Symbolic Reachability and Beyound

or how UPPAAL really works

Kim Guldstrand Larsen

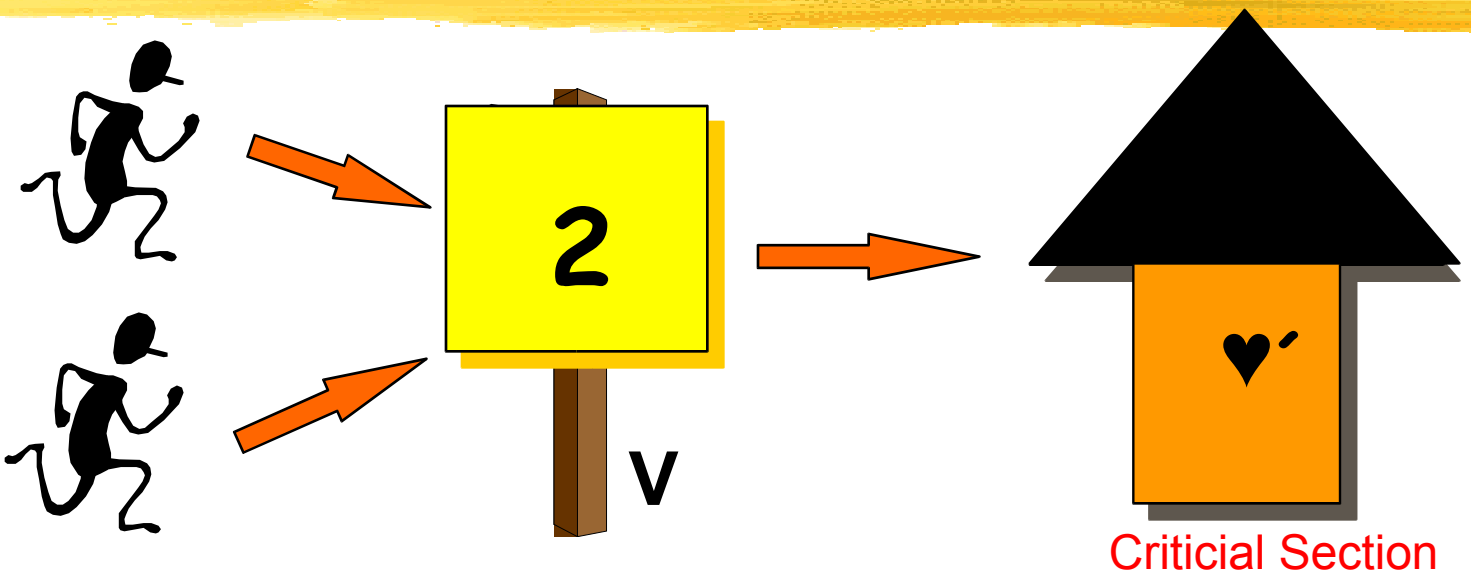
BRICS@Aalborg

REGIONS

review

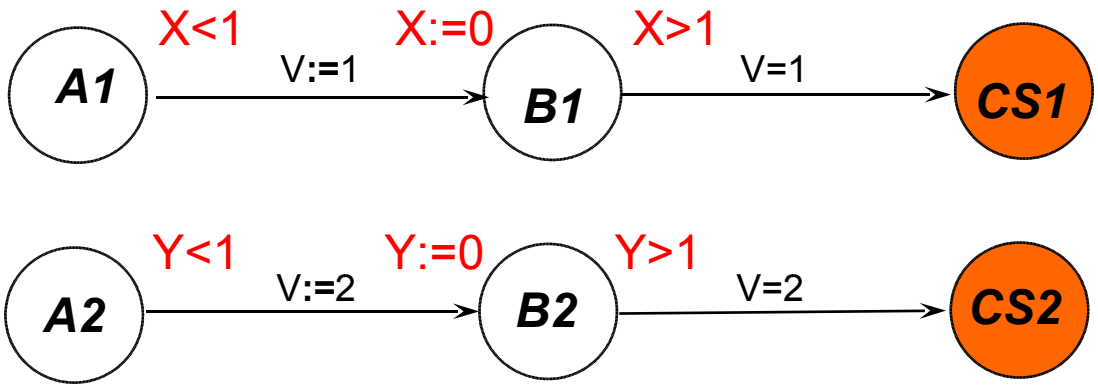
Fischer's Protocol

a simple real time mutual exclusion algorithm



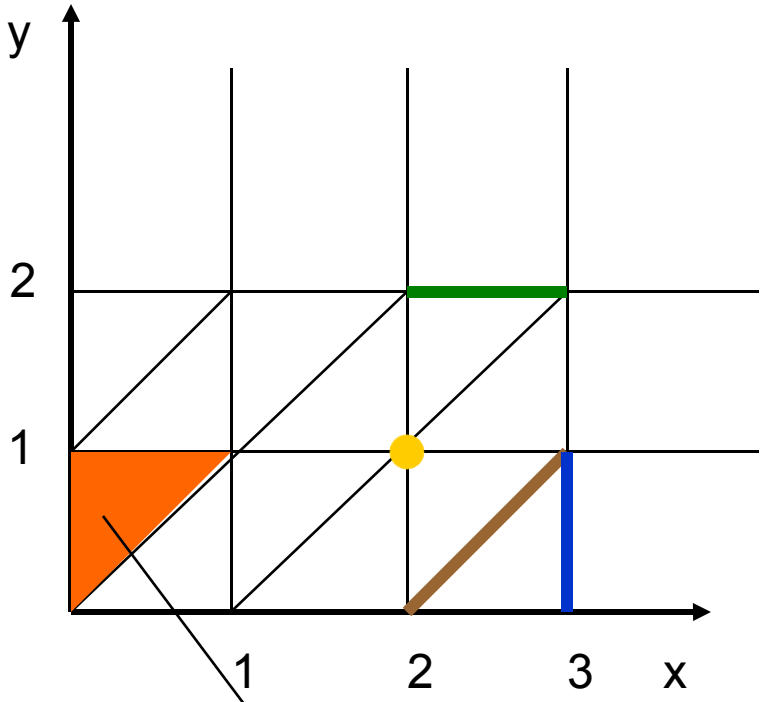
Init

V=1



Regions

Finite partitioning of state space



Definition

$w \approx w'$ iff w and w' satisfy the exact same conditions of the form

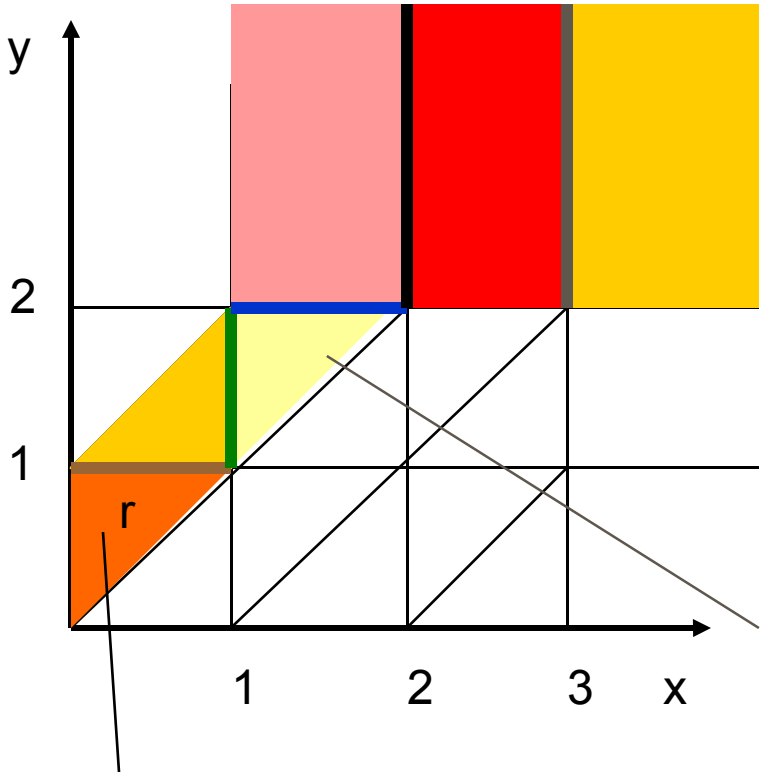
$$x_i \leq n \text{ and } x_i - x_j \leq n$$

where $n \leq \max$

An equivalence class (i.e. a *region*)
in fact there is only a *finite* number of regions!!

Regions

Finite partitioning of state space



Definition

$w \approx w'$ iff w and w' satisfy the exact same conditions of the form

$$x_i \leq n \text{ and } x_i - x_j \leq n$$

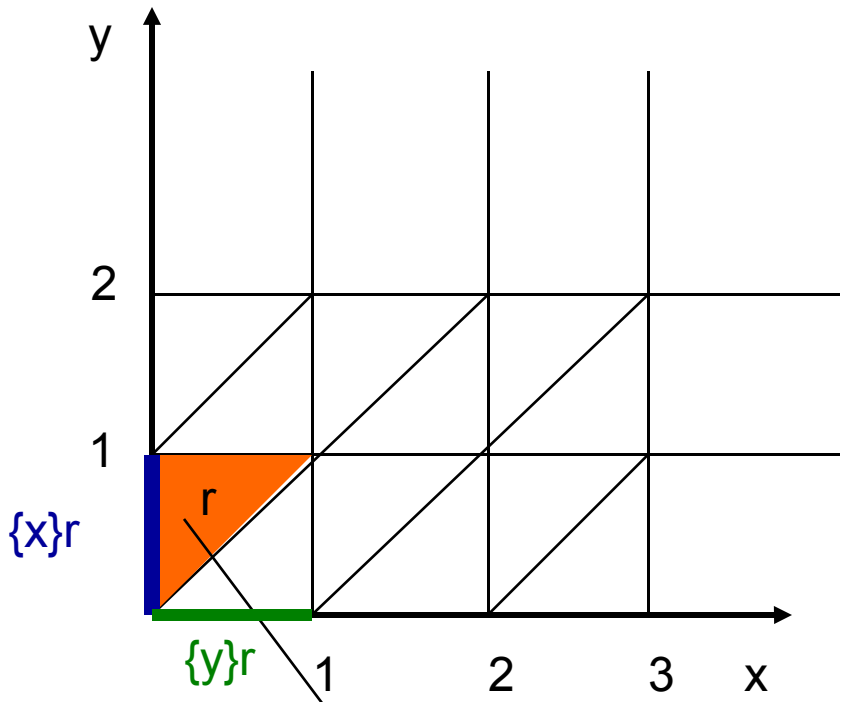
where $n \leq \max$

Successor regions, Succ(r)

An equivalence class (i.e. a *region*)

Regions

Finite partitioning of state space



Reset regions

An equivalence class (i.e. a *region*) r

Definition

$w \approx w'$ iff w and w' satisfy the exact same conditions of the form

$$x_i \le n \text{ and } x_i - x_j \le n$$

where $n \le \max$

THEOREM

Whenever $uv \approx u'v'$ then

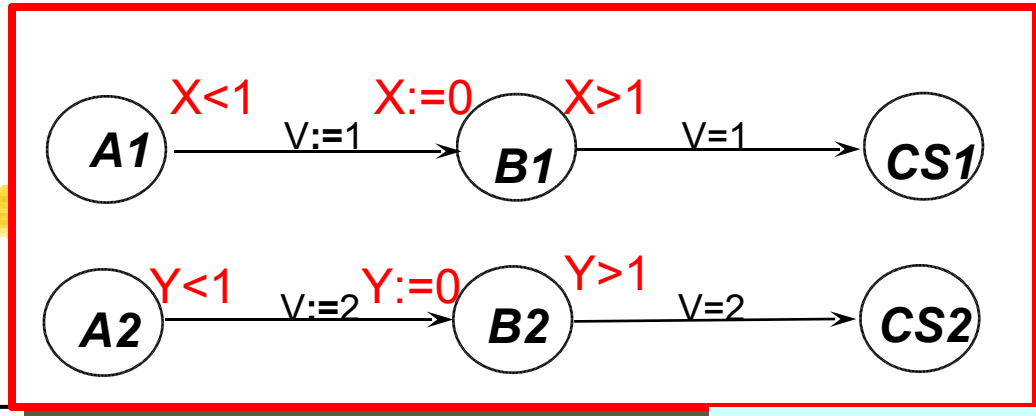
$$[(l,u),v] \text{ sat } \varphi$$

$$\Leftrightarrow$$

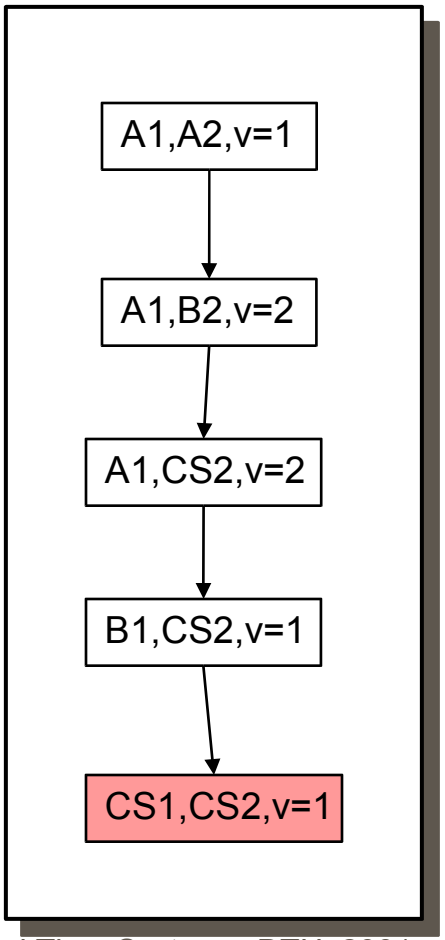
$$[(l,u'),v'] \text{ sat } \varphi$$

$$AG\left(\neg\left(CS_1 \wedge CS_2\right)\right)$$

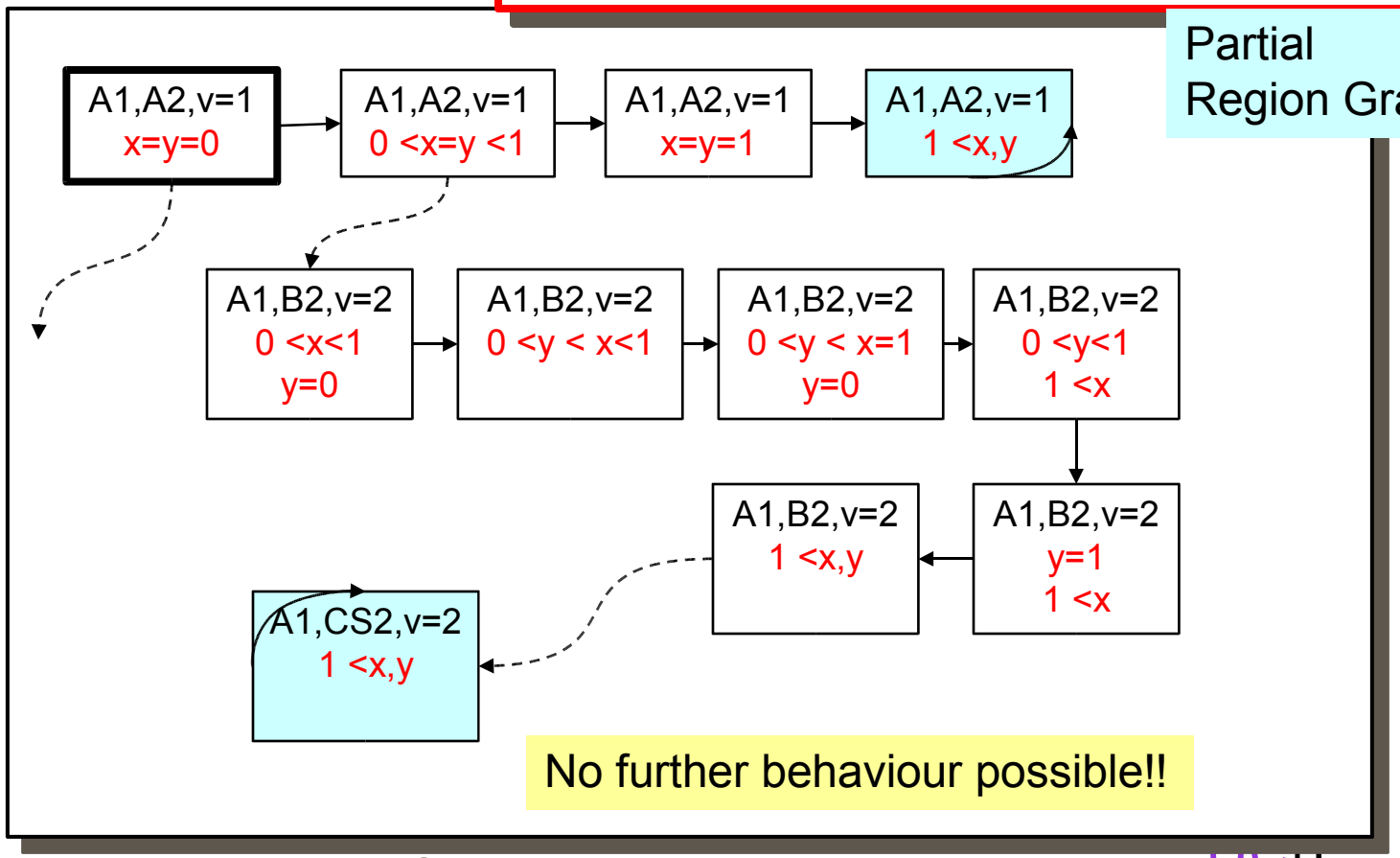
Fischers again



Untimed case



Timed case



Partial Region Graph

No further behaviour possible!!

Roughly speaking....

Model checking a timed automata against a TCTL-formula amounts to model checking its region graph against a CTL-formula

Problem to be solved

The worst-case time complexity of model checking TCTL*-formula* ϕ *over timed automaton* $\mathcal{A}$*, with the clock constraints of* ϕ *and* $\mathcal{A}$ *in* Ψ *is:*

$$\mathcal{O}\left(|\phi| \times (n! \times 2^n \times \prod_{x \in \Psi} c_x \times |L|^2)\right).$$

☺ (i) linear in the length of the formula ϕ

😐 (ii) exponential in the number of clocks in $\mathcal{A}$ and ϕ

☹ (iii) exponential in the maximal constants with which clocks are compared in $\mathcal{A}$ and ϕ.

Model Checking TCTL is PSPACE-hard

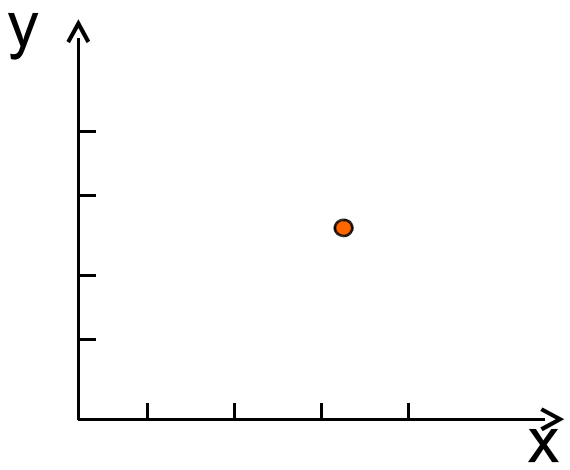
THE UPPAAL ENGINE

Reachability & Zones

Property and system dependent partitioning

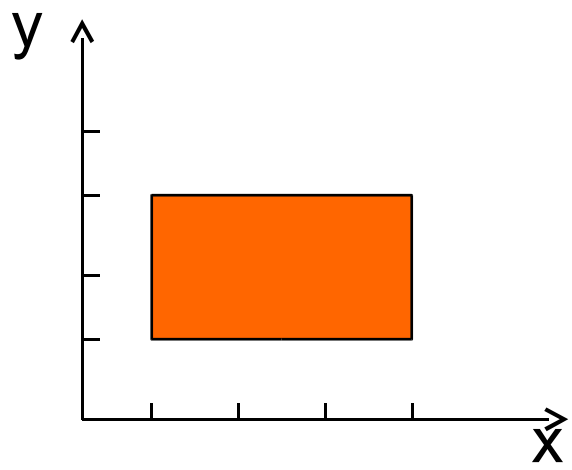
Zones
From infinite to finite

State
(n, x=3.2, y=2.5)

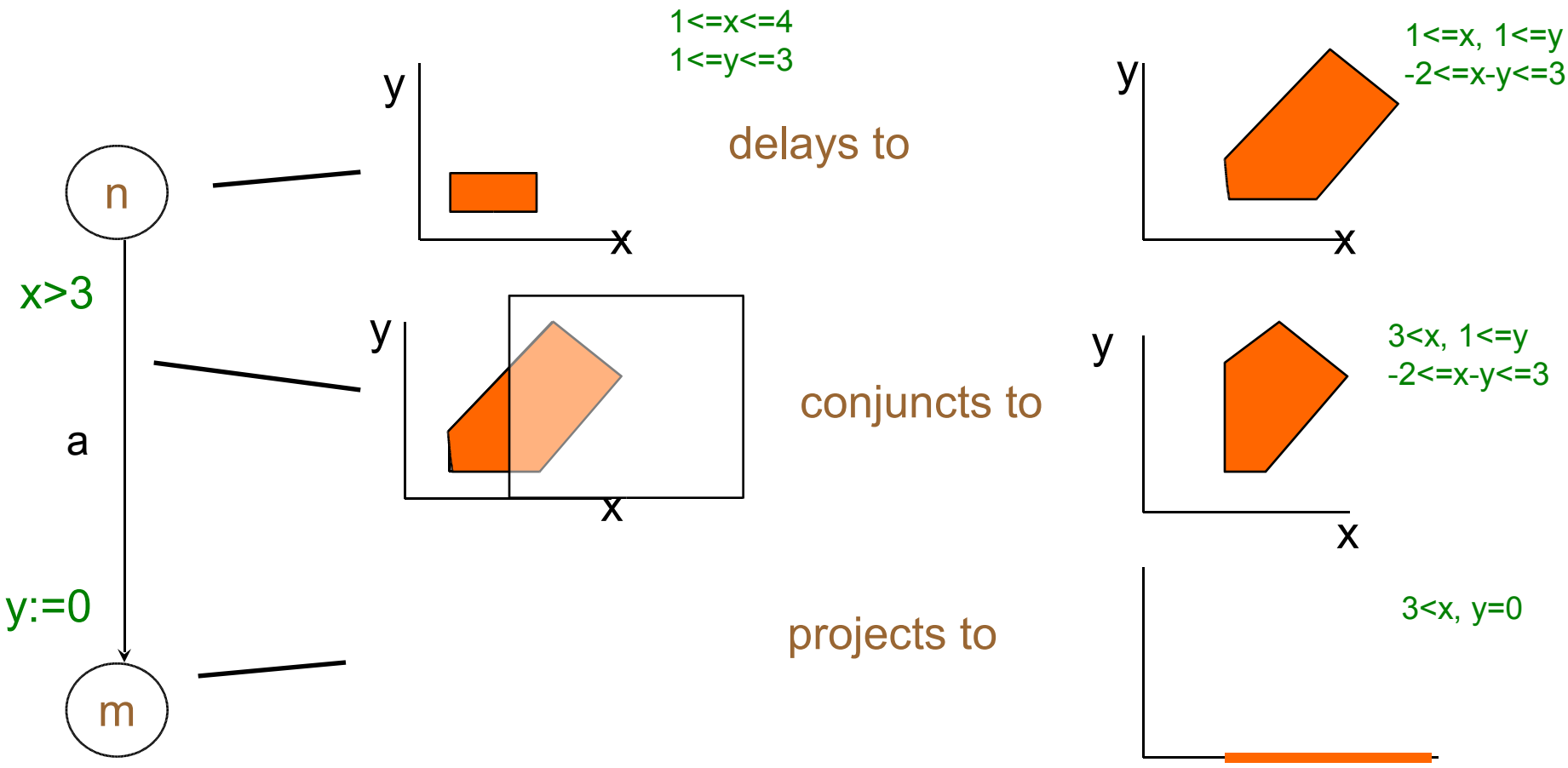


Symbolic state (set)
(n, $1 \le x \le 4, 1 \le y \le 3$)

Zone:
conjunction of
x-y<=n, x<=>n



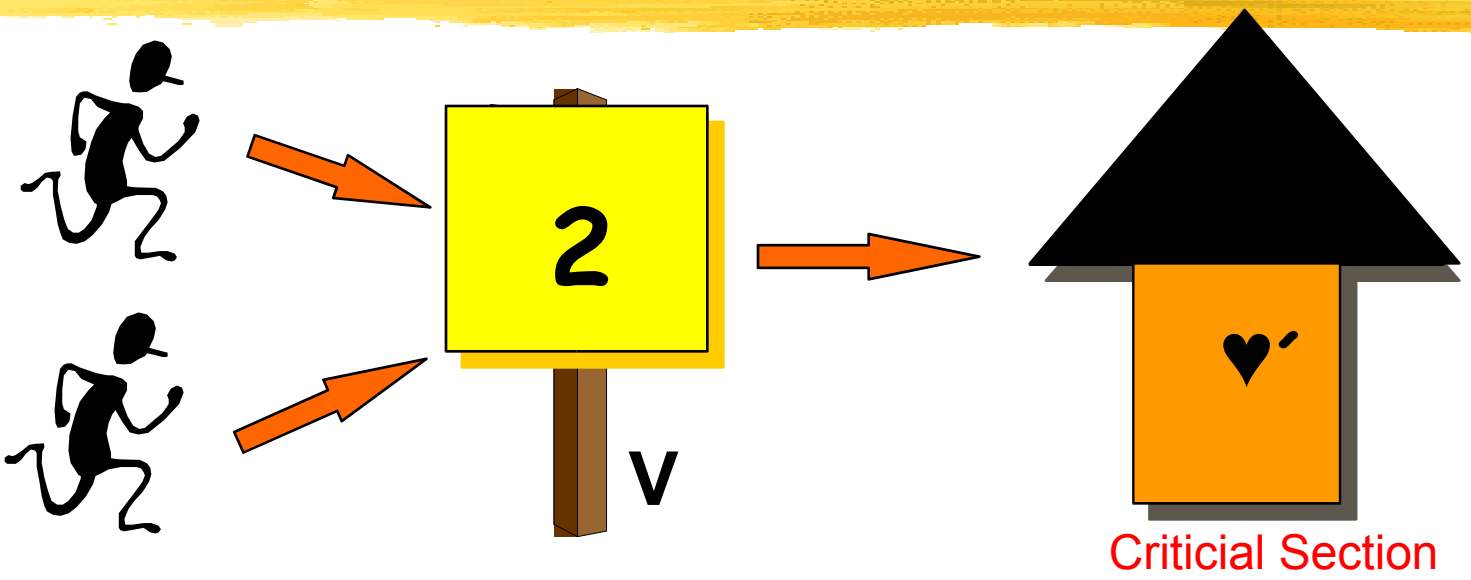
Symbolic Transitions

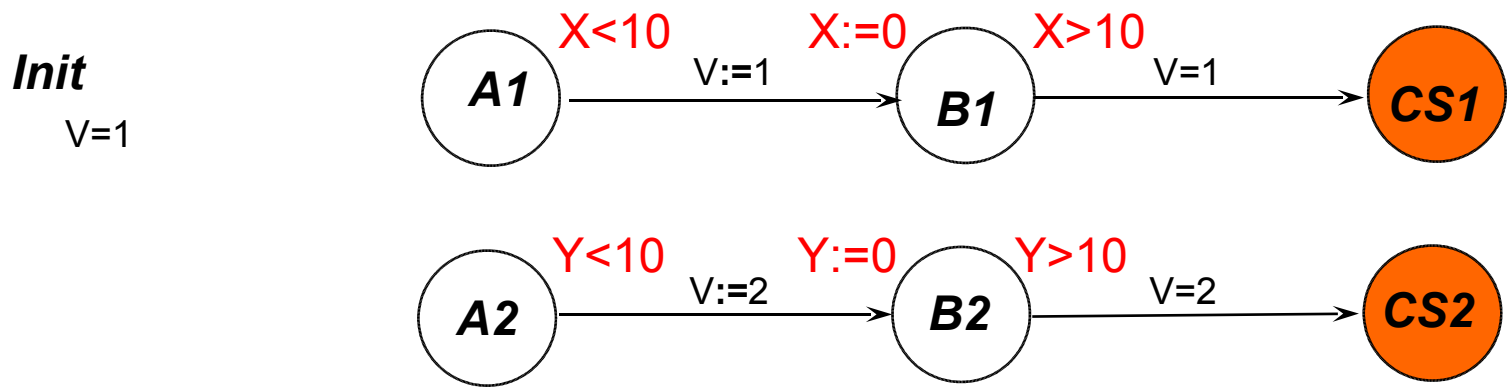


Thus (n,1<=x<=4,1<=y<=3) =a => (m,3<x, y=0)

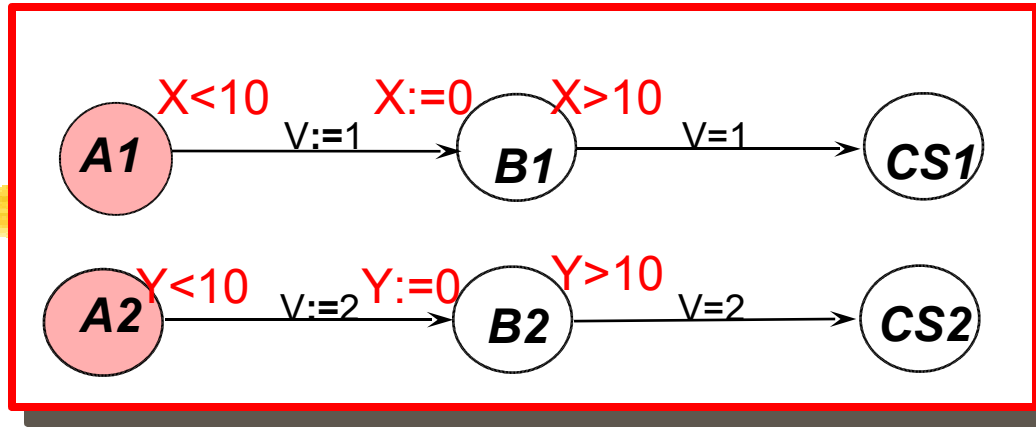
Fischer's Protocol

analysis using zones

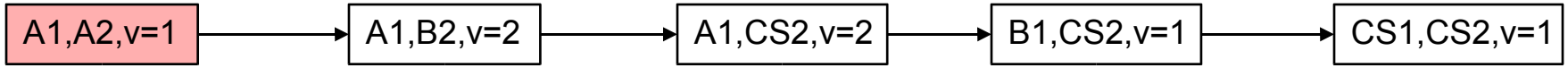




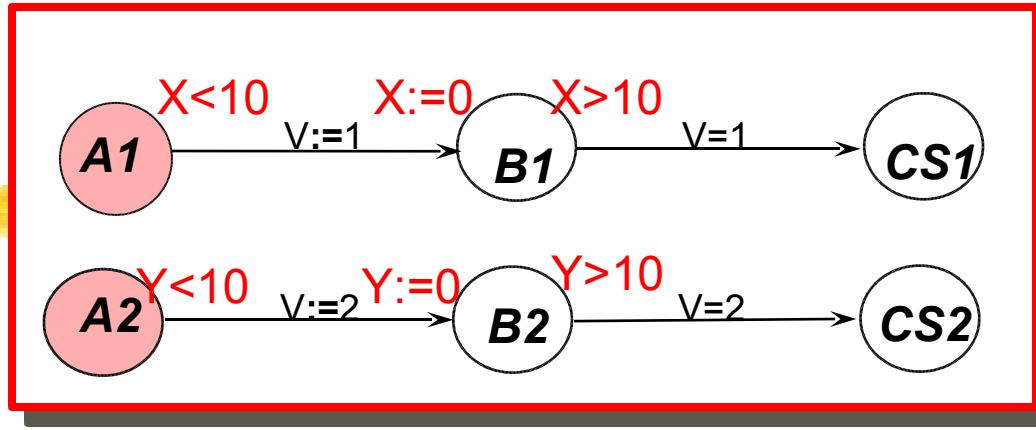
Fischers cont.



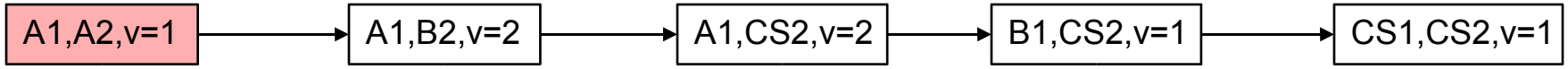
Untimed case



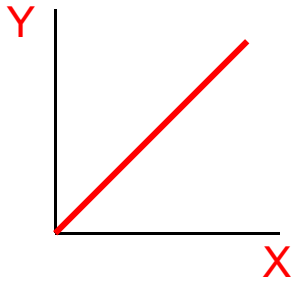
Fischers cont.



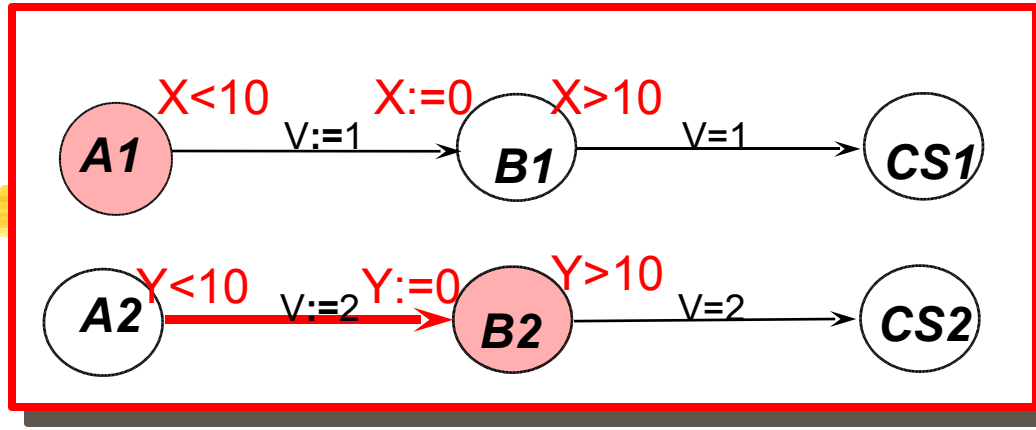
Untimed case



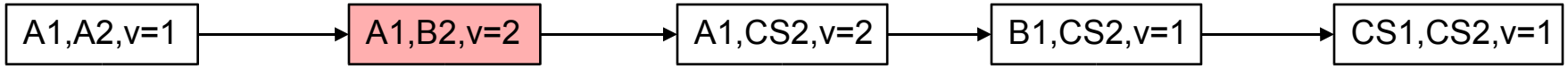
Taking time into account



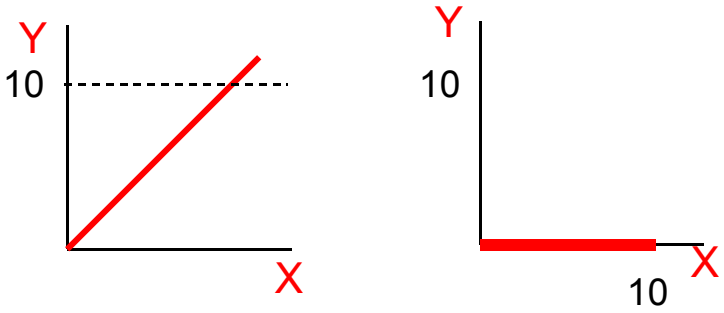
Fischers cont.



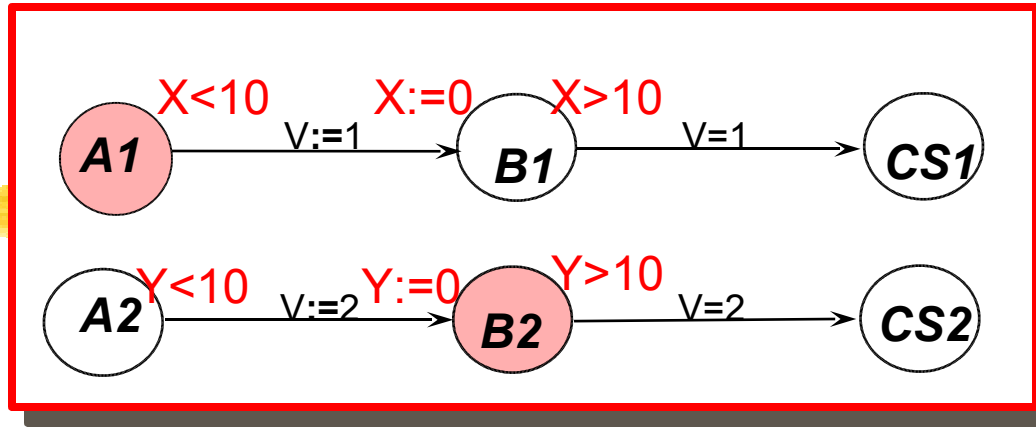
Untimed case



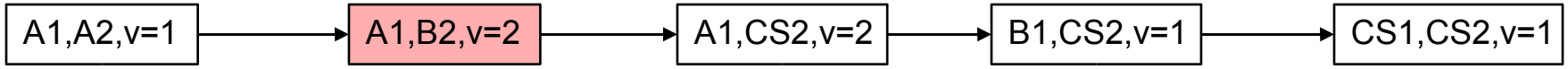
Taking time into account



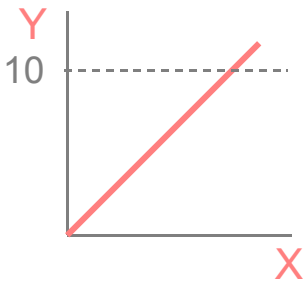
Fischers cont.

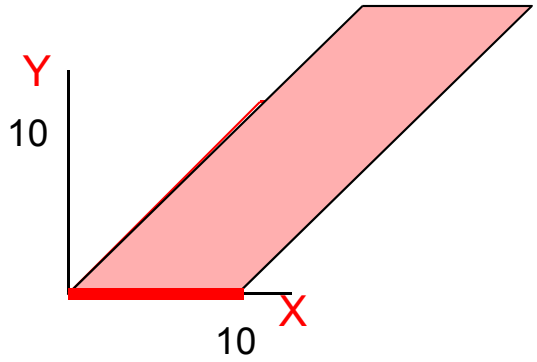


Untimed case

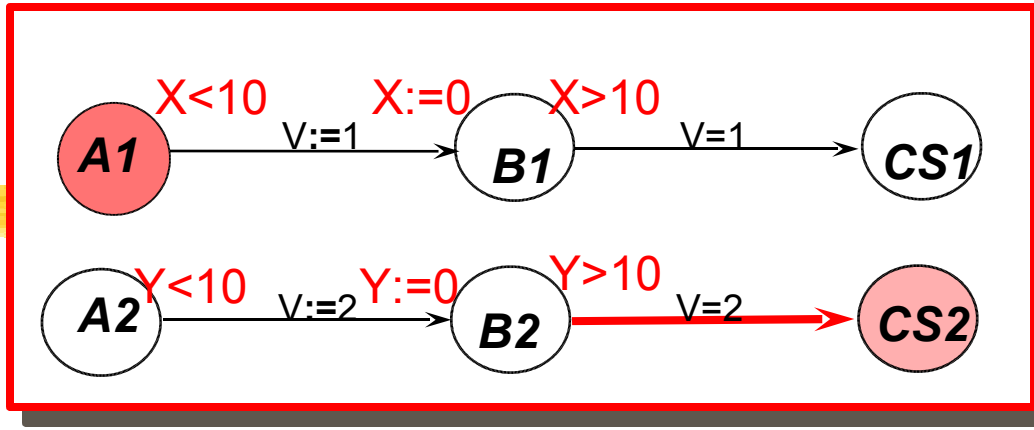


Taking time into account





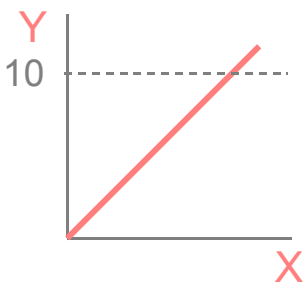
Fischers cont.

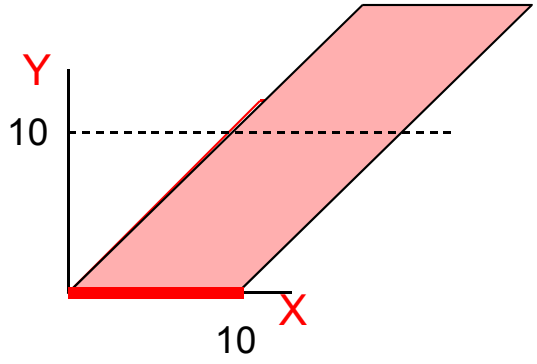


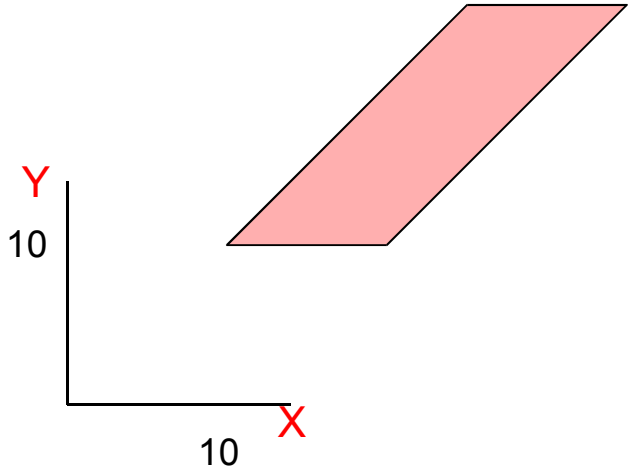
Untimed case

A1,A2,v=1 → A1,B2,v=2 → A1,CS2,v=2 → B1,CS2,v=1 → CS1,CS2,v=1

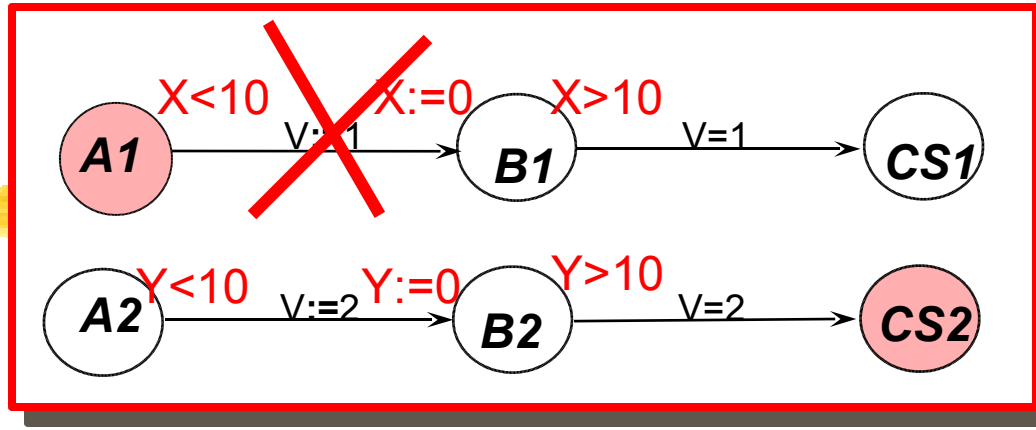
Taking time into account







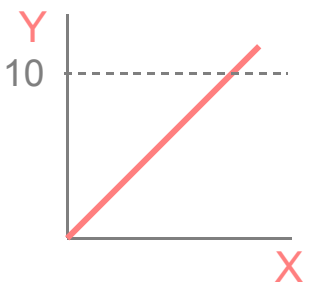
Fischers cont.

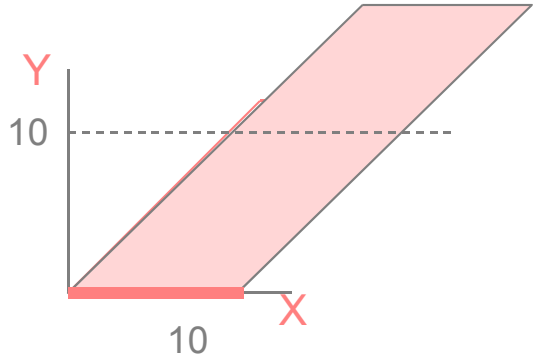


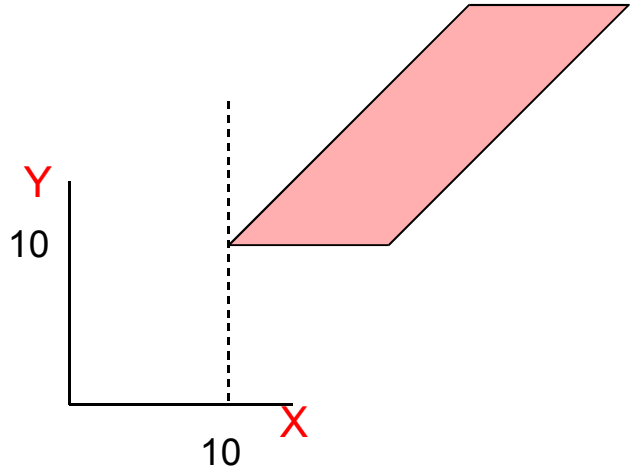
Untimed case

A1,A2,v=1 → A1,B2,v=2 → A1,CS2,v=2 → B1,CS2,v=1 → CS1,CS2,v=1

Taking time into account

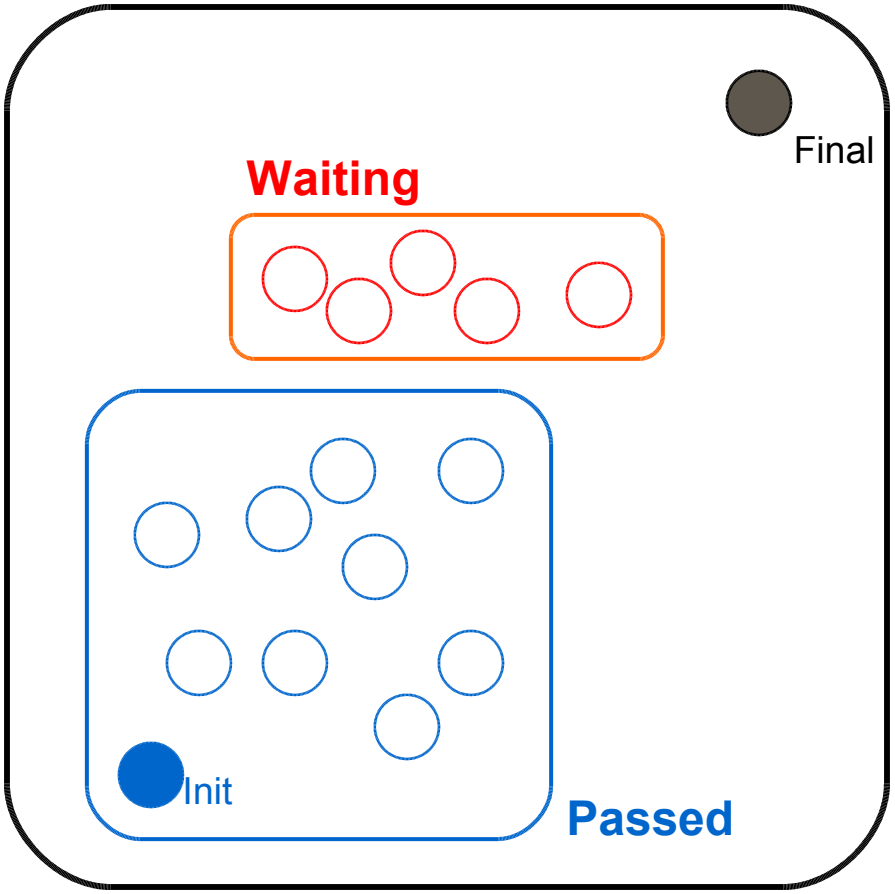






Forward Rechability

Init -> Final ?



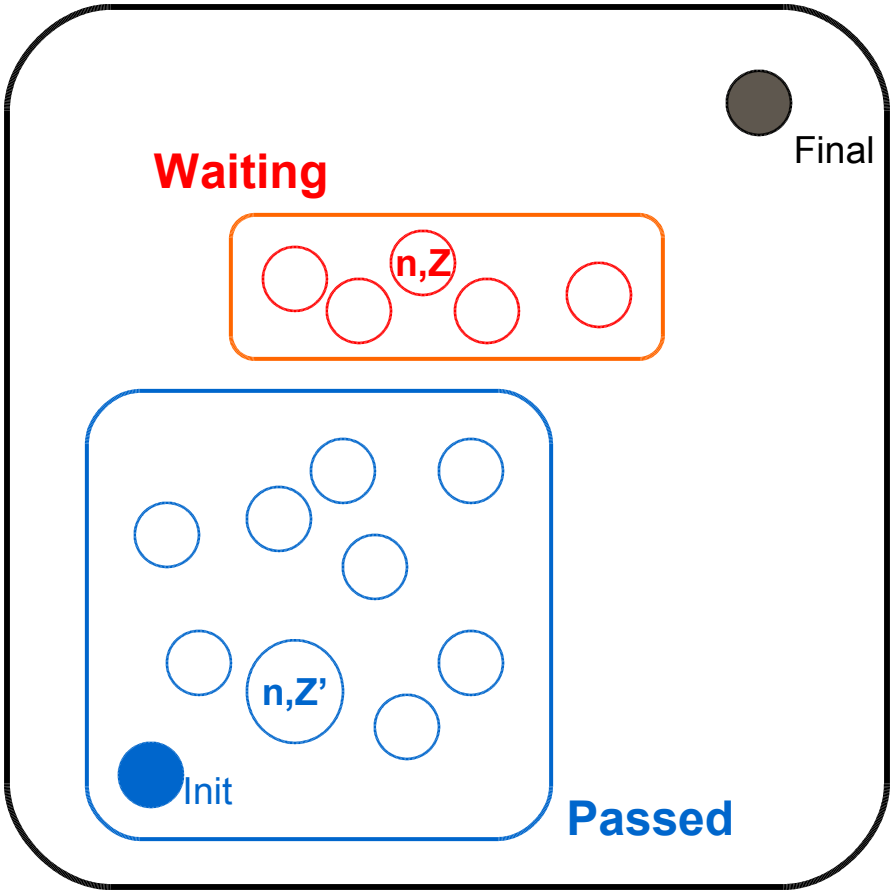
INITIAL **Passed** := Ø;
Waiting := {(n0,Z0)}

REPEAT

UNTIL **Waiting** = Ø
or
Final is in **Waiting**

Forward Rechability

Init -> Final ?



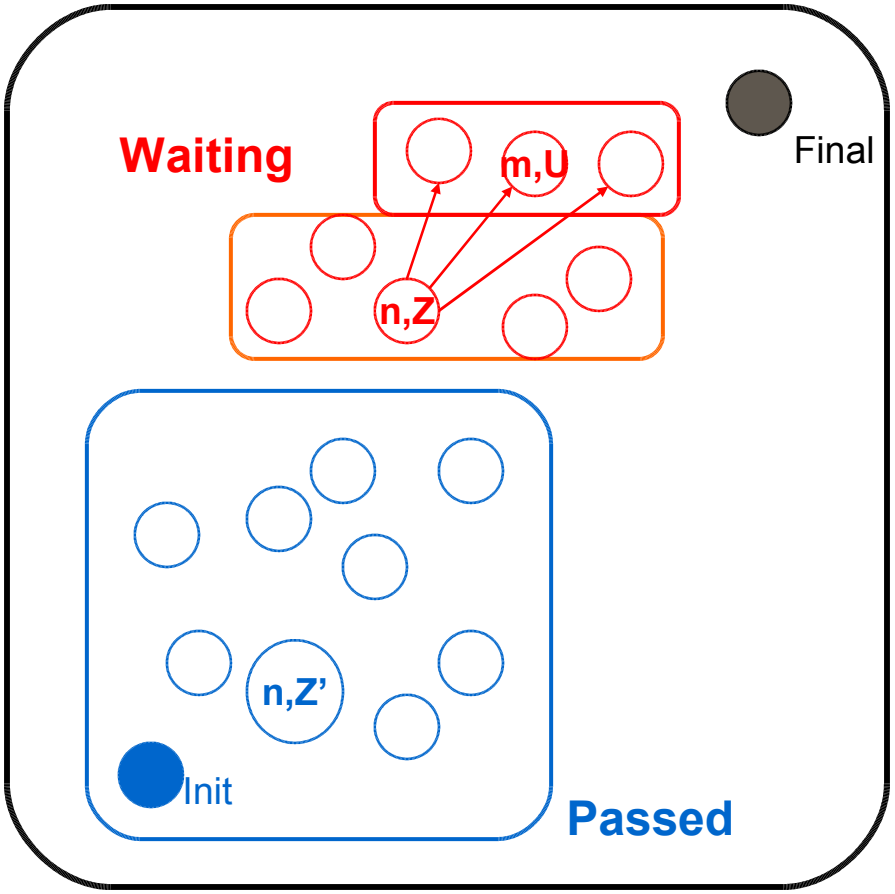
INITIAL **Passed** := Ø;
Waiting := {(n0,Z0)}

REPEAT
- pick (n,Z) in **Waiting**
- **if** for some Z' ¿ Z
(n,Z') in **Passed** **then** **STOP**

UNTIL **Waiting** = Ø
or
Final is in **Waiting**

Forward Rechability

Init -> Final ?



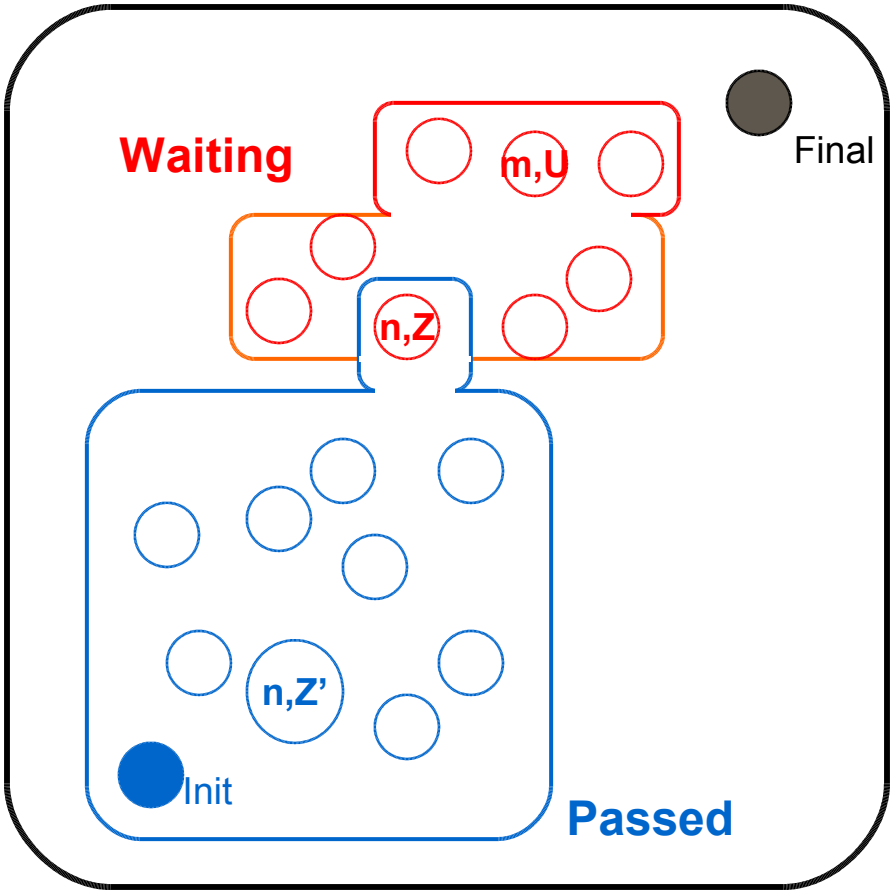
INITIAL **Passed** := Ø;
Waiting := {(n0,Z0)}

REPEAT
- pick (n,Z) in **Waiting**
- **if** for some Z' ¿ Z
  (n,Z') in **Passed** **then** **STOP**
- **else** /explore/ add
  { (m,U) : (n,Z) => (m,U) }
  to **Waiting**;

UNTIL **Waiting** = Ø
or
Final is in **Waiting**

Forward Rechability

Init -> Final ?



INITIAL **Passed** := Ø;
Waiting := {(n0,Z0)}

REPEAT
- pick (n,Z) in **Waiting**
- **if** for some Z' ¿ Z
  (n,Z') in **Passed** **then** **STOP**
- **else** /explore/ add
  { (m,U) : (n,Z) => (m,U) }
  to **Waiting**;
  Add (n,Z) to **Passed**

UNTIL **Waiting** = Ø
or
Final is in **Waiting**

Canonical Dastructures for Zones

Difference Bounded Matrices

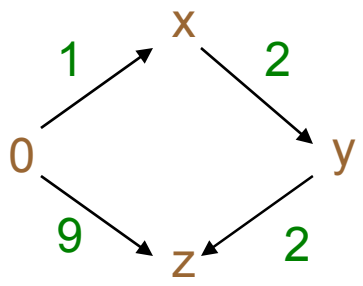
Bellman 1958, Dill 1989

Inclusion

D1

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

Graph

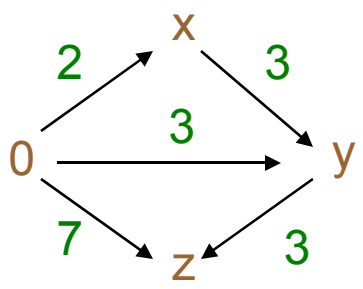


? ¿ ?

D2

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

Graph



Canonical Dastructures for Zones

Difference Bounded Matrices

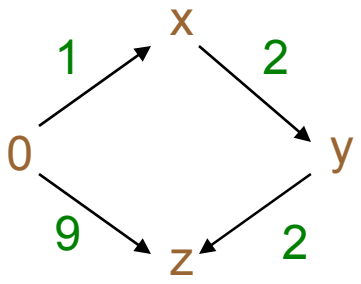
Bellman 1958, Dill 1989

Inclusion

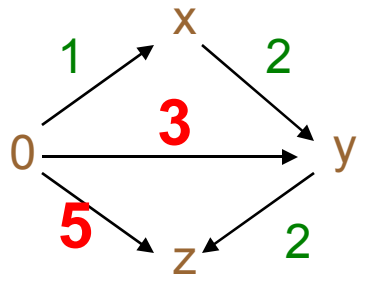
D1

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

Graph



Shortest Path Closure

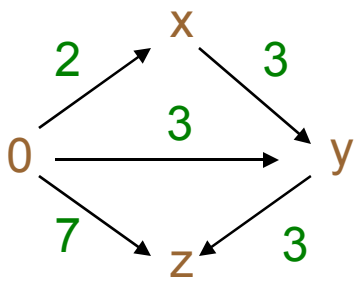


? ¿ ?

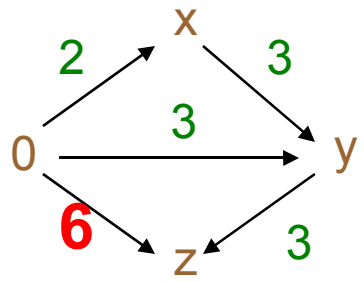
D2

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

Graph



Shortest Path Closure



Canonical Dastructures for Zones

Difference Bounded Matrices

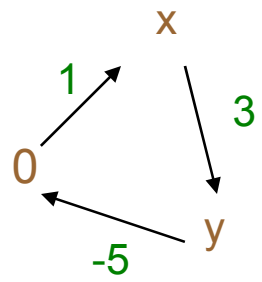
Bellman 1958, Dill 1989

Emptyness

D

x<=1
y<= -5
y-x<=3

Graph

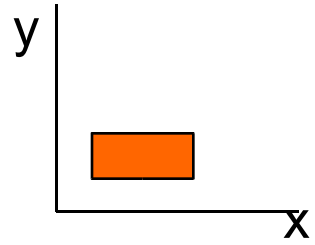


Negative Cycle
iff
empty solution set

Canonical Dastructures for Zones

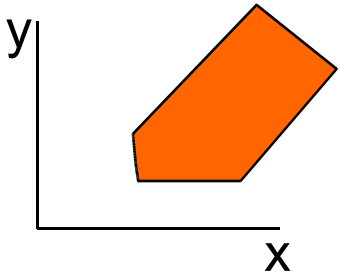
Difference Bounded Matrices

Future



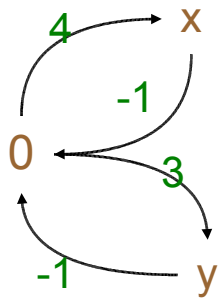
D

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

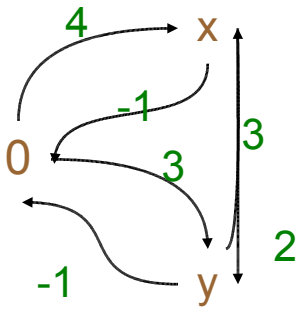


Future D

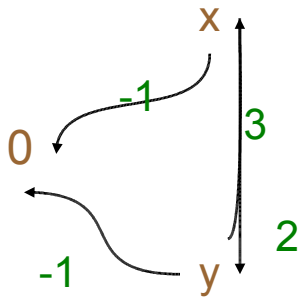
1<=x, 1<=y
-2<=x-y<=3



Shortest Path Closure



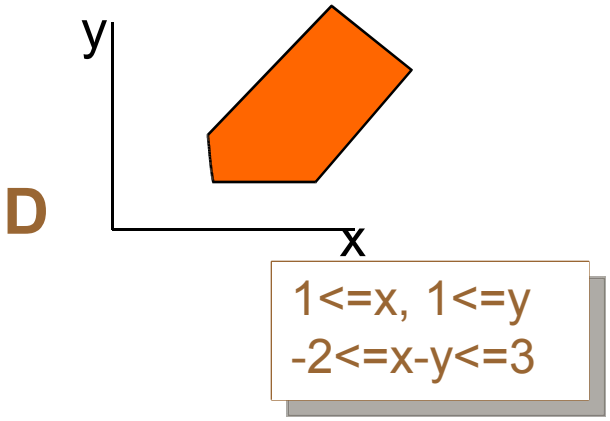
Remove upper bounds on clocks

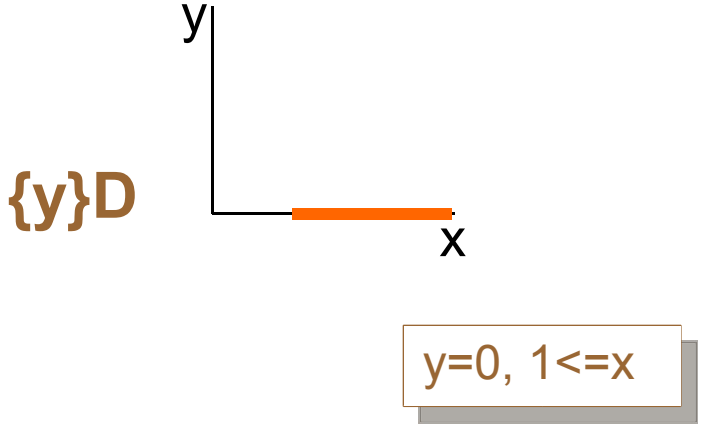


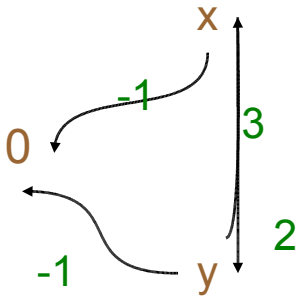
Canonical Dastructures for Zones

Difference Bounded Matrices

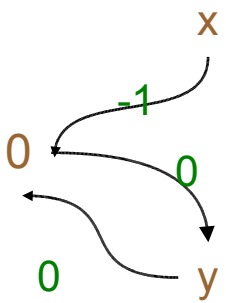
Reset







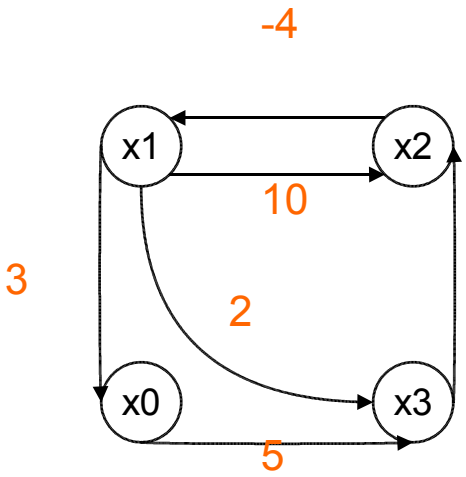
Remove all bounds involving y and set y to 0



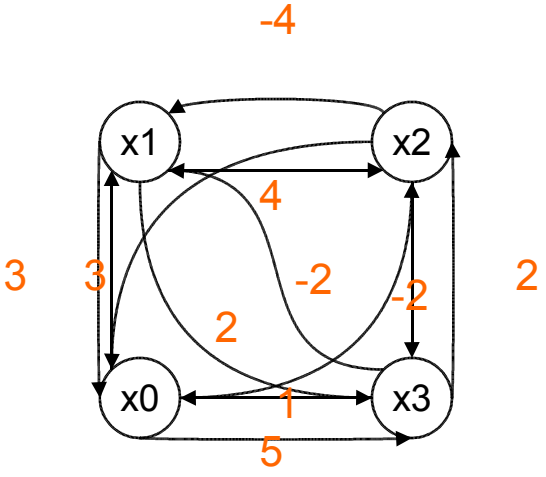
Improved Datastructures

Compact Datastructure for Zones

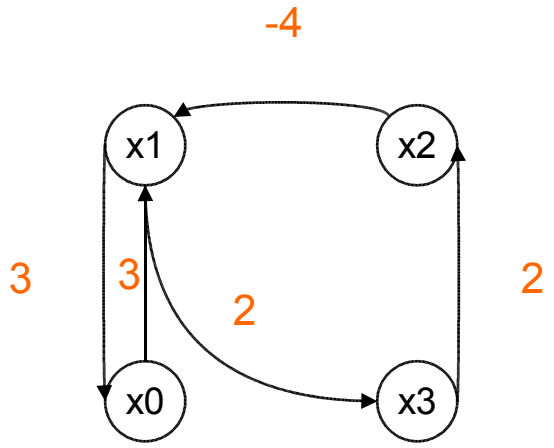
x1-x2<=4
x2-x1<=10
x3-x1<=2
x2-x3<=2
x0-x1<=3
x3-x0<=5



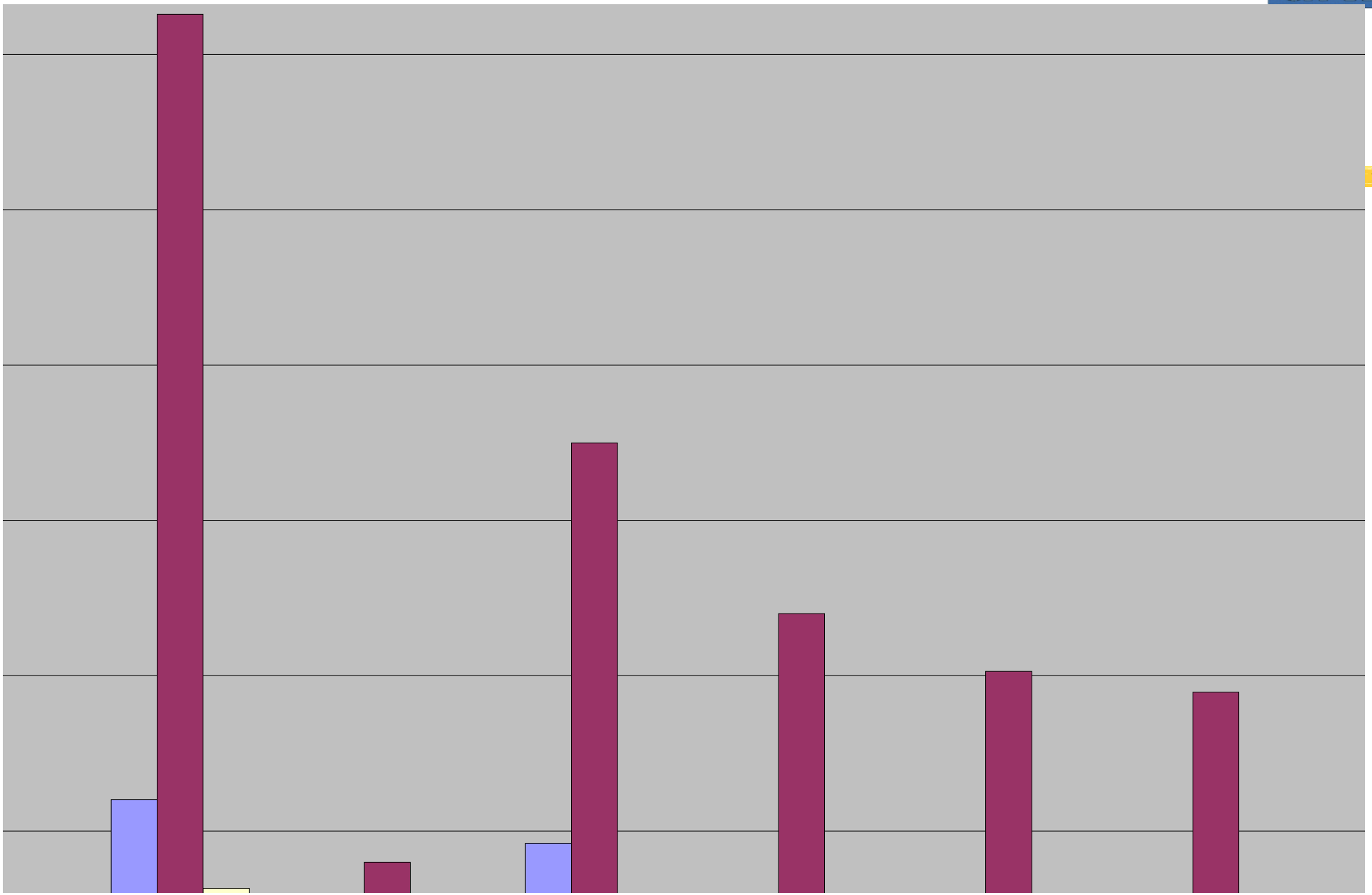
Shortest Path Closure O(n^3)

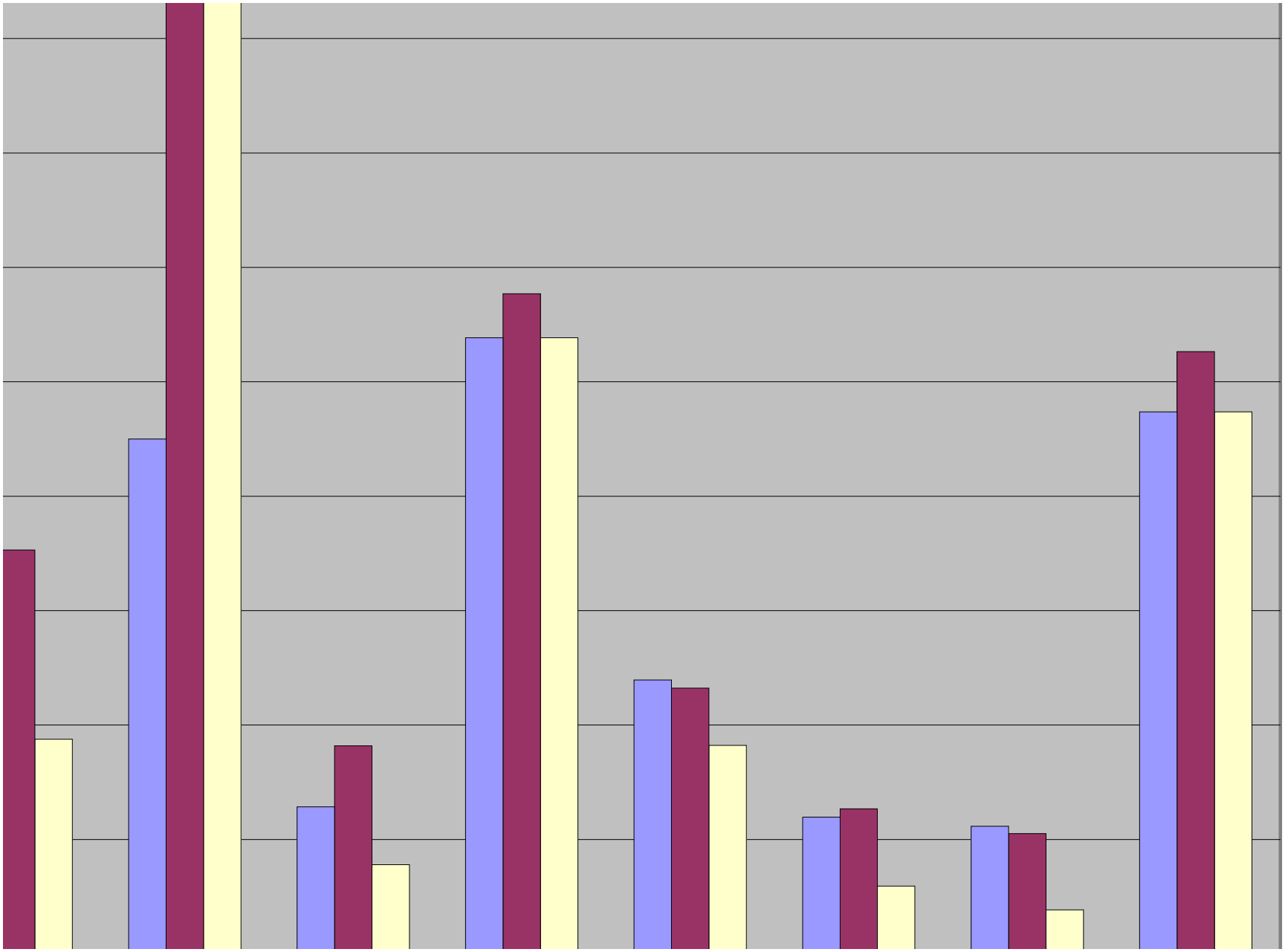


Shortest Path Reduction O(n^3)



Canonical wrt =
Space worst O(n^2)
practice O(n)





Beyond Reachability

-Bounded Liveness

-Abstraction & Simulation

Logical Formulas

Safety Properties:

F ::= A[ ] P | ——— Always P

E<> P ——— Possibly P

atomic properties

clock comparison

where P ::= Proc.l | x = n | v = n |

x<=n | x<n |

P and P | not P | P or P |

P imply P

Process Proc at location l

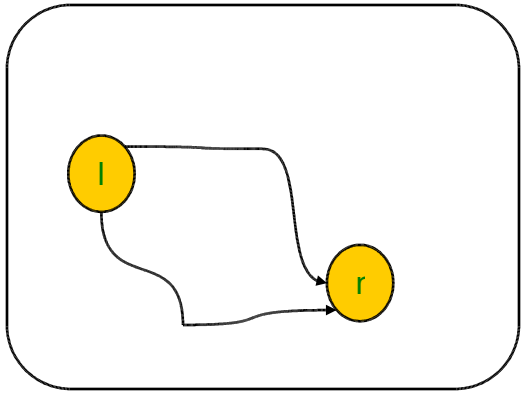
boolean combinations

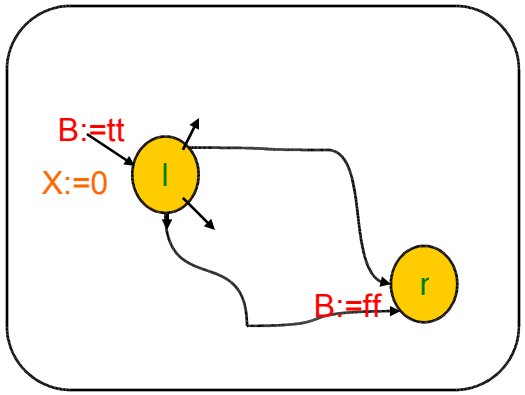
Beyound Safety

Decoration

$$\mathrm{AG}\,(a \Rightarrow \mathrm{AF}_{\leq t}\, b)$$

TACAS98a





Leadsto:
Whenever l is reached
then n is reached with t

Decoration
new clock **X**
boolean **B**

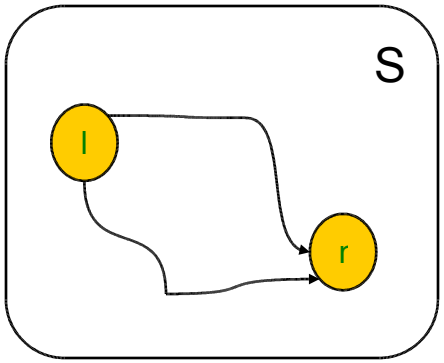
A[] (B implies x<=t)

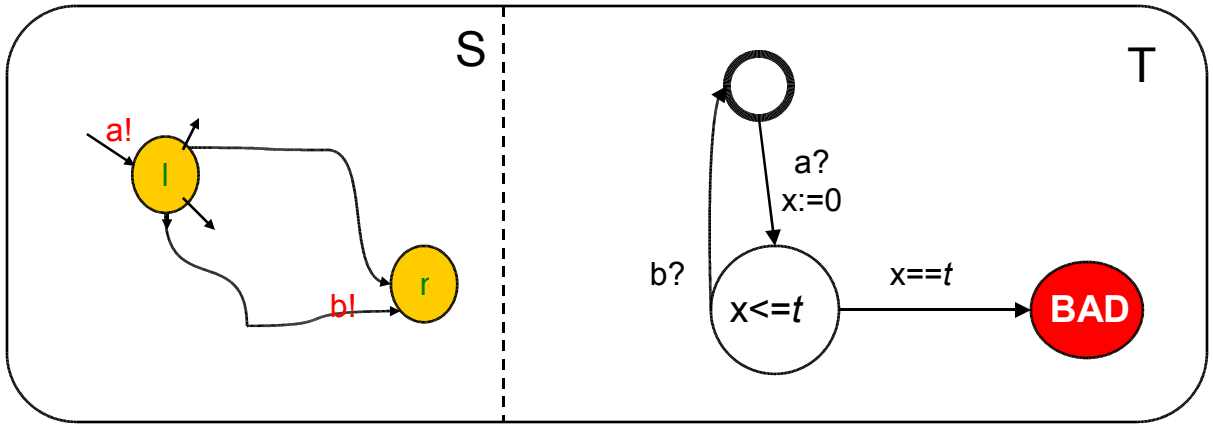
Beyond Safety

Test automata

$$AG\,(a \Rightarrow AF_{\leq t}\, b)$$

TACAS98b

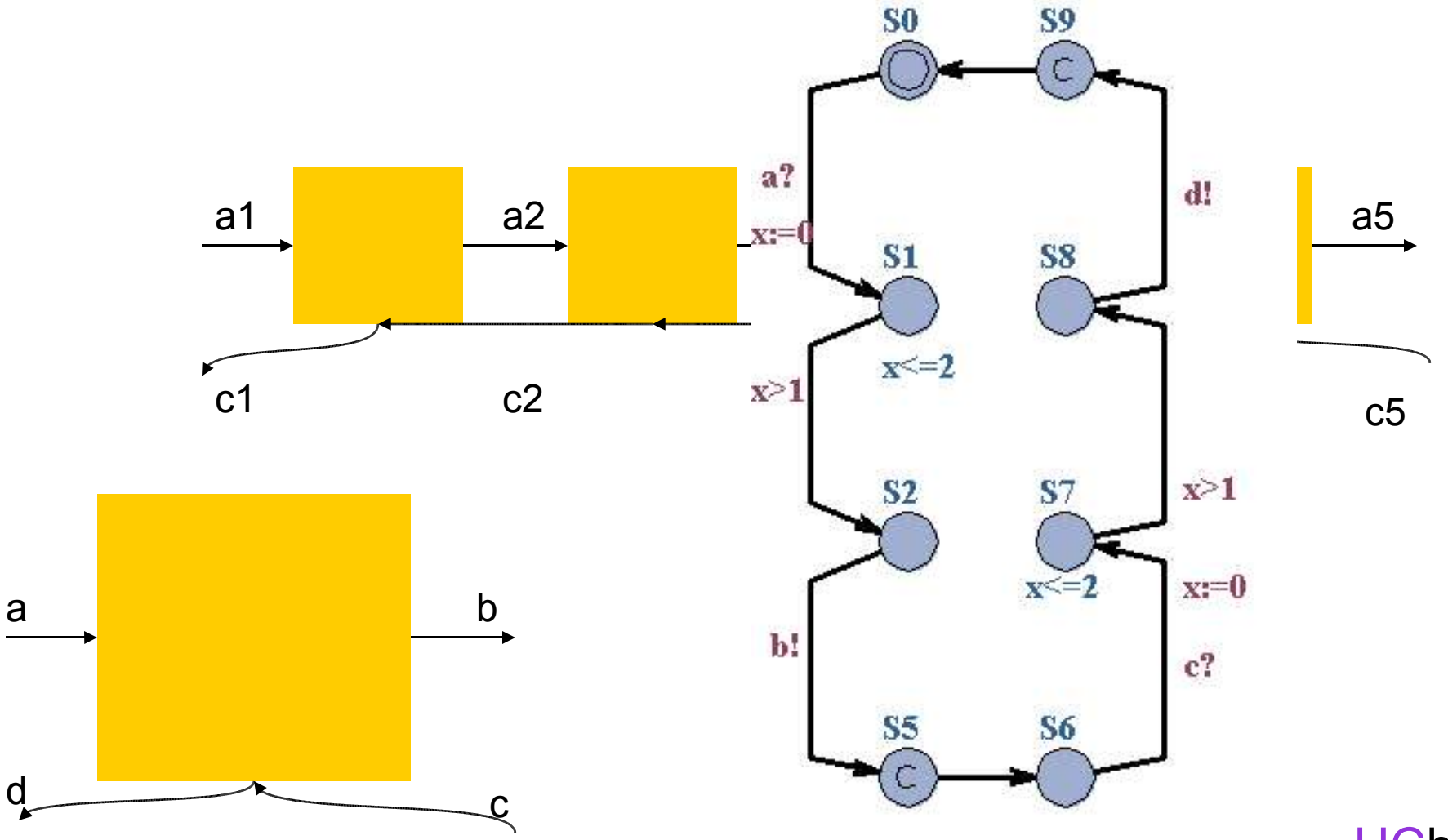




b urgent!

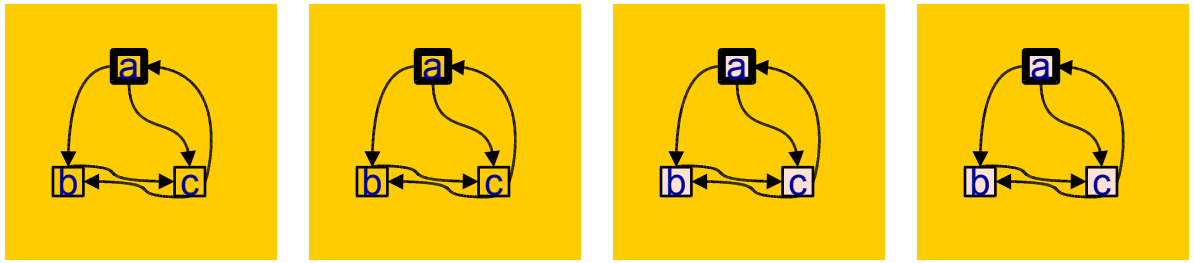
A[] (not T.BAD)

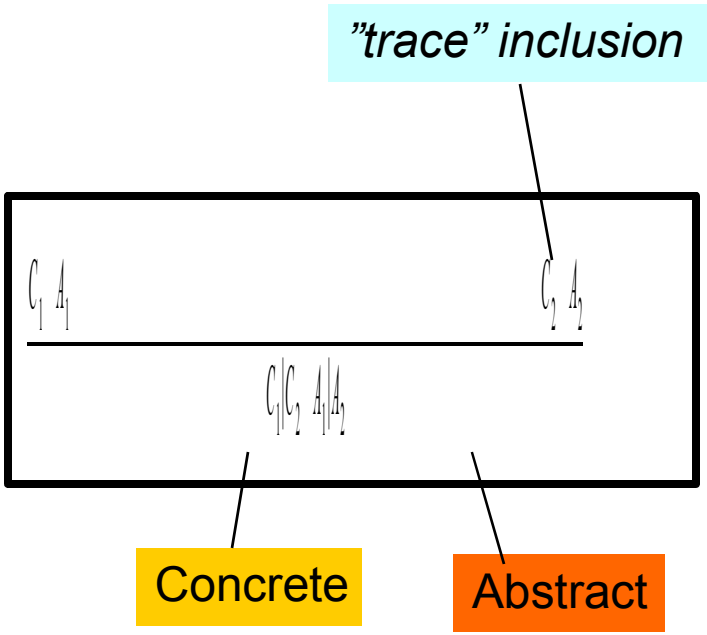
Example *bounded liveness*

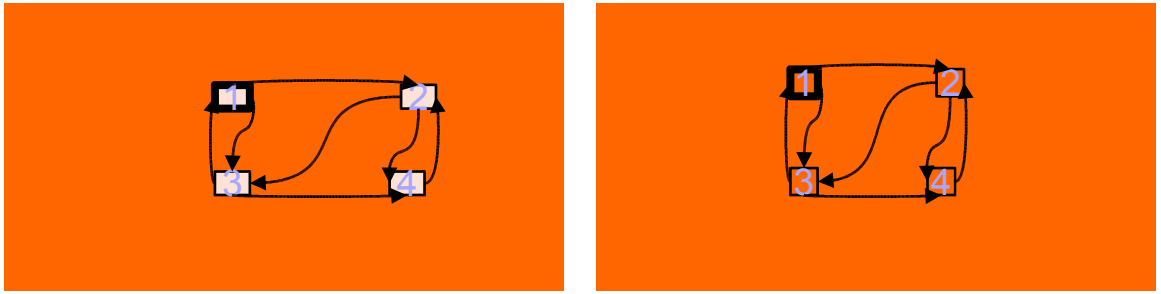


Abstraction & Compositionality

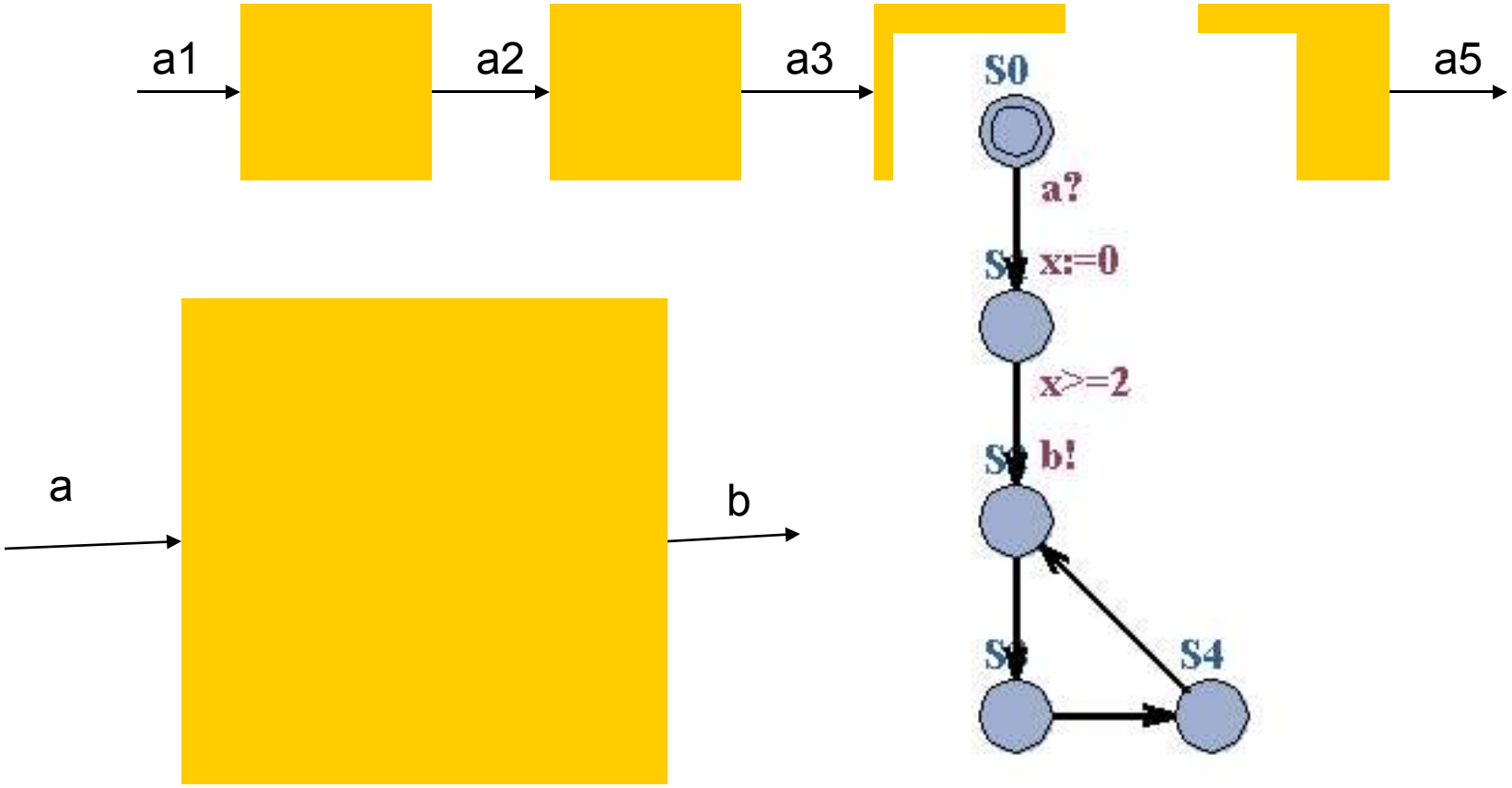
dealing w stateexplosion



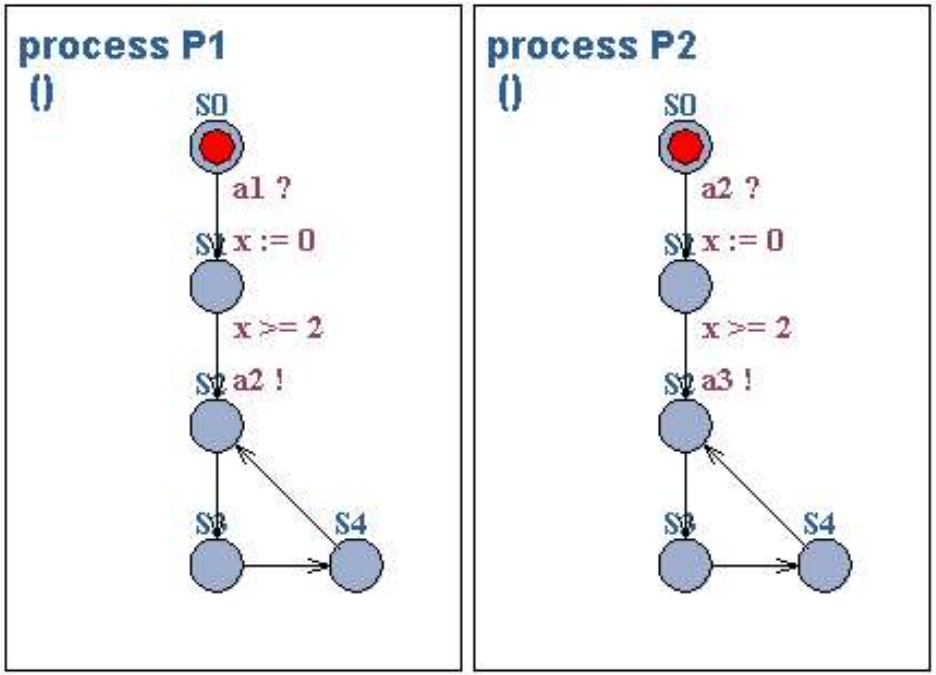




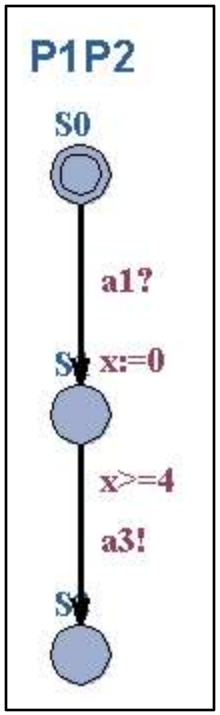
Abstraction *Example*



Example *Continued*

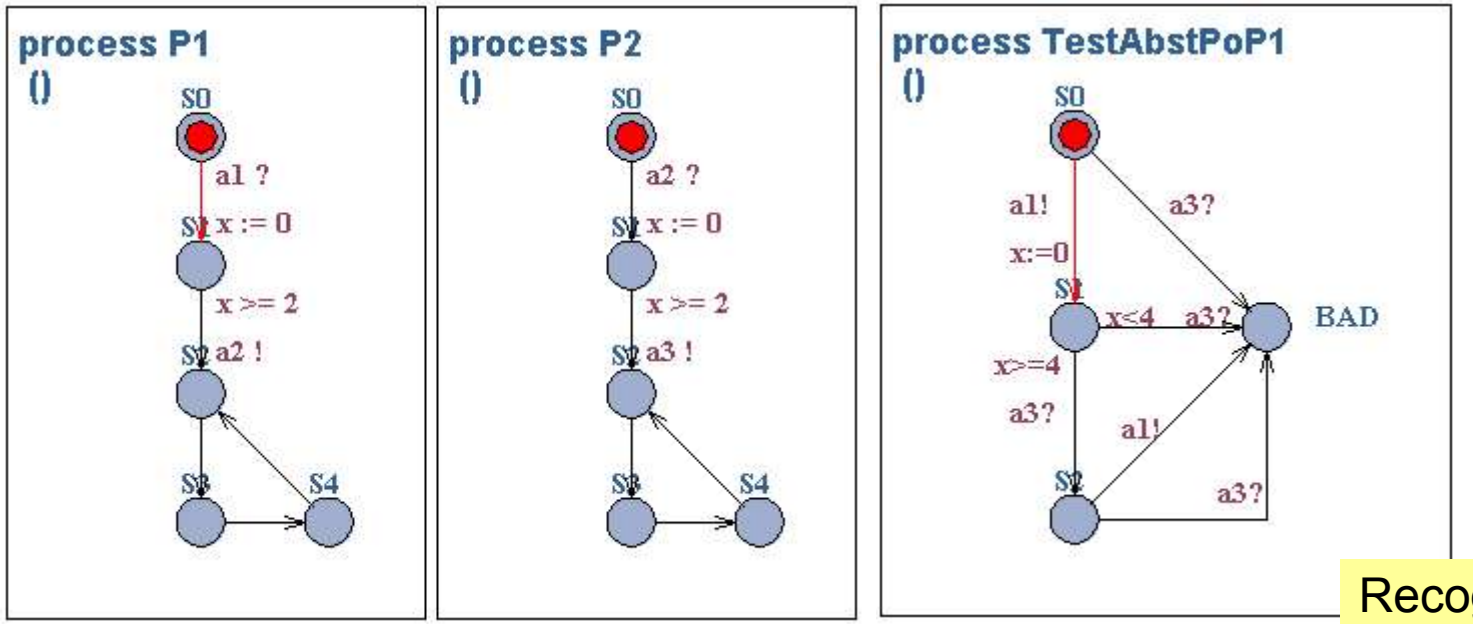


abstracted by



Proving abstractions

using reachability



Recognizes all the BAD computations of PoP1

A[] not TestAbstPoP1.BAD