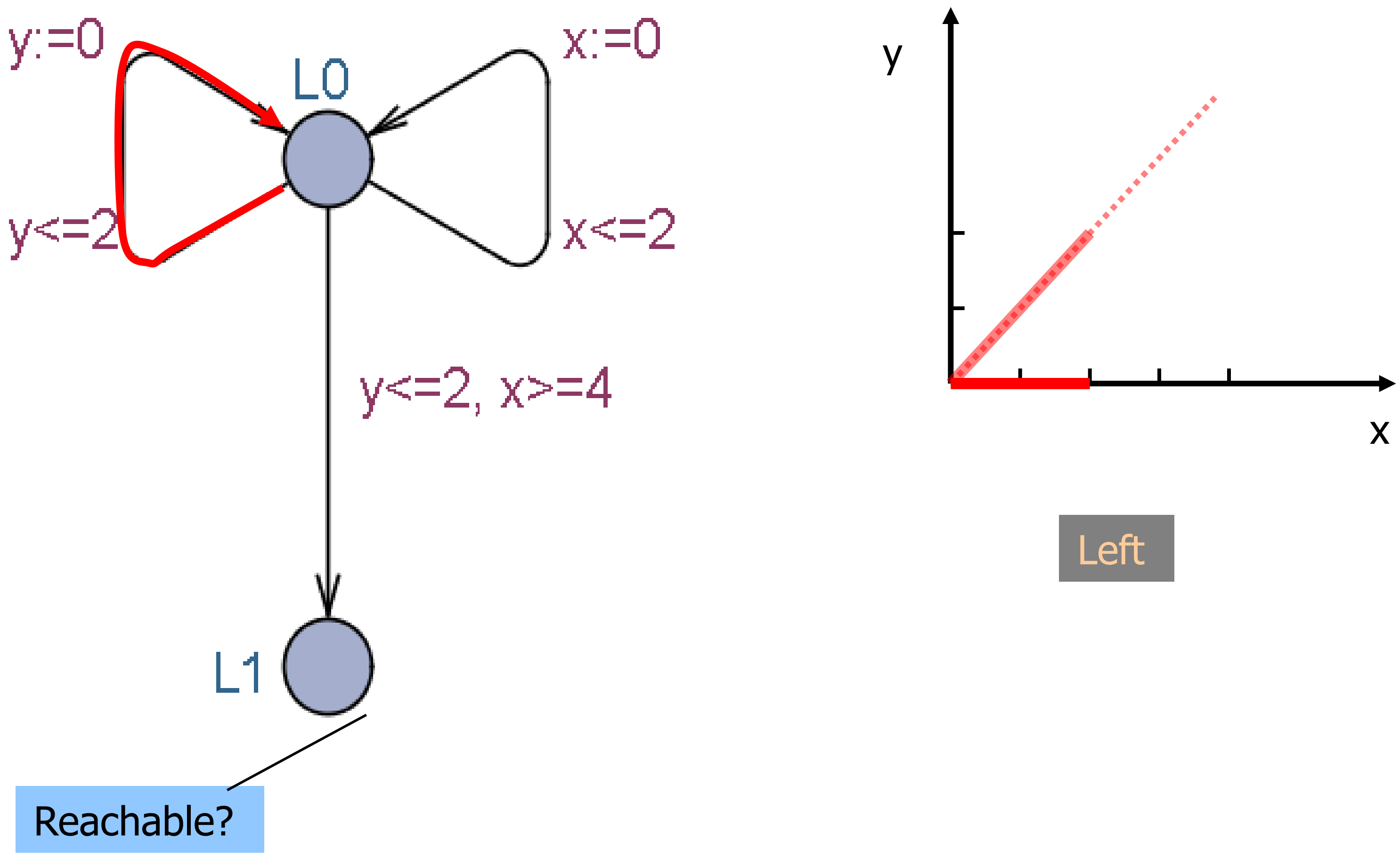




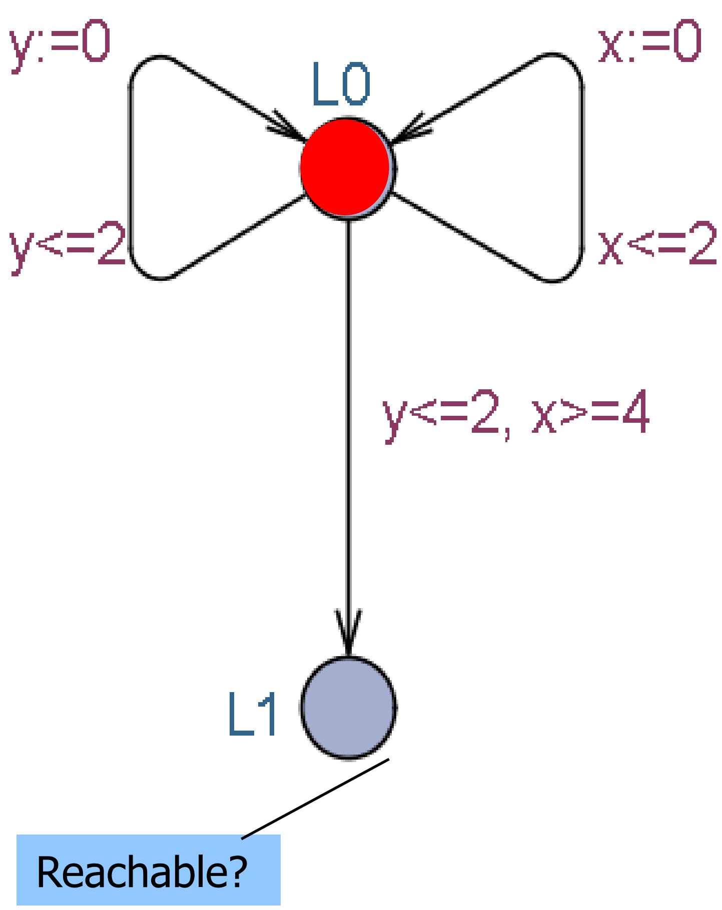
Left

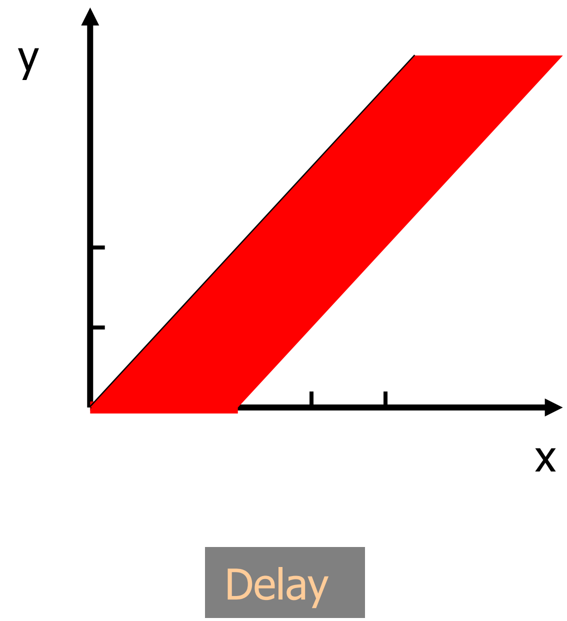
Reachable?

Symbolic Exploration

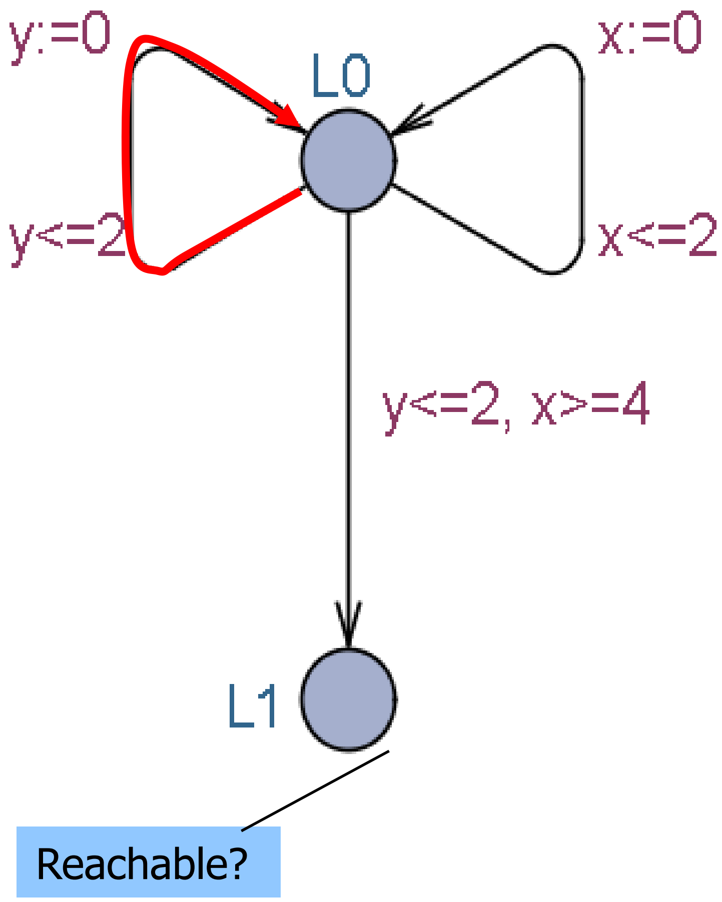


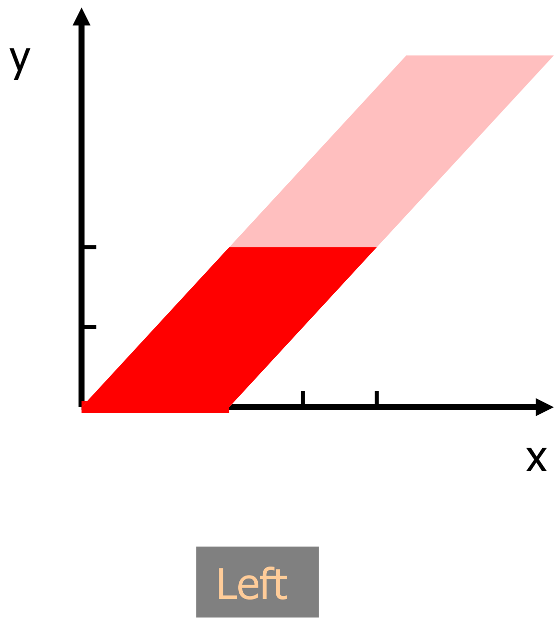
Symbolic Exploration



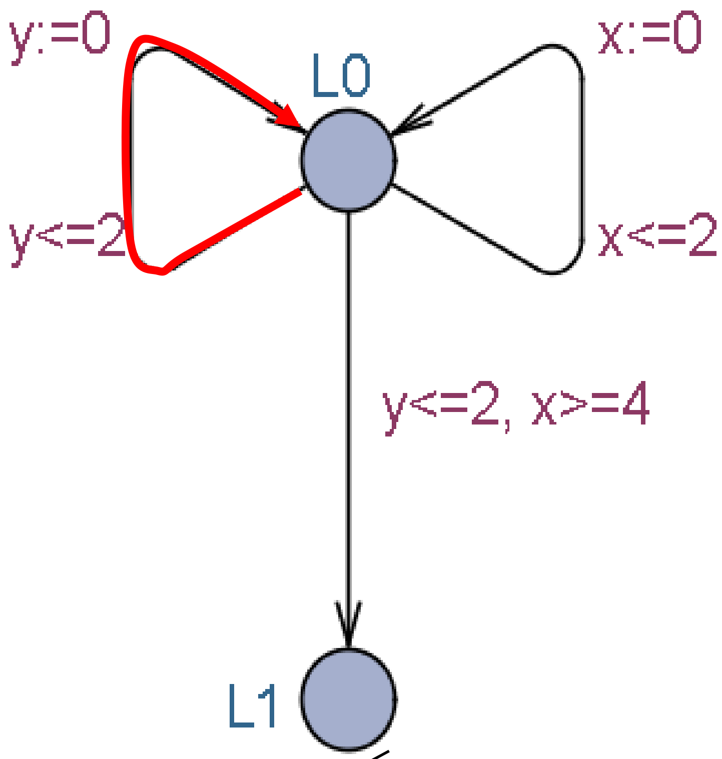


Symbolic Exploration

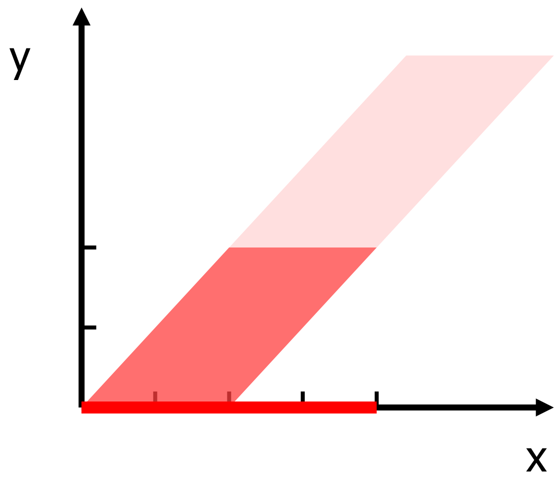




Symbolic Exploration

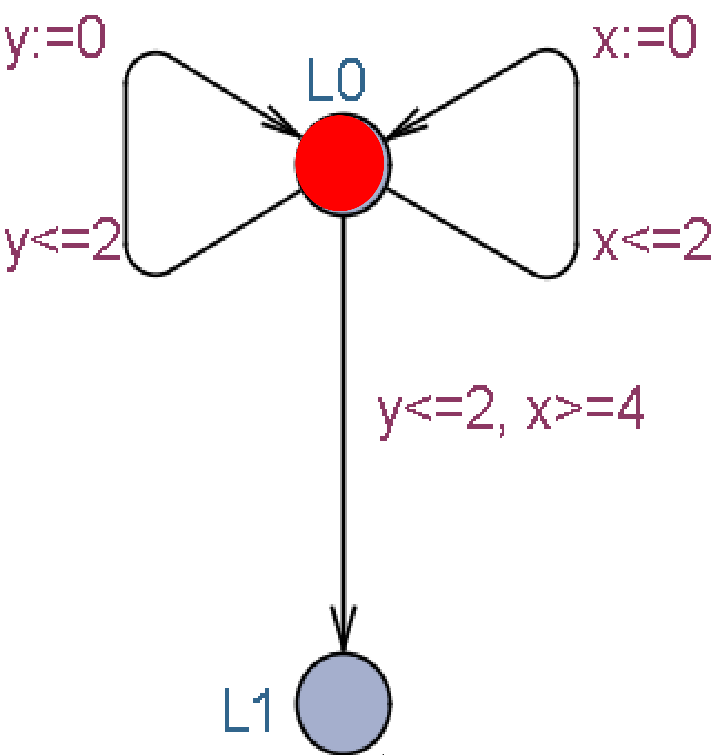


Reachable?

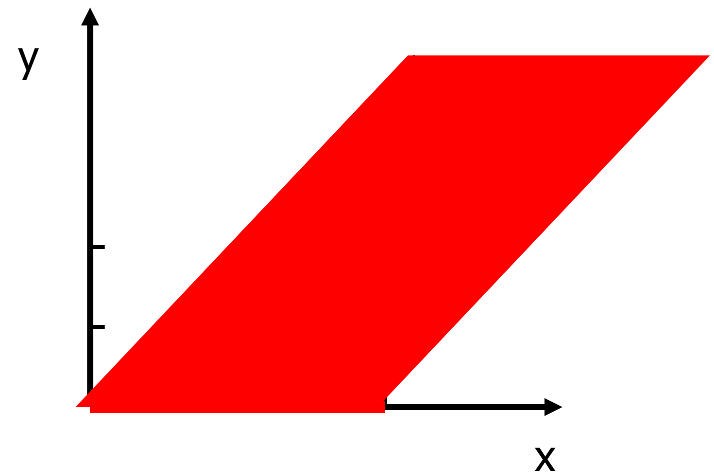


Left

Symbolic Exploration

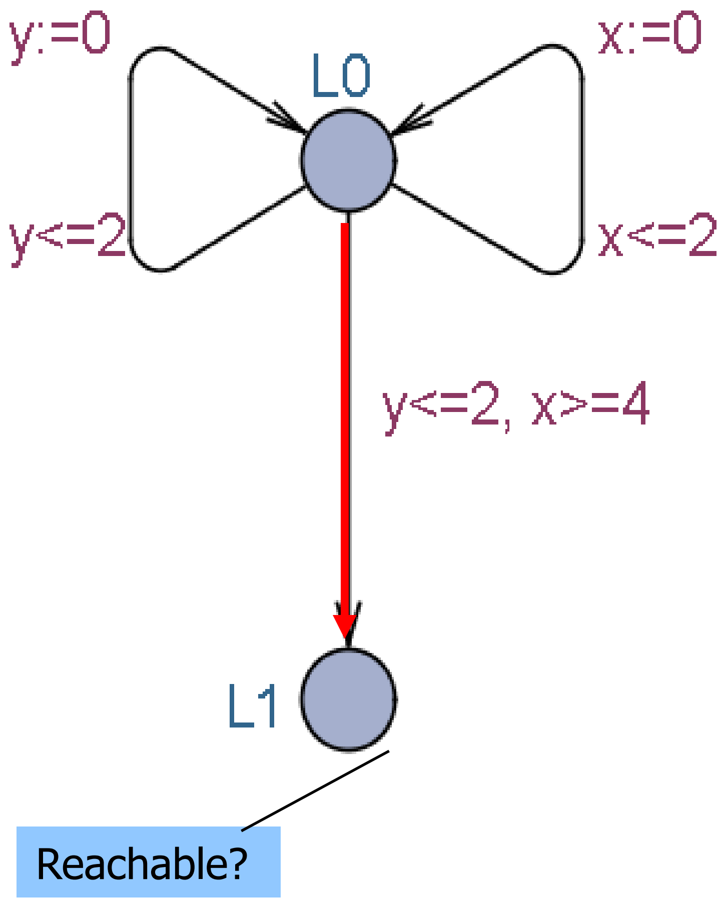


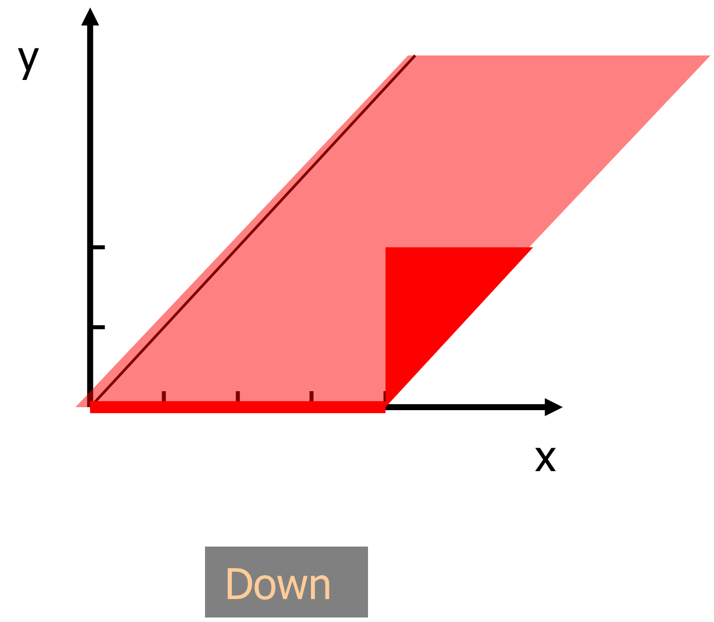
Reachable?



Delay

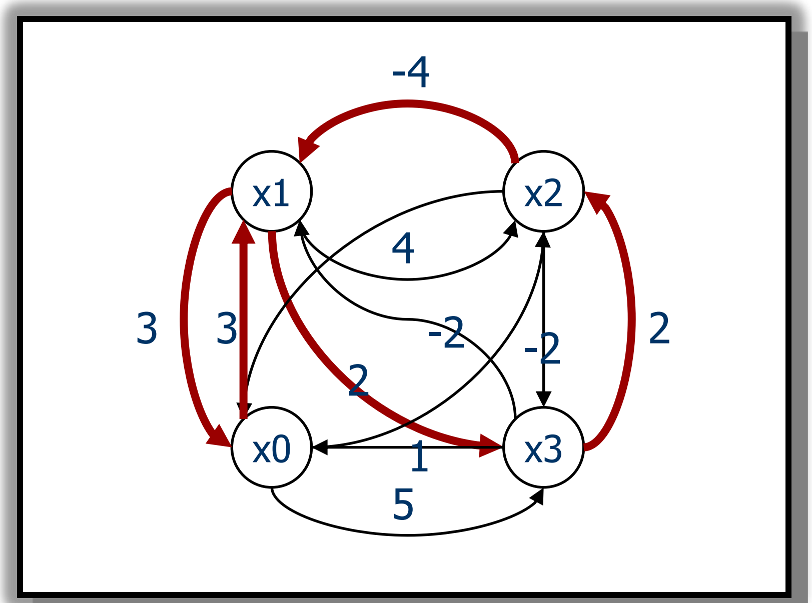
Symbolic Exploration

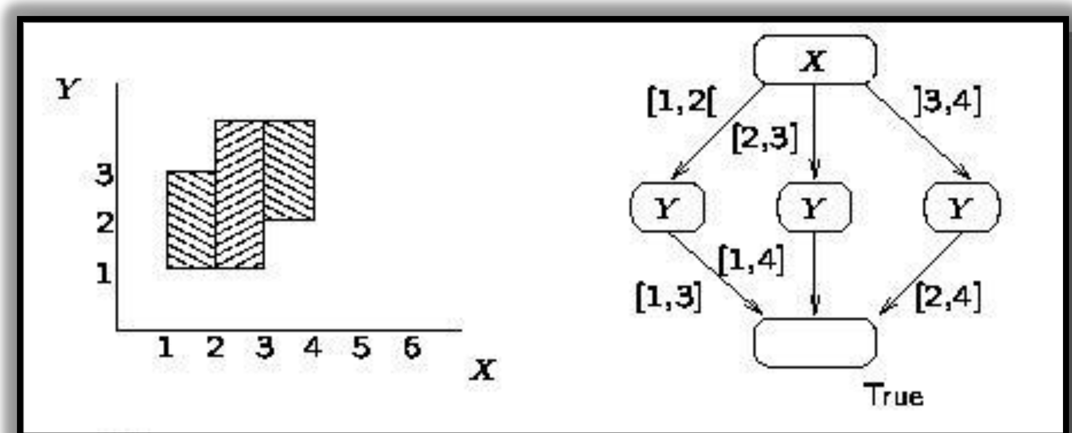




Datastructures for Zones

- Difference Bounded Matrices (DBMs)
- Minimal Constraint Form
  [RTSS97]
- Clock Difference Diagrams
  [CAV99]





Inclusion Checking (DBMs)

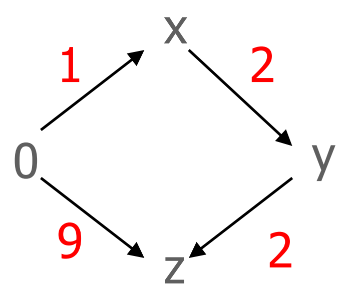
Bellman 1958, Dill 1989

Inclusion

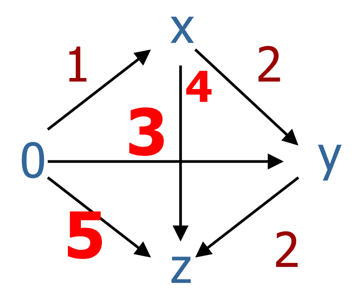
D1

x<=1
y-x<=2
z-y<=2
z<=9

Graph



Shortest Path Closure

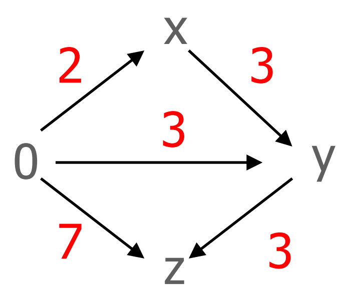


? ⊆ **?**

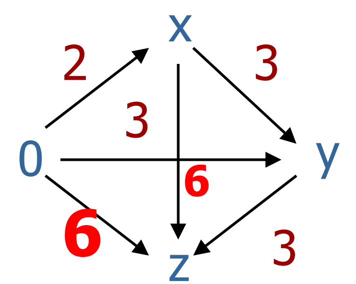
D2

x<=2
y-x<=3
y<=3
z-y<=3
z<=7

Graph

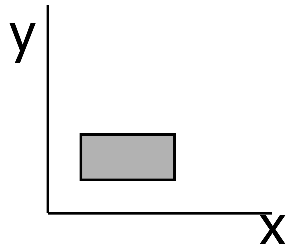


Shortest Path Closure

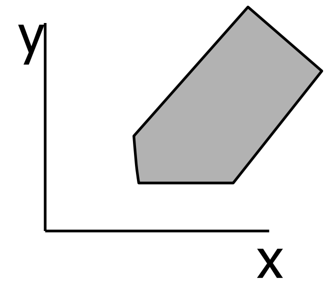


Future (DBMs)

D

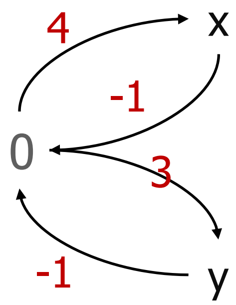


1<= x <=4
1<= y <=3

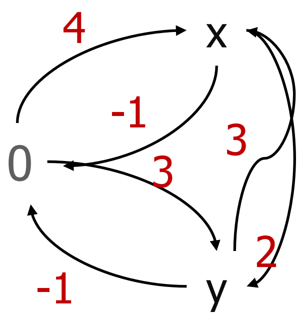


Future D

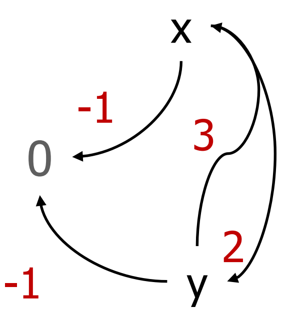
1<=x, 1<=y
-2<=x-y<=3



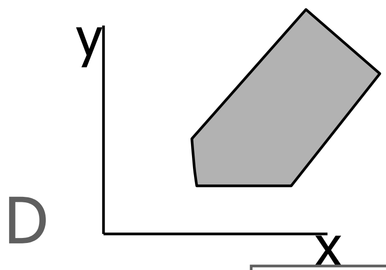
Shortest Path Closure



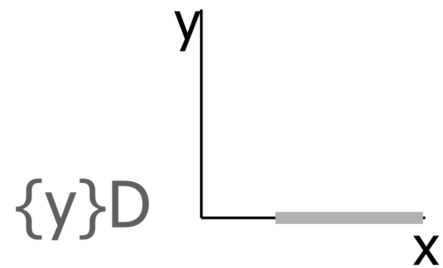
Remove upper bounds on clocks



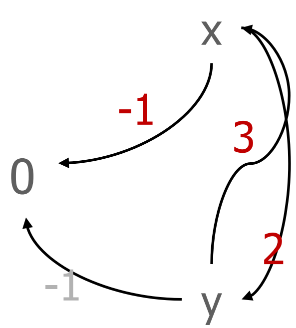
Reset (DBMs)



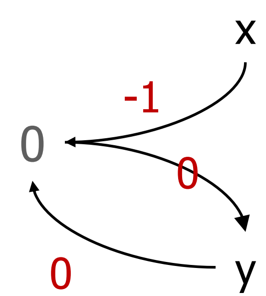
1<=x, 1<=y
-2<=x-y<=3



y=0, 1<=x

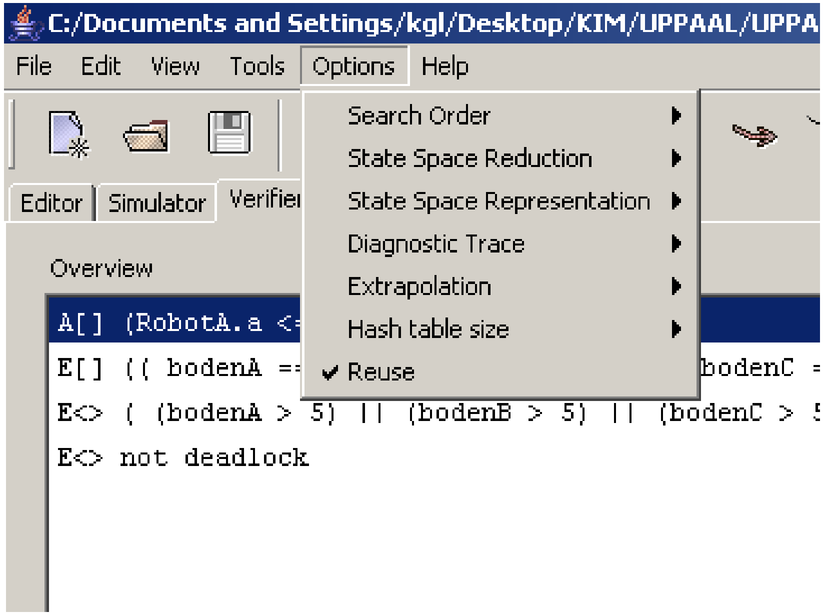


Remove all bounds involving y and set y to 0



Verification Options

Verification Options



Search Order
- Depth First
- Breadth First

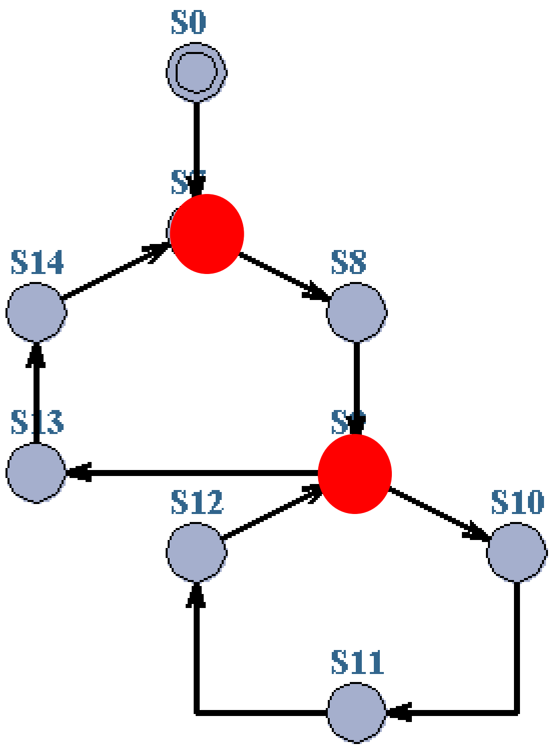
State Space Reduction
- None
- Conservative
- Aggressive

State Space Representation
- DBM
- Compact Form
- Under Approximation
- Over Approximation

Diagnostic Trace
- Some
- Shortest
- Fastest

Extrapolation
Hash Table size
Reuse

State Space Reduction



Cycles:

Only symbolic states involving loop-entry points need to be saved on Passed list

To Store or Not To Store

Behrmann, Larsen, Pelanek 2003

117 states$_{total}$

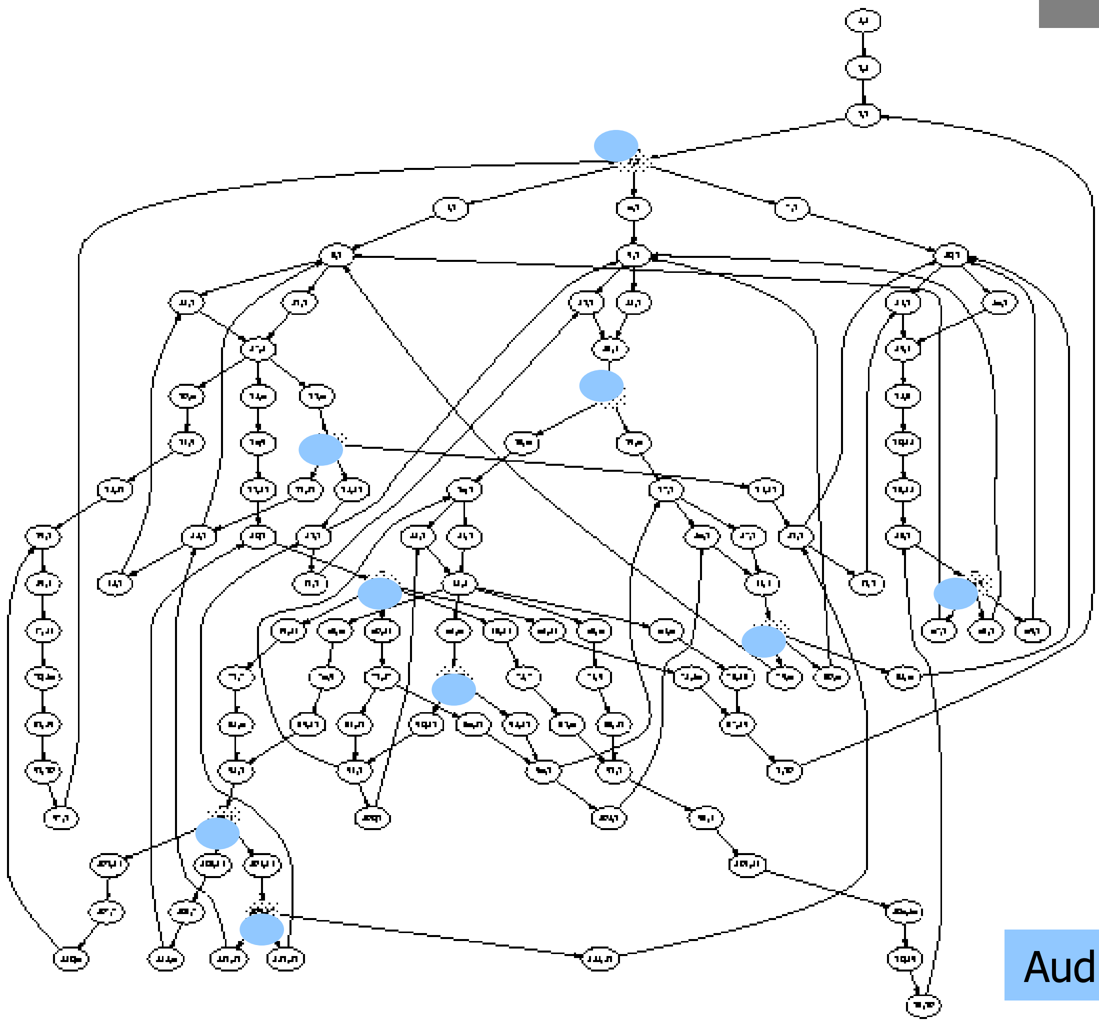
$\rightarrow$

81 states$_{entrypoint}$

$\rightarrow$

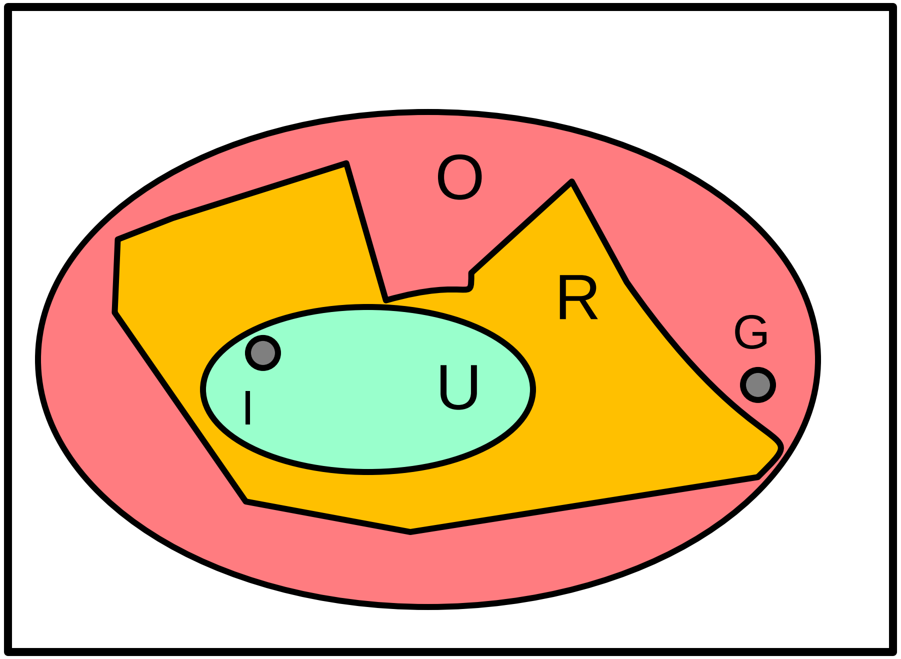
9 states

Time OH
less than 10%



Audio Protocol

Over/Under Approximation



Declared State Space

Question:

$G \in R$?

How to use:

$G \in O$?

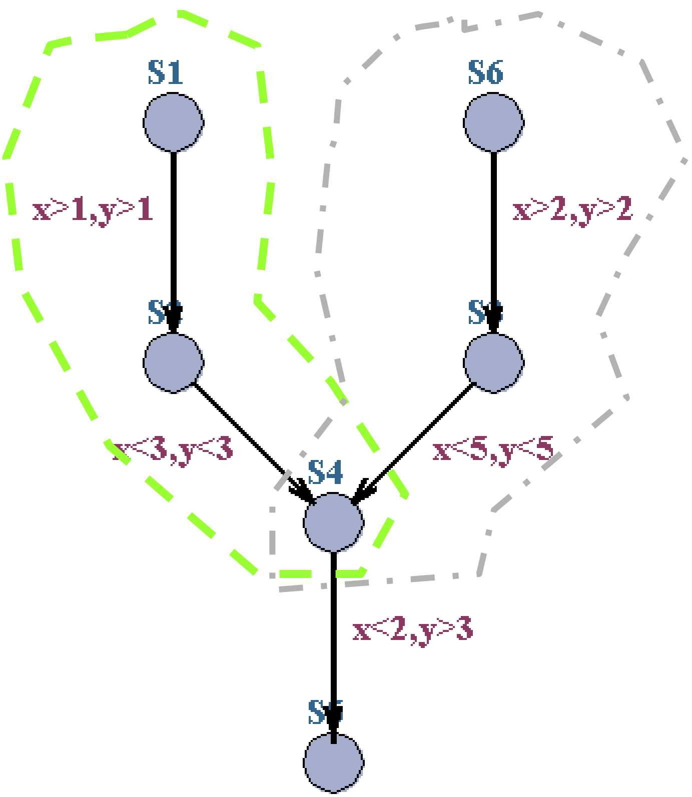
$G \in U$?

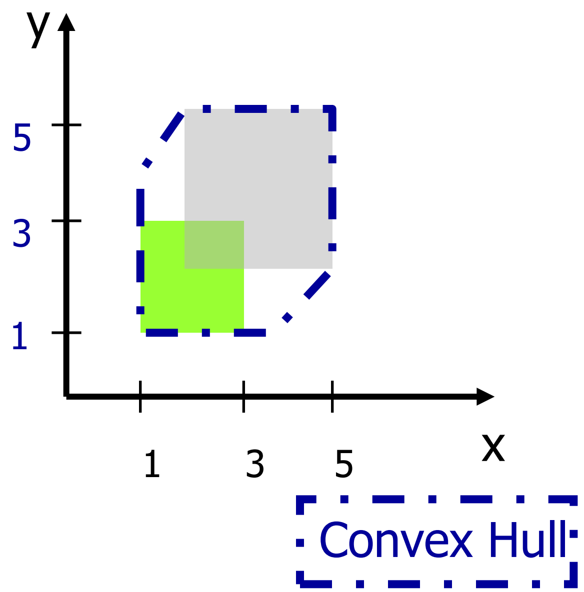
$G \in U \Rightarrow G \in R$

$\neg(G \in O) \Rightarrow \neg(G \in R)$

Over-approximation

Convex Hull

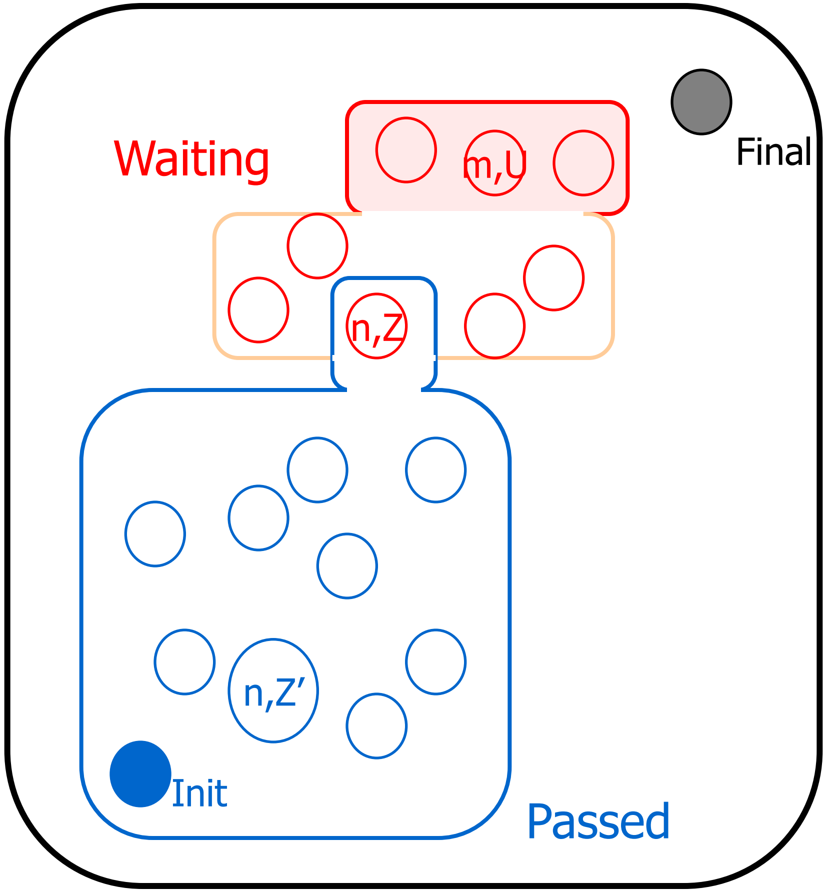




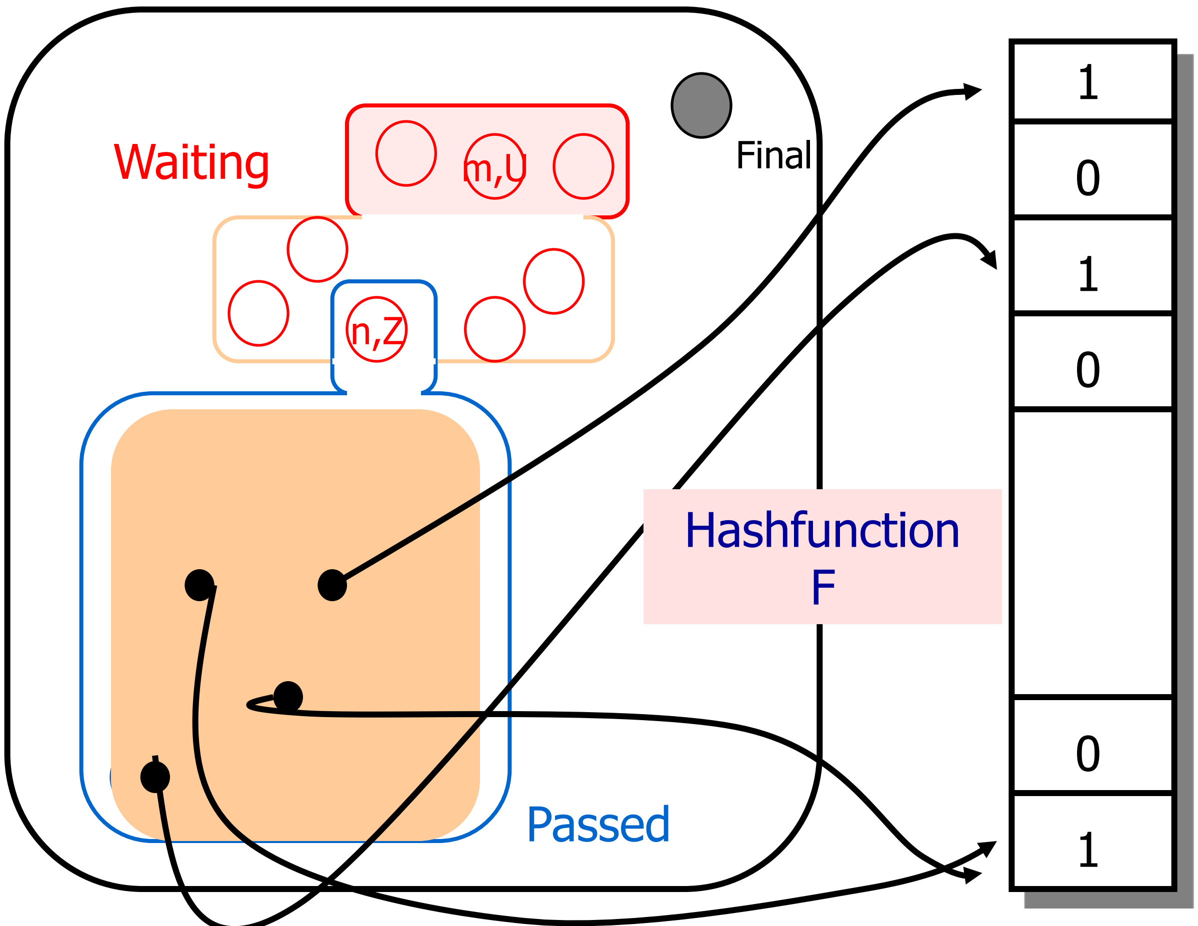
TACAS04: An EXACT method performing as well as Convex Hull has been developed based on abstractions taking max constants into account distinguishing between clocks, locations and $\leq$ & $\geq$

Under-approximation

Bitstate Hashing



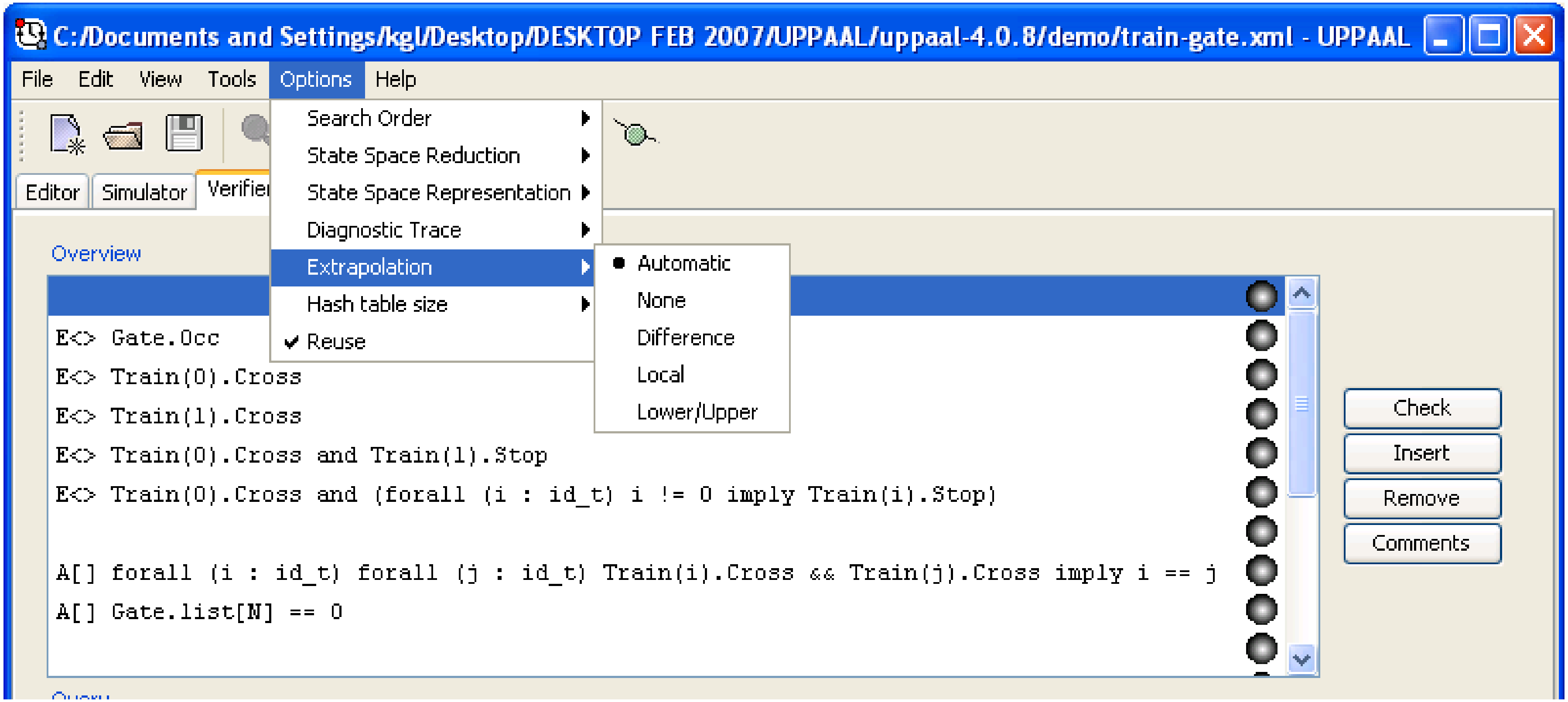
Under-approximation
Bitstate Hashing



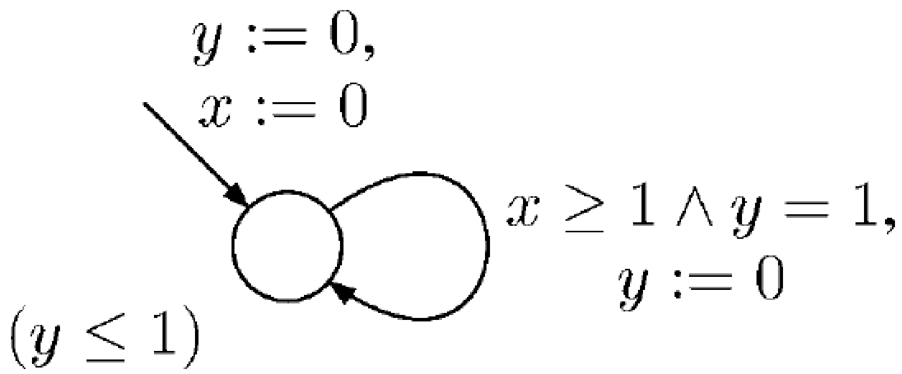
Passed=
Bitarray

UPPAAL
4 - 512 Mbits

Extrapolation

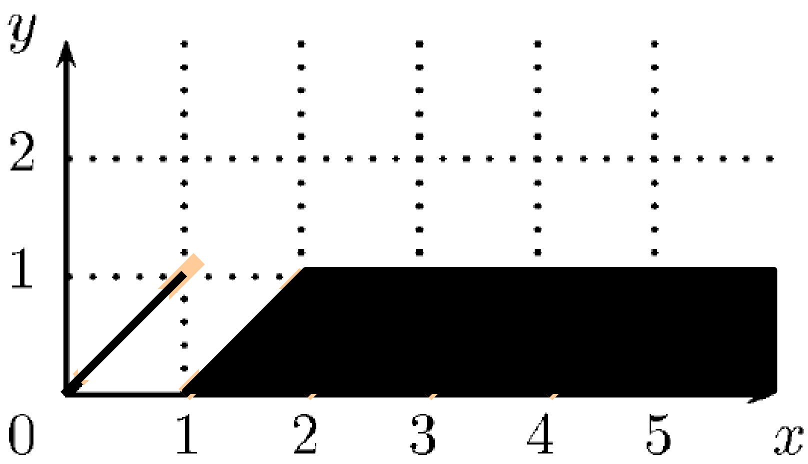


Forward Symbolic Exploration



TERMINATION not garanteed

Need for Finite Abstractions



Abstractions

$$a : \mathcal{P}(R_{\geq 0}^{X}) \hookrightarrow \mathcal{P}(R_{\geq 0}^{X}) \text{ such that } W \subseteq a(W)$$

$$\frac{(\ell, W) \Rightarrow (\ell', W')}{(\ell, W) \Rightarrow_a (\ell', a(W'))} \quad \text{if } W = a(W)$$

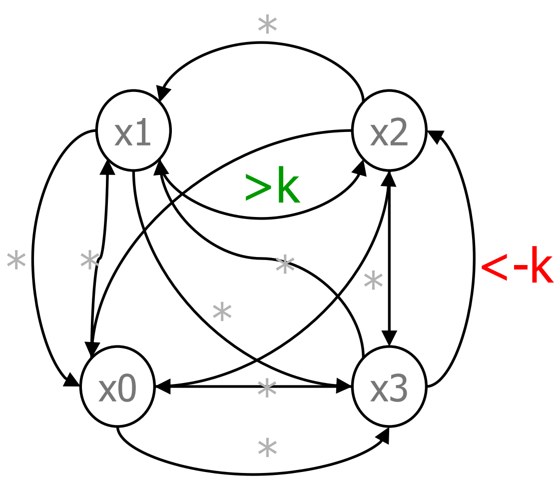
We want $\Rightarrow_a$ to be:

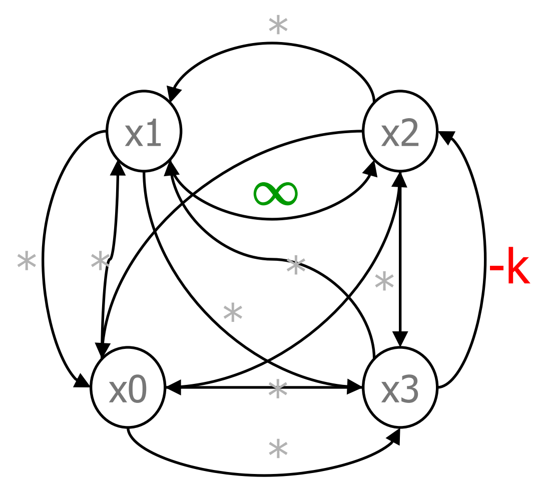
- sound & complete wrt reachability
- finite
- easy to compute
- as coarse as possible

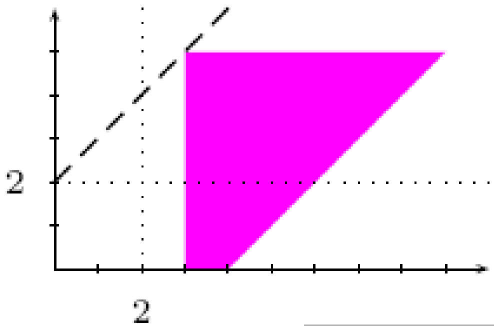
Abstraction by Extrapolation

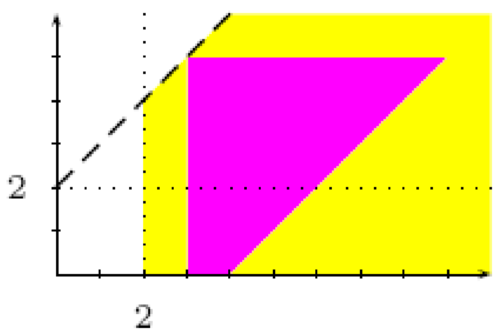
[Daws,Tripakis 98]

Let *k* be the largest constant appearing in the TA





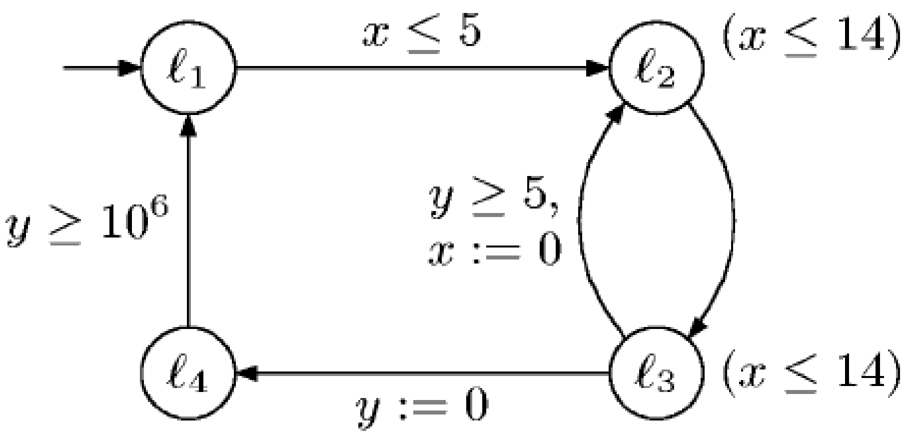




Sound & Complete
Ensures Termination

Location Dependency

[Behrmann, Bouyer, Fleury, Larsen 03]



$k_x = 5 \;\; k_y = 10^6$

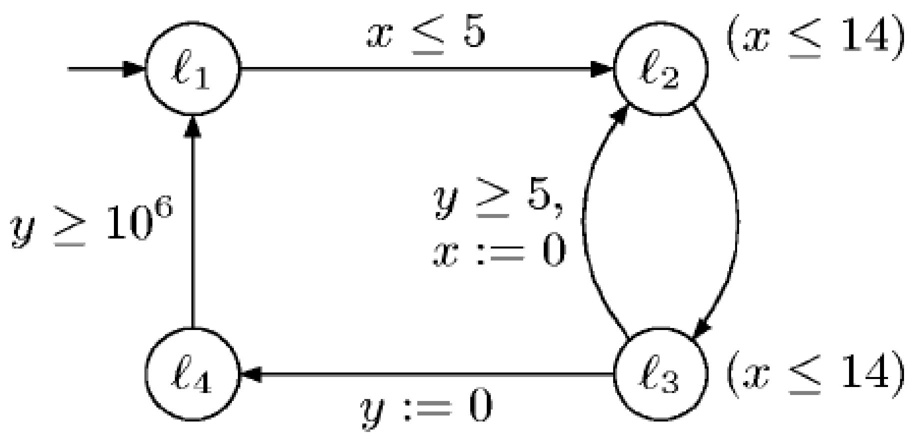
Will generate all symbolic states of the form

$(l_2,\ x \in [0,14]\ ,\ y \in [5,14n]\ ,\ y-x \in [5,14n-14])$

for $n \leq 10^6/14$!!

But $y \geq 10^6$ is not RELEVANT in l_2

Location Dependent Constants



$k_x = 5 \quad k_y = 10^6$

k_x^i	$= 14$	for $i \in \{1,2,3,4\}$
k_y^i	$= 5$	for $i \in \{1,2,3\}$
k_y^4	$= 10^6$	

k_j^i may be found as solution to simple linear constraints!

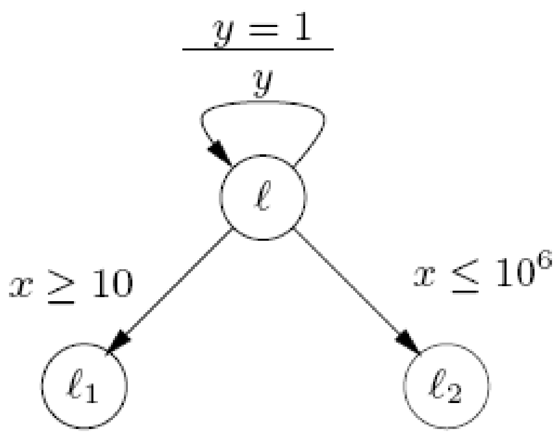
Active Clock Reduction:
$k_j^i = -\infty$

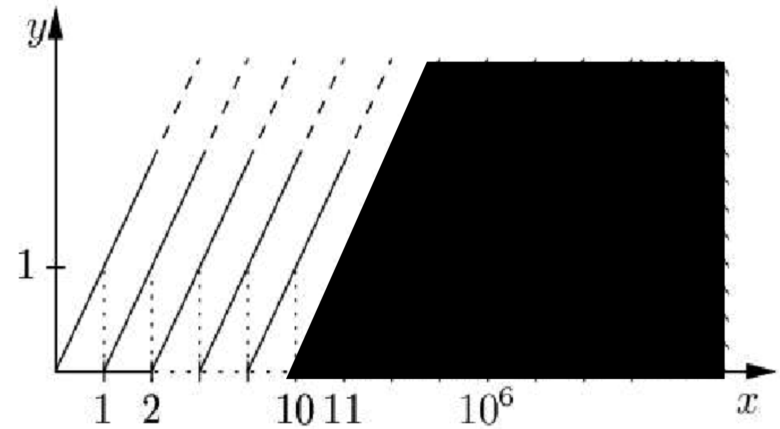
Experiments

	Constant BIG	Global Method	Active-clock Reduction	Local Constants
Naive Example	10^3	0.05s/1MB	0.05s/1MB	0.00s/1MB
	10^4	4.78s/3MB	4.83s/3MB	0.00s/1MB
	10^5	484s/13MB	480s/13MB	0.00s/1MB
	10^6	stopped	stopped	0.00s/1MB
Two Processes	10^3	3.24s/3MB	3.26s/3MB	0.01s/1MB
	10^4	5981s/9MB	5978s/9MB	0.37s/2MB
	10^5	stopped	stopped	72s/5MB
Asymmetric Fischer	10^3	0.01s/1MB	0.01s/1MB	0.01s/1MB
	10^4	2.20s/3MB	2.20s/3MB	0.85s/2MB
	10^5	333s/19MB	333s/19MB	160s/13MB
	10^6	33307s/122MB	33238s/122MB	16330s/65MB
Bang & Olufsen	25000	stopped	159s/243MB	123s/204MB

Lower and Upper Bounds

[Behrmann, Bouyer, Larsen, Pelanek 04]





$k_x^l = 10^6$

Given that $x \leq 10^6$ is an *upper* bound implies that

(l, v_x, v_y) *simulates* (l, v'_x, v_y)

whenever $v'_x \geq v_x \geq 10$.

For reachability downward closure wrt simulation suffices!

Simulation

$\preccurlyeq$ is the largest relation satisfying

1. if $(\ell_1, \nu_1) \preccurlyeq (\ell_2, \nu_2)$ then $\ell_1 = \ell_2$
2. if $(\ell_1, \nu_1) \preccurlyeq (\ell_2, \nu_2)$ and $(\ell_1, \nu_1) \longrightarrow (\ell_1', \nu_1')$, then there exists (ℓ_2', ν_2') such that $(\ell_2, \nu_2) \longrightarrow (\ell_2', \nu_2')$ and $(\ell_1', \nu_1') \preccurlyeq (\ell_2', \nu_2')$
3. if $(\ell_1, \nu_1) \preccurlyeq (\ell_2, \nu_2)$ and $(\ell_1, \nu_1) \xrightarrow{\epsilon(\delta)} (\ell_1, \nu_1 + \delta)$, then there exists δ' such that $(\ell_2, \nu_2) \xrightarrow{\epsilon(\delta')} (\ell_2, \nu_2 + \delta')$ and $(\ell_1, \nu_1 + \delta) \preccurlyeq (\ell_2, \nu_2 + \delta')$

Proposition

If $(\ell, \nu_1) \preccurlyeq (\ell, \nu_2)$ and if a discrete state ℓ' is reachable from (ℓ, ν_1), then it is also reachable from (ℓ, ν_2).

Maximal Bounds

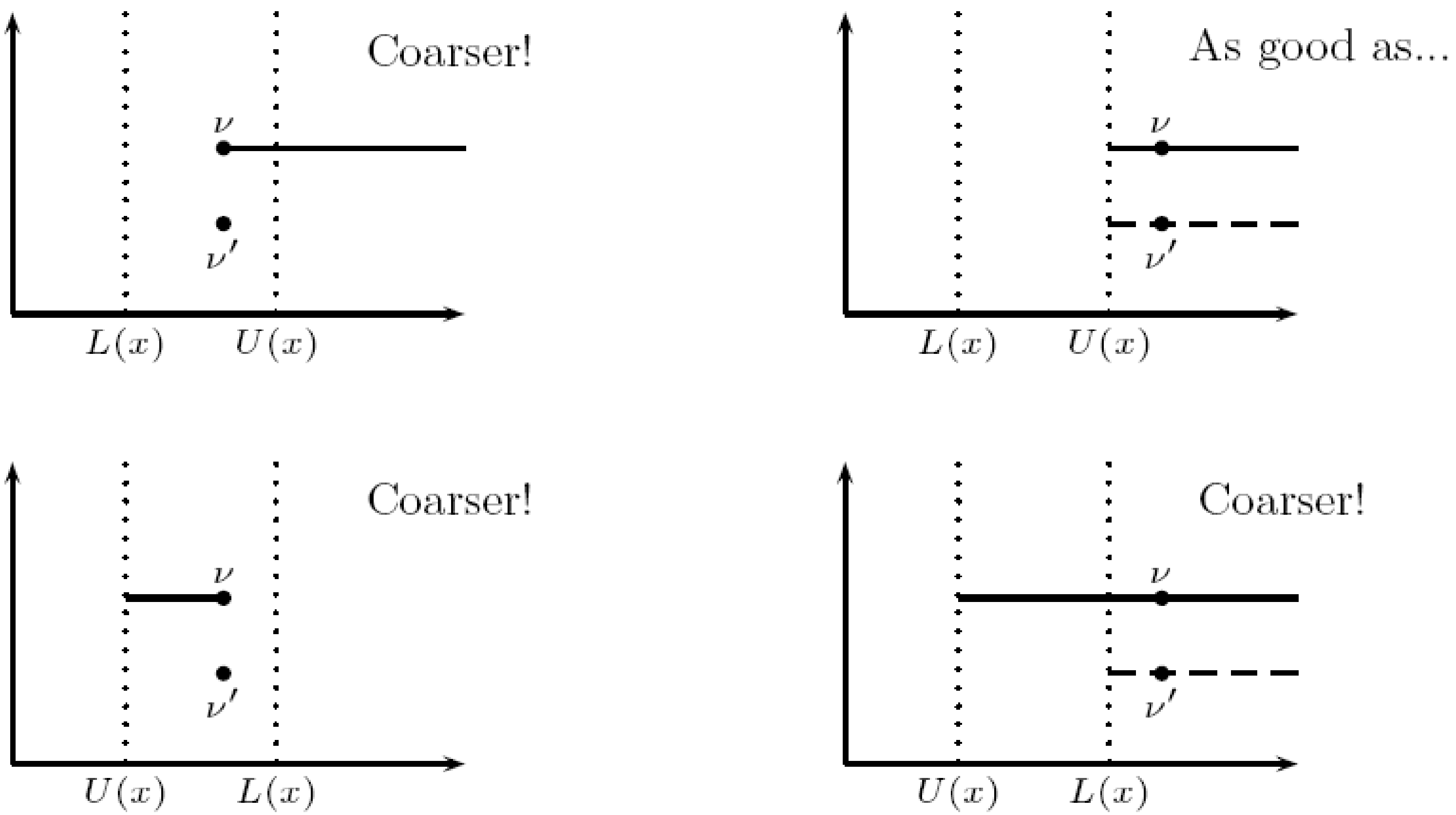
$M(x)$: the maximum constant k with $x \sim k$,
$L(x)$: the maximum constant k with $x\{\geq,>\}k$,
$U(x)$: the maximum constant k with $x\{\leq,<\}k$.

$$\nu \equiv_M \nu' \overset{\text{def}}{\iff}$$

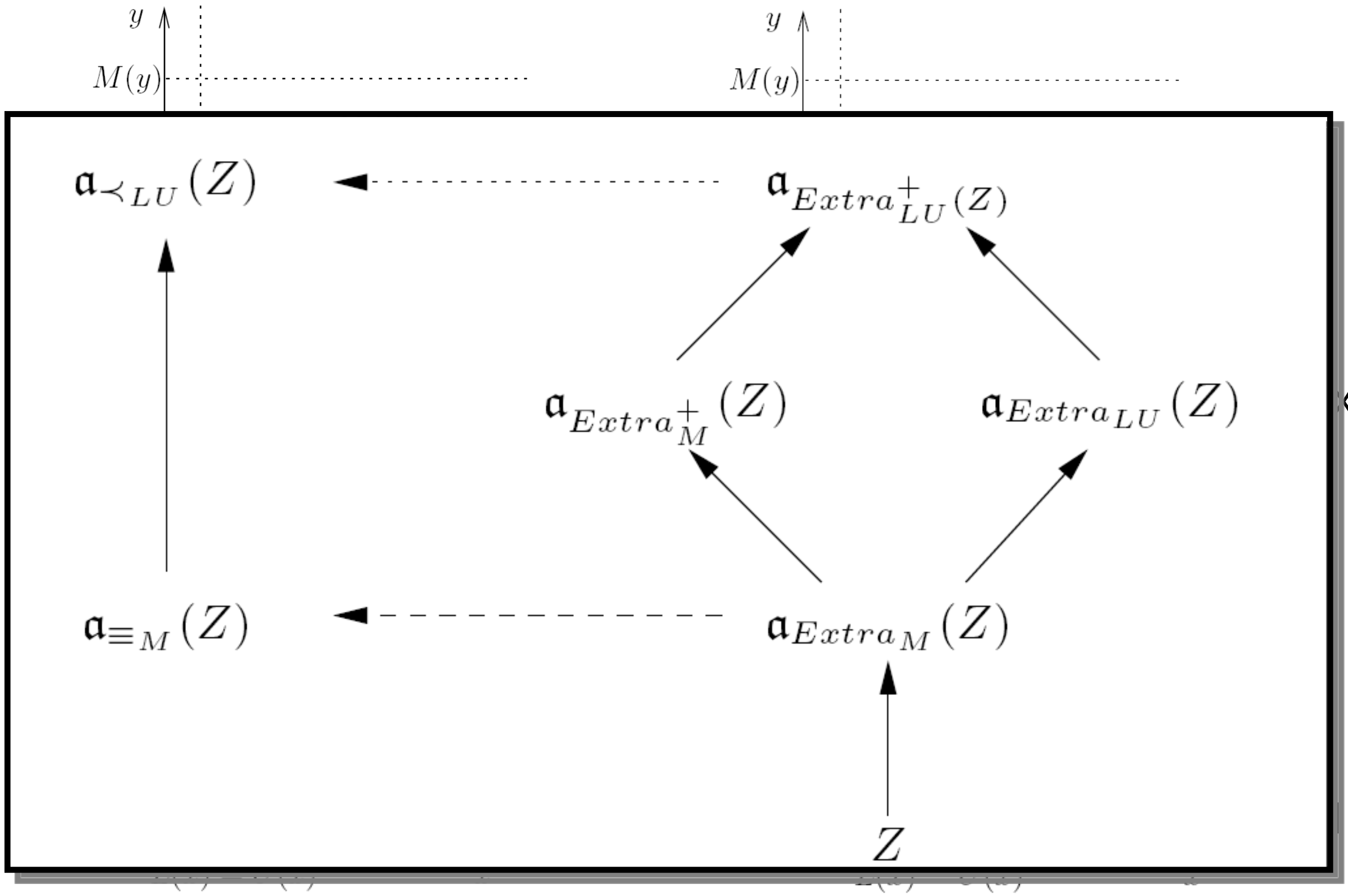
$$\forall x \in X : \text{either } \nu(x) = \nu'(x) \text{ or } \left(\nu(x) > M(x) \text{ and } \nu'(x) > M(x)\right)$$

$$\nu' \prec_{LU} \nu \quad \overset{\text{def}}{\iff} \quad \textit{for each clock } x, \begin{cases} \textit{either } \nu'(x) = \nu(x) \\ \textit{or } L(x) < \nu'(x) < \nu(x) \\ \textit{or } U(x) < \nu(x) < \nu'(x) \end{cases}$$

Maximum Bounds Abstraction



Extrapolation Using Zones



xtrapolation

w LU

Experiments

		Classical			Loc. dep. Max			Loc. dep. LU			Convex Hull		
		-n1			-n2			-n3			-A		
	Model	Time	States	Mem	Time	States	Mem	Time	States	Mem	Time	States	Mem
Fischer	f5	4.02	82,685	5	0.24	16,980	3	0.03	2,870	3	0.03	3,650	3
	f6	597.04	1,489,230	49	6.67	158,220	7	0.11	11,484	3	0.10	14,658	3
	f7				352.67	1,620,542	46	0.47	44,142	3	0.45	56,252	5
	f8							2.11	164,528	6	2.08	208,744	12
	f9							8.76	598,662	19	9.11	754,974	39
	f10							37.26	2,136,980	68	39.13	2,676,150	143
	f11							152.44	7,510,382	268			
CSMA/CD	c5	0.55	27,174	3	0.14	10,569	3	0.02	2,027	3	0.03	1,651	3
	c6	19.39	287,109	11	3.63	87,977	5	0.10	6,296	3	0.06	4,986	3
	c7				195.35	813,924	29	0.28	18,205	3	0.22	14,101	4
	c8							0.98	50,058	5	0.66	38,060	7
	c9							2.90	132,623	12	1.89	99,215	17
	c10							8.42	341,452	29	5.48	251,758	49
	c11							24.13	859,265	76	15.66	625,225	138
	c12							68.20	2,122,286	202	43.10	1,525,536	394
	bus	102.28	6,727,443	303	66.54	4,620,666	254	62.01	4,317,920	246	45.08	3,826,742	324
	philips	0.16	12,823	3	0.09	6,763	3	0.09	6,599	3	0.07	5,992	3
	sched	17.01	929,726	76	15.09	700,917	58	12.85	619,351	52	55.41	3,636,576	427

Related & Future Work

- DDD: Andersen et al.
- NDD: Asarin, Bozga, Kerbrat, Maler, Pnueli, Rasse.
- IDD: Strehl, Thiele.

- No efficient algorithm for FUTURE and RESET operation on CDD.
- No canonical form.

- An efficient, fully symbolic engine for TA is still missing!!

Additional "secrets"

- Sharing among symbolic states
  - location vector / discrete values / zones
- Distributed implementation of UPPAAL
- Symmetry Reduction
- Sweep Line Method
- Guiding wrt Heuristic Value
  - User-supplied / Auto-generated
- Slicing wrt "C" Code

Open Problems

- Fully symbolic exploration of TA (both discrete and continuous part) ?
- Canonical form for CDD's ?
- Partial Order Reduction ?
- Compositional Backwards Reachability ?
- Bounded Model Checking for TA ?
- Exploitation of multi-core processors ?
- …