Using (Timed) Petri Nets for Verification of Parametrized (Timed) Systems

Parosh Aziz Abdulla

Uppsala University

Outline

- Introduction
- Parametrized Systems
- Parametrized Finite-State Processes
  - Petri Nets
  - Symbolic Reachability Analysis
  - Well Quasi-Orderings
- Parametrized Timed Processes
  - Timed Petri Nets
  - Symbolic Reachability Analysis – Existential Zones
  - Better Quasi-Orderings

Program Verification

- **Instance**
  - P: **Program**
  - ϕ: **Specification**
- **Question**
  - $P \models \phi$?

Model Checking

- **Automatic Verification**

Finite-State Systems

$$P \models \phi$$

- P: finite state space

  ϕ: CTL, PTL, etc.

- Applications

  - hardware and protocol verification

- Limitations
  - state explosion
  - infinite-state systems

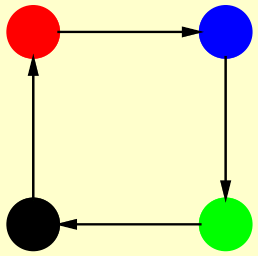
Sources of Infiniteness

1. Unbounded Data Structures
   - Timed Automata
   - Push-down Automata
   - Communicating Finite-State Machines
   - Counter Machines

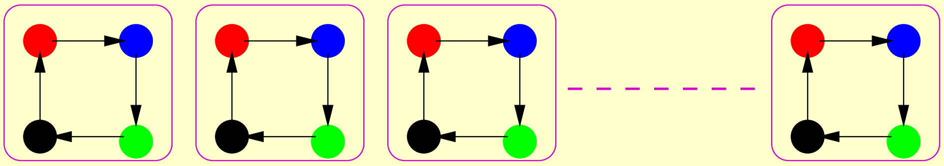
2. Unbounded Control Structures
   - Petri Nets
   - Parametrized Systems
     - e.g. mutual exclusion protocols, cache coherence protocols, broadcast protocols

Parametrized Systems

- start with a cell:



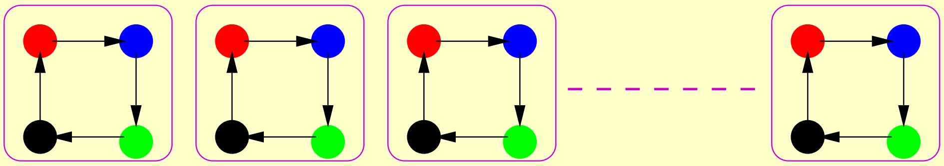
- consider an arbitrary number of cells:



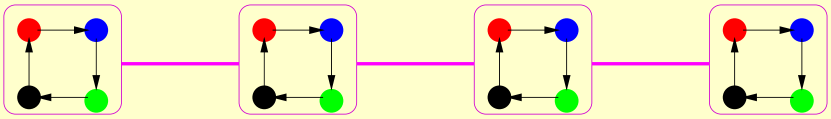
- Examples: mutual exclusion protocols, cache coherence protocols, broadcast protocols

Structure

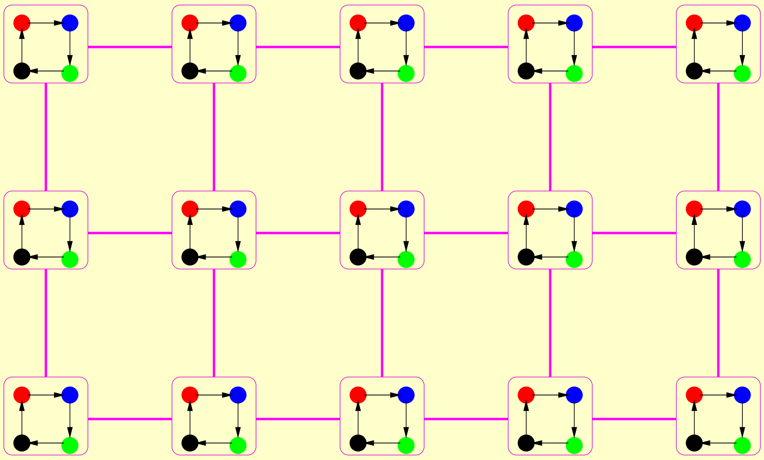
- Set



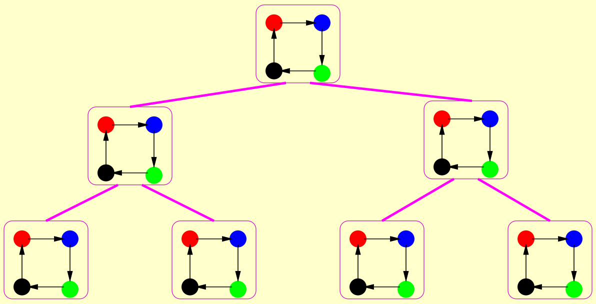
- Array



- Matrix



- Tree



Type of Cells

- **Simple:** finite-state process
- **Extended:** clocks, buffers, counters, etc

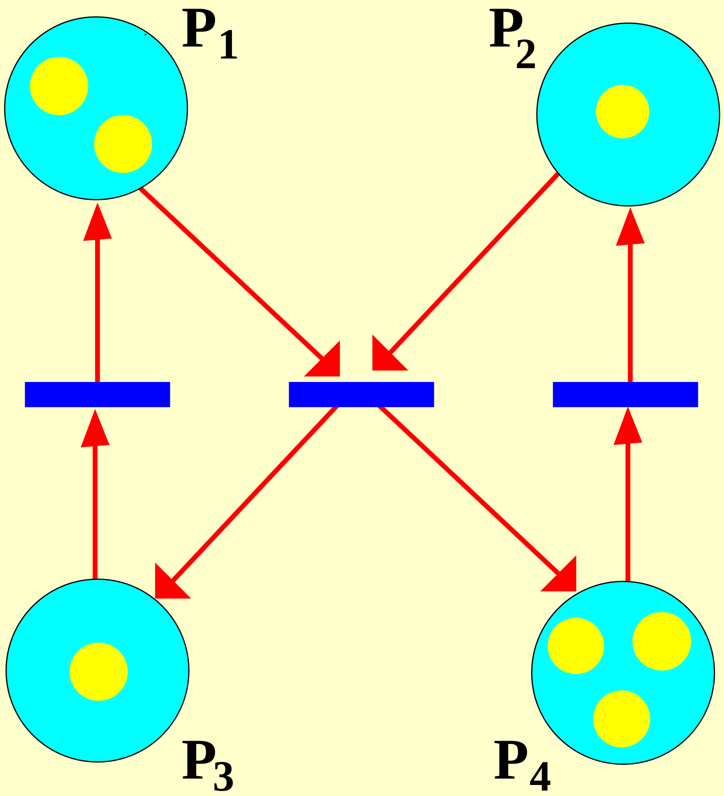
Type of Communication

- binary (rendez-vous)
- broadcast
- neighbour
- global
  -
  -
  -

We Consider:

- Sets (no structure)
- binary communication
- cells:
  - finite-state processes: Petri nets
  - timed processes: timed Petri nets

Petri Nets

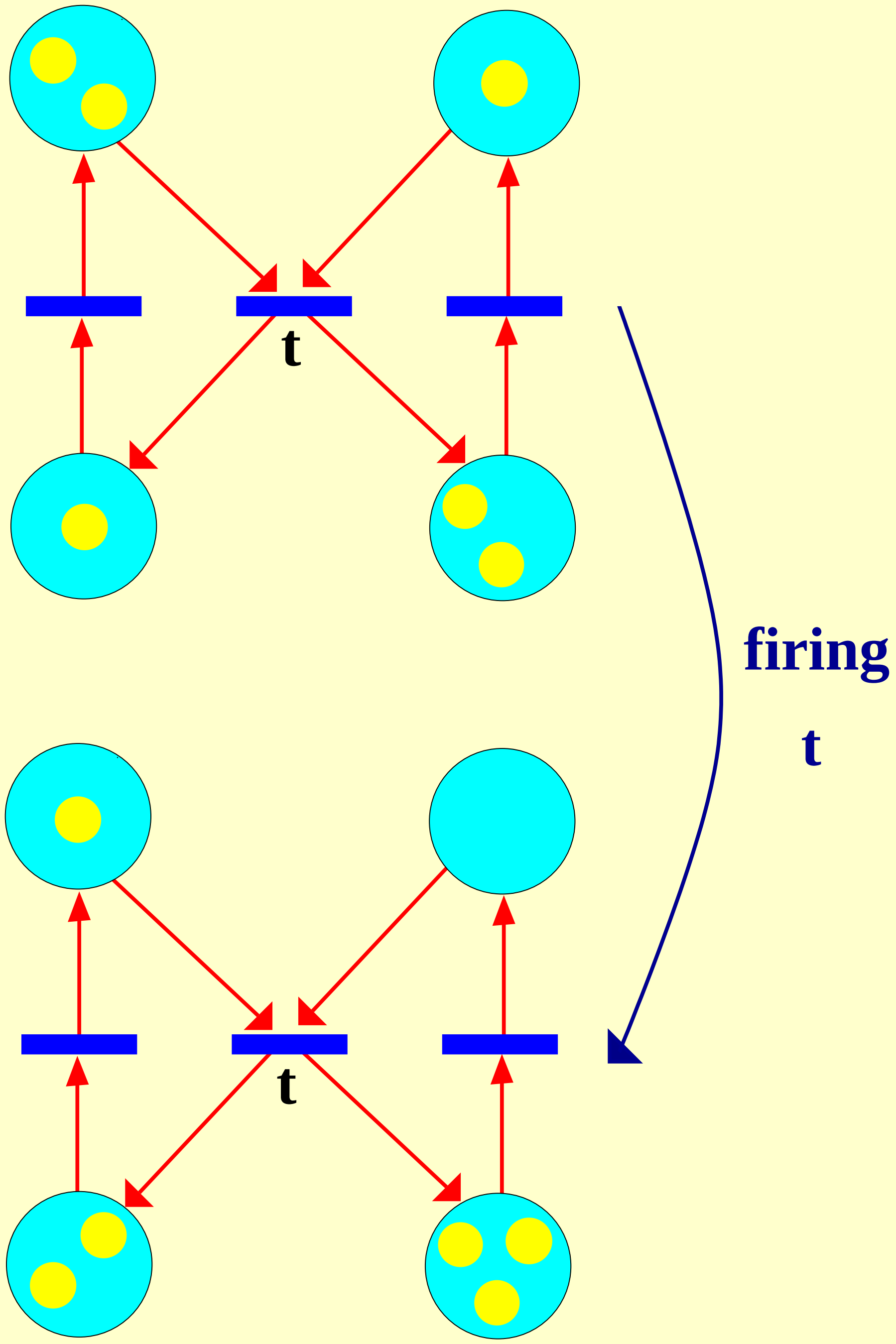


Marking

M : **mapping from places to** *Nat*

$M(P_1) = 2 \quad M(P_2) = 1$
$M(P_3) = 1 \quad M(P_4) = 3$

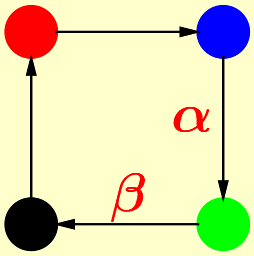
Transition Relation



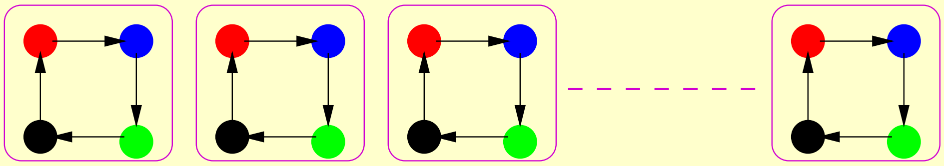
Parametrized System of Finite-State Processes (German and Sistla)

Finite-state process $\rightarrow$

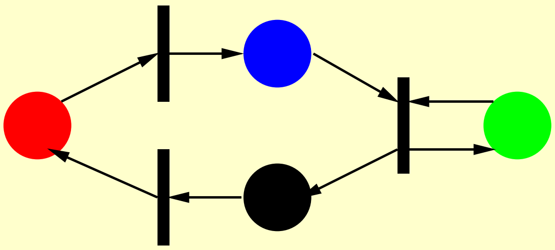
synchronize: α, β



Parametrized system



Petri net representation $\rightarrow$



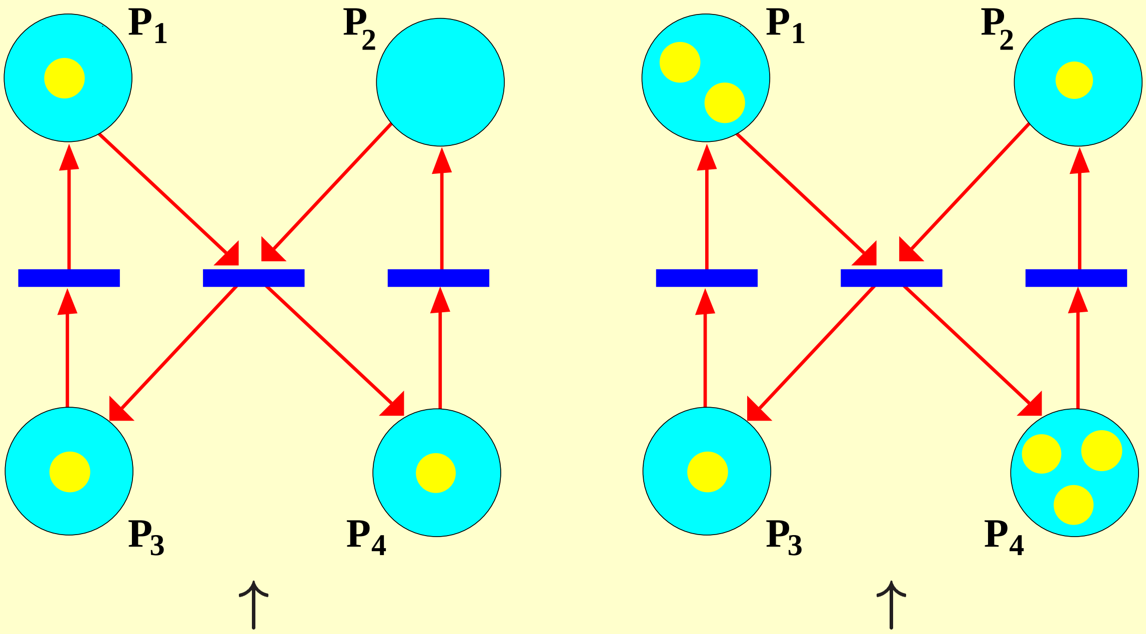
Applications

Broadcast Protocols Esparza, Finkel, Mayr

Cache Coherence Protocols Delzanno

Ordering on Markings

$M_1 \leq M_2$ **iff** $\forall p \,.\, M_1(p) \leq M_2(p)$



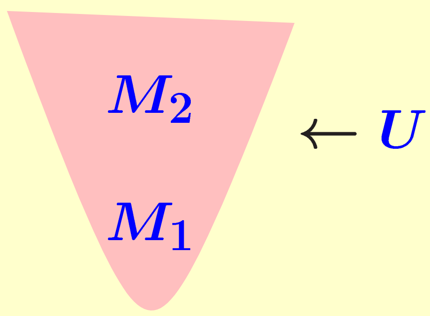
$$M_1 \qquad\qquad \leq \qquad\qquad M_2$$

Upward-Closed Sets of Markings U

$M_1 \in U$ **and** $M_1 \leq M_2$

imply

$M_2 \in U$



Coverability Problem

Instance: M_{init} and U_{final}

$$U_{final}$$
$$\downarrow$$

Question: $M_{init} \longrightarrow \cdots \longrightarrow M$?

- coverability models safety properties:
  - U: set of bad states

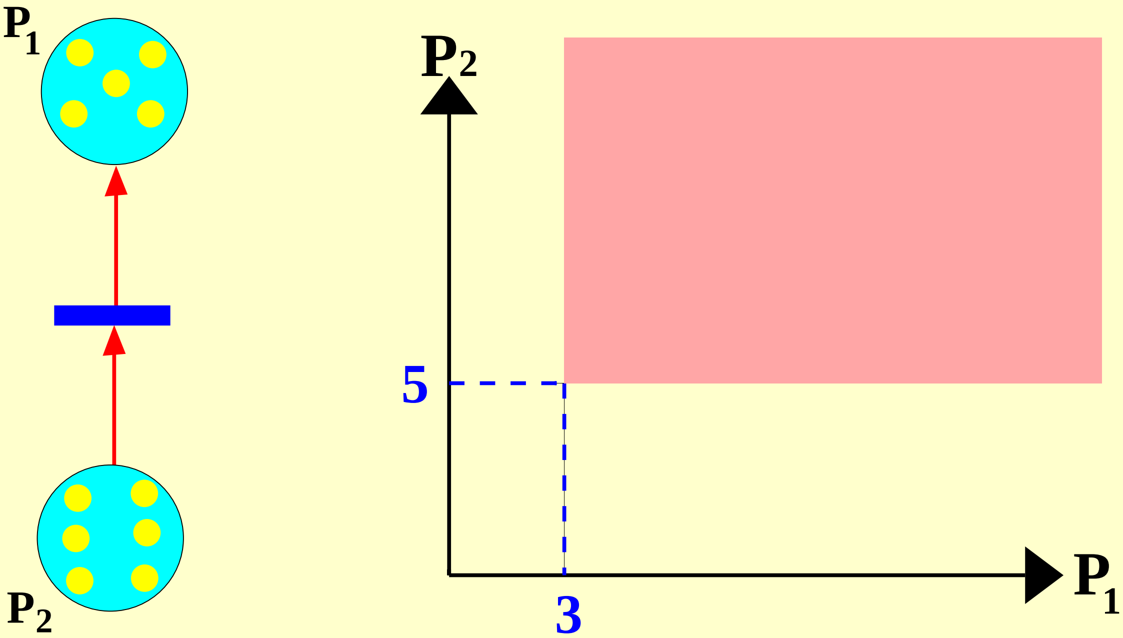
- how to check coverability?
  - symbolic reachability analysis

Symbolic Representation – Minimal Elements

N : mapping from places to *Nat*

$[\![N]\!] = \{M \mid N \leq M\}$

$N(P_1) = 3 \qquad N(P_2) = 5$



$\uparrow \qquad\qquad\qquad\qquad \uparrow$

$M \quad \in \quad [\![N]\!]$

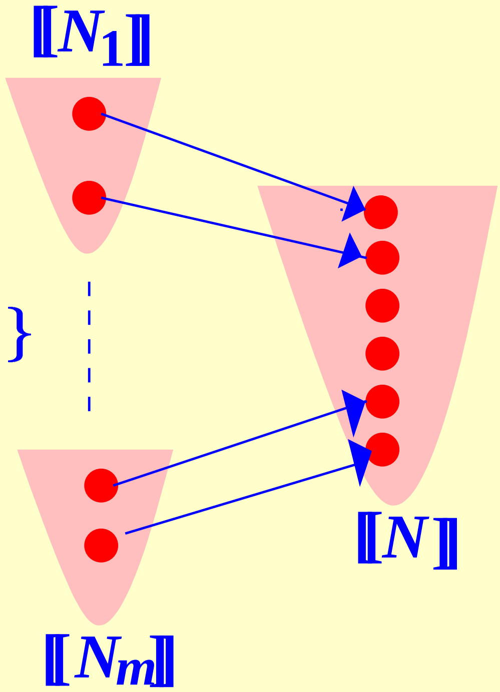
---

if $M \leq M'$ then $M' \in [\![E]\!]$

Pre

N: **minimal element**

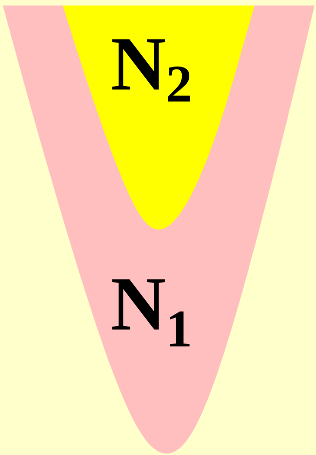
$Pre(N) = \{N_1, \ldots, N_m\}$



$\sqsubseteq$: **"Stronger than"**

N_1, N_2 : **minimal elements**

$N_1 \sqsubseteq N_2$ **iff** $[\![N_2]\!] \subseteq [\![N_1]\!]$



Backward Reachability Algorithm: M_{init} , N_{final}

---

start with N_{final}, apply Pre repeatedly

$\psi_0,\ \psi_1,\ \psi_2,\ \psi_3,\ \ldots$

$\psi_0 = \{N_{final}\}$

$\psi_{i+1} = \psi_i \cup \{N' \mid \exists N \in \psi_i \,.\, N' \in Pre(N)\}$

ψ_i: N_{final} reachable within i steps

Termination :

new minimal elements $\sqsupseteq$ previous ones

$\forall N' \in \psi_{j+1} \,.\, \exists N \in \psi_j \,.\, N \sqsubseteq N'$

Reachability : membership of M_{init} in generated minimal elements

$\exists N \in \psi_j \,.\, M_{init} \in [\![N]\!]$?

Backward Reachability Algorithm:

M_{init} , N_{final}

- start with N_{final}, apply Pre repeatedly

$N_{final} = N_0 \ , \ N_1 \ , \ N_2 \ , \ \ldots$

---

iteration i : N_{final} reachable within i steps

Termination : new existential zones $\sqsupseteq$ previous ones

---

Reachability : membership of M_{init} in generated minimal elements

Termination

= well quasi-ordering (WQO) of minimal elements under $\sqsubseteq$

N_0 , N_1 , N_2 , . . .

$\exists\, i\, ,\, j\, .\, (i < j)$ and $(N_i \sqsubseteq N_j)$

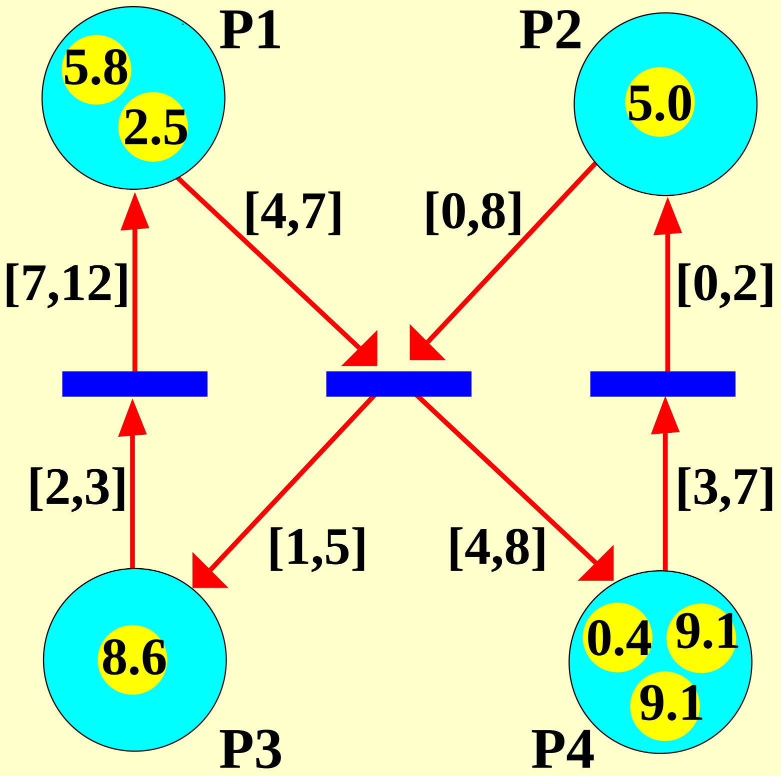
Properties of WQO

- equality on a finite domain is a WQO
- WQOs are preserved when building:

  finite sets, bags, and strings

Consequence: Minimal Elements are WQO

Timed Petri Nets



- Tokens have "ages": Real numbers
- Conditions on ages: Intervals

Bag (of real numbers)

mapping from reals to natural numbers

$$B = \{4.5\ ,\ 8.0\ ,\ 4.5\}$$

$$B(4.5) = 2 \quad B(8.0) = 1 \quad B(1.5) = 0$$

Marking

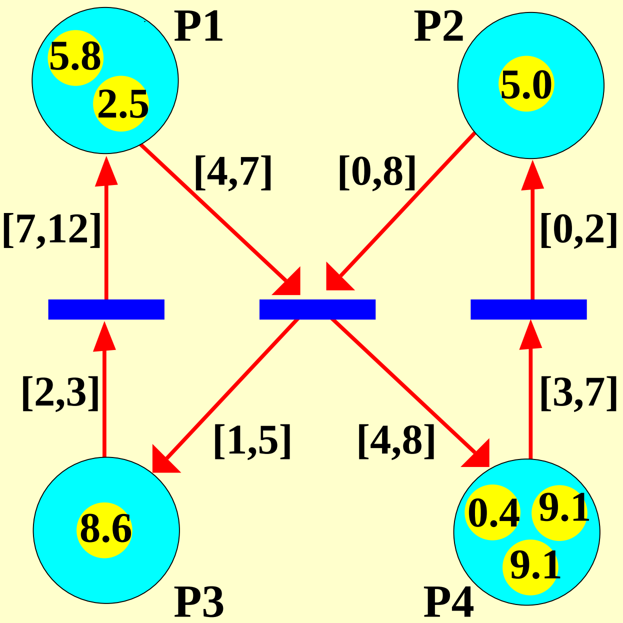
mapping from places to bags

$$M(P_1) = \{5.8,\ 2.5\}$$

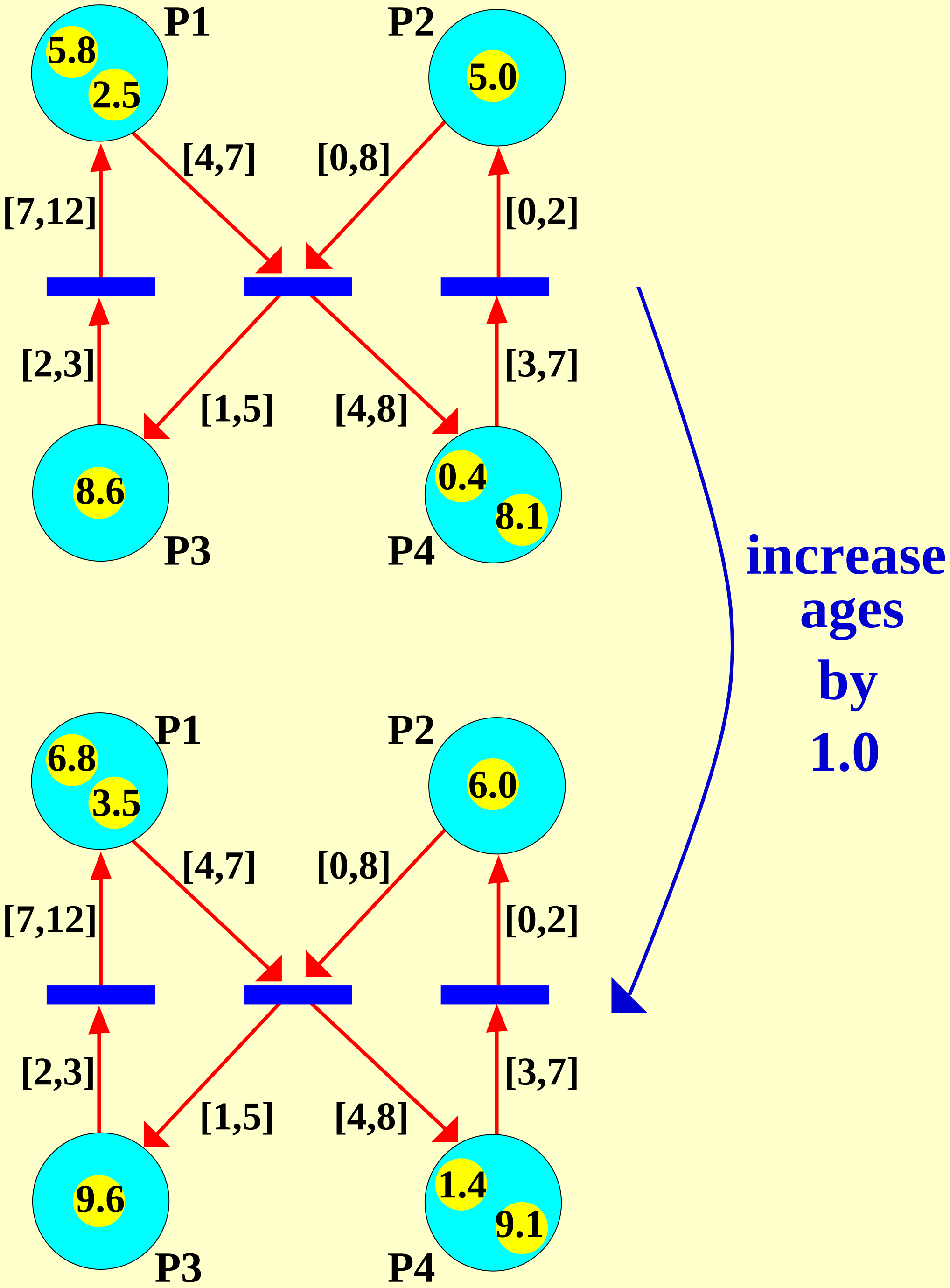
$$M(P_2) = \{5.0\}$$

$$M(P_3) = \{8.1\}$$

$$M(P_4) = \{0.4,\ 9.1\ ,9.1\}$$

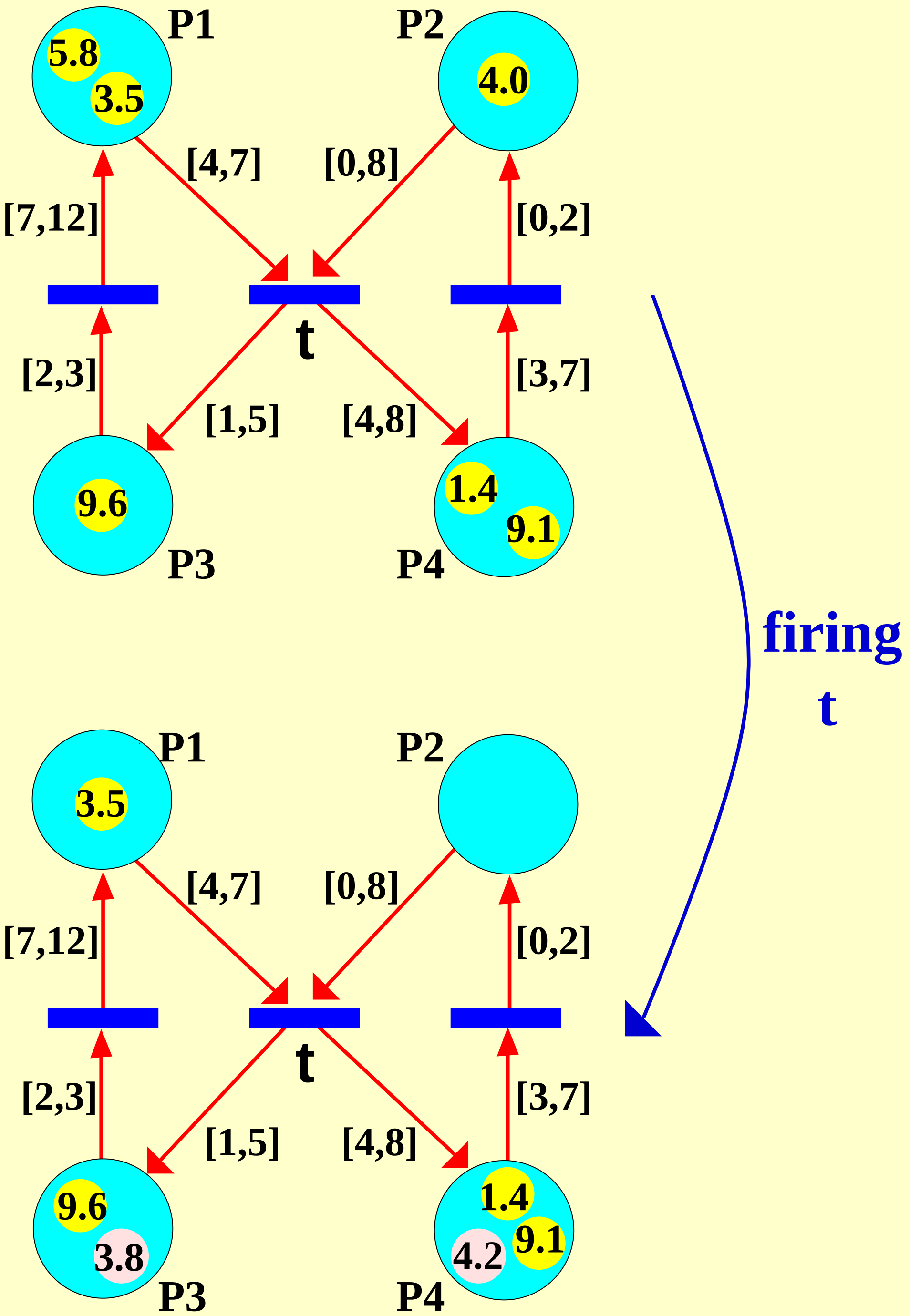


Timed Transitions $\longrightarrow_T$



Remark: lazy behaviour !!

Discrete Transitions $\longrightarrow_D$



Transition Relation

$$\longrightarrow \; = \; (\longrightarrow_T \;\cup\; \longrightarrow_D)$$

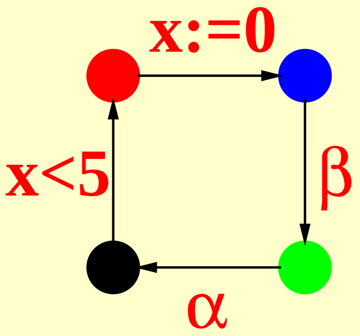
$$M_1 \longrightarrow M_2 \; = \; (M_1 \longrightarrow_T M_2) \;\; \text{or} \;\; (M_1 \longrightarrow_D M_2)$$

Remark

- unbounded number of real-valued clocks
  - infinite in two directions

Parametrized System of Timed Processes

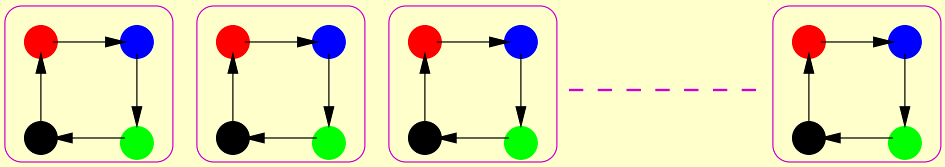
timed process $\rightarrow$



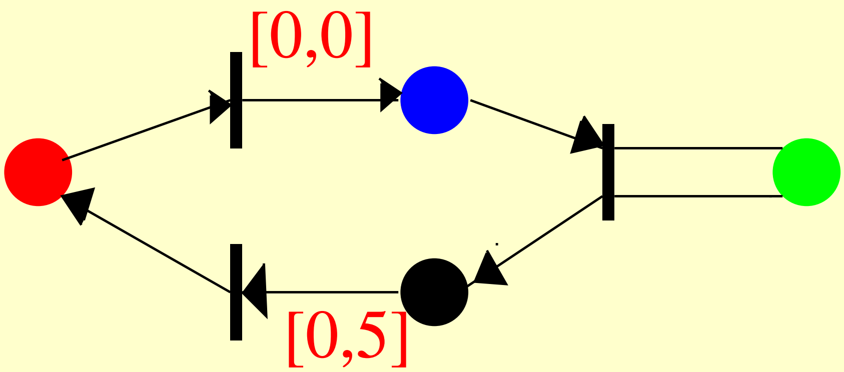
synchronize: α, β

clock operations:
conditions, reseting

Parametrized system

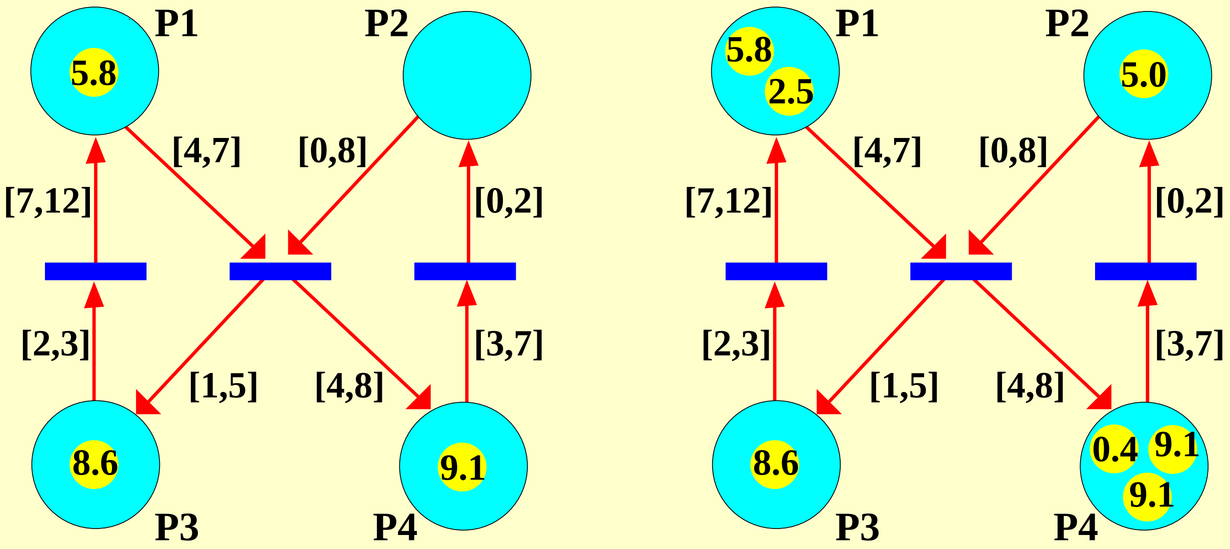


Timed Petri net representation



Ordering on Markings

$$M_1 \leq M_2 \quad \textbf{iff} \quad \forall p,\ x.\ M_1(p)(x) \leq M_2(p)(x)$$



$\uparrow$ $\uparrow$

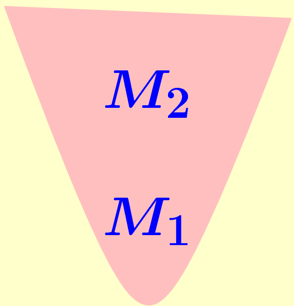
$$M_1 \qquad \leq \qquad M_2$$

Upward-Closed Sets of Markings U

$M_1 \in U$ **and** $M_1 \leq M_2$

imply

$M_2 \in U$



$\leftarrow U$

Coverability Problem

Instance: M_{init} and U_{final}

U_{final}

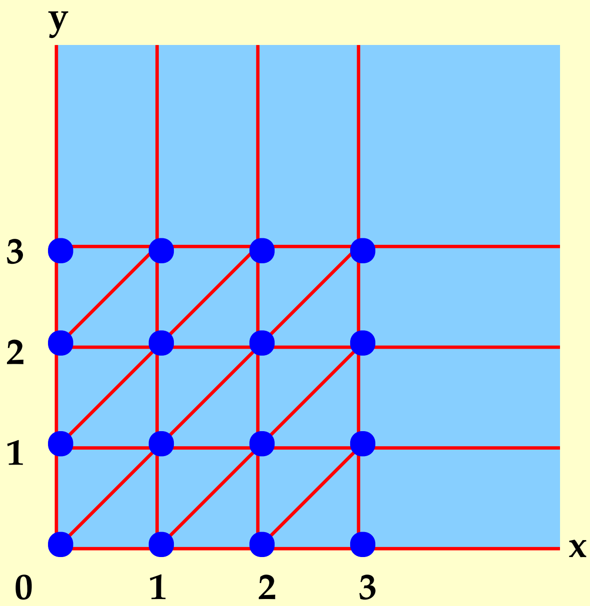
$\downarrow$

Question: $M_{init} \longrightarrow \cdots \longrightarrow M$ **?**

- coverability models safety properties:
  - U: set of bad states
- how to check coverability?
  - symbolic reachability analysis

Regions

- finite number of clocks



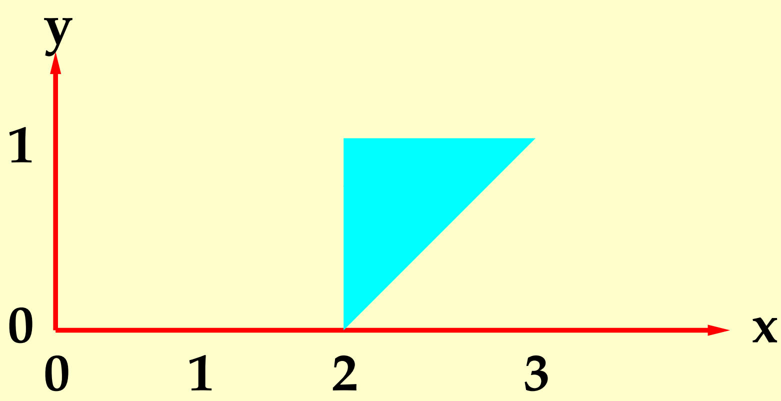
two clocks: x, y

$cmax = 3$

- Equivalence relation on clock values

- clock values equivalent if
  - same integral parts
  - same ordering of fractional parts
  - clock values beyond $cmax$ equivalent

Example

- $R:$ 

- $V(x) = 2.4, \; V(y) = 0.8$

- $V \in [\![R]\!]$

- not sufficiently powerful for timed Petri nets

Existential Regions

$$ER:$$
$$\exists x_1, \ldots, x_n.\ R(x_1, \ldots, x_n)\ \wedge\ P(x_1, \ldots, x_n)$$

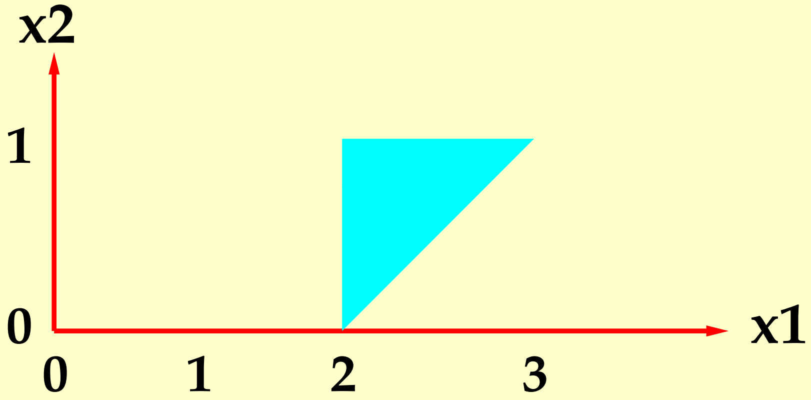
- $x_1, \ldots, x_n$: tokens
- $R(x_1, \ldots, x_n)$: region
- $P(x_1, \ldots, x_n)$: assign tokens to places

- ER: minimal set of conditions

Existential Regions – Example

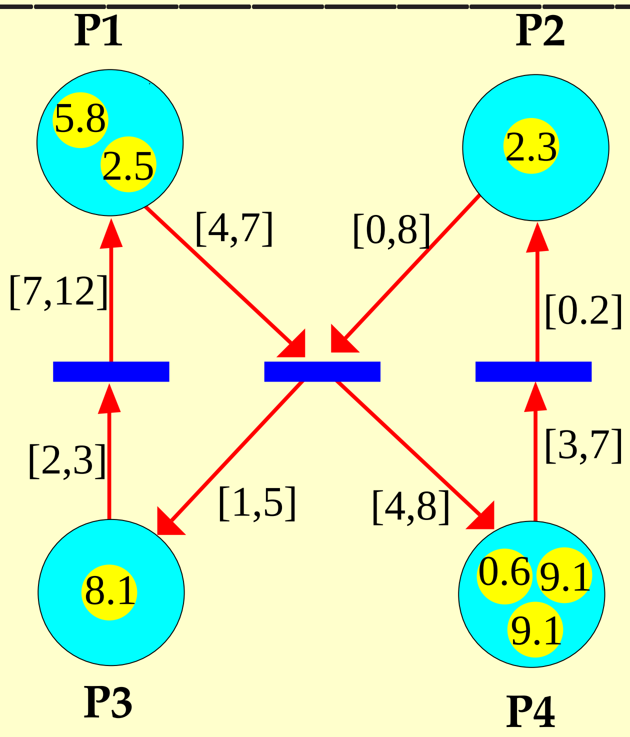
$ER: \quad \exists x_1, x_2.\ R(x_1, x_2)\ \wedge\ P(x_1, x_2)$

$R(x_1, x_2)$



$P(x_1, x_2)$: x_1 in P_2 , x_2 in P_4

M :



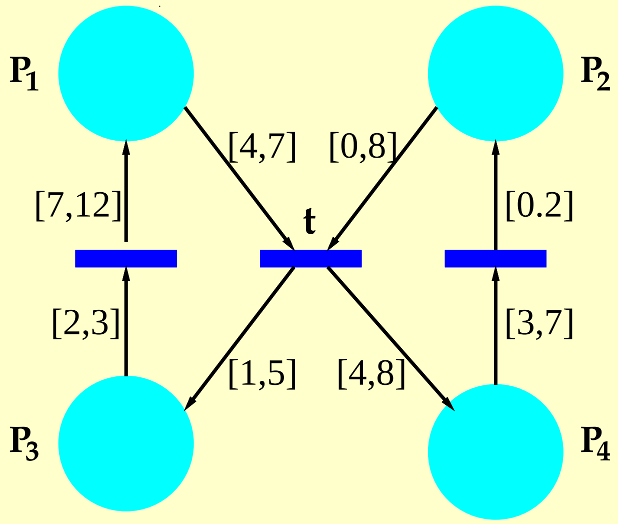
$\in\ [\![ER]\!]$

if $M \leq M'$ then $M' \in [\![ER]\!]$

Constraint Explosion Problem $Pre(\phi)$ large

ER :

$\exists x.$ (3 —— 4
x in P_3)

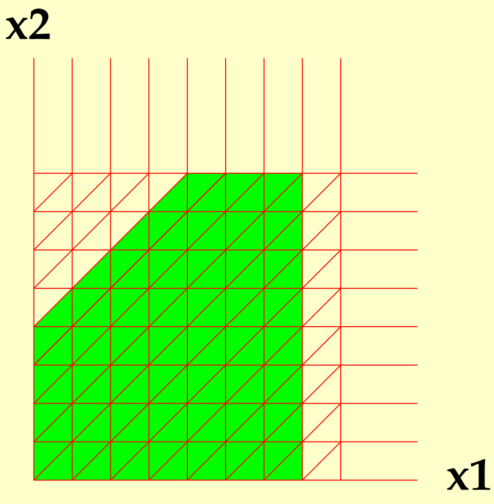


$Pre(ER, t)$:

$\exists\ x_1\ x_2$.

x_1 in P_1

x_2 in P_2



130

existential

regions !!

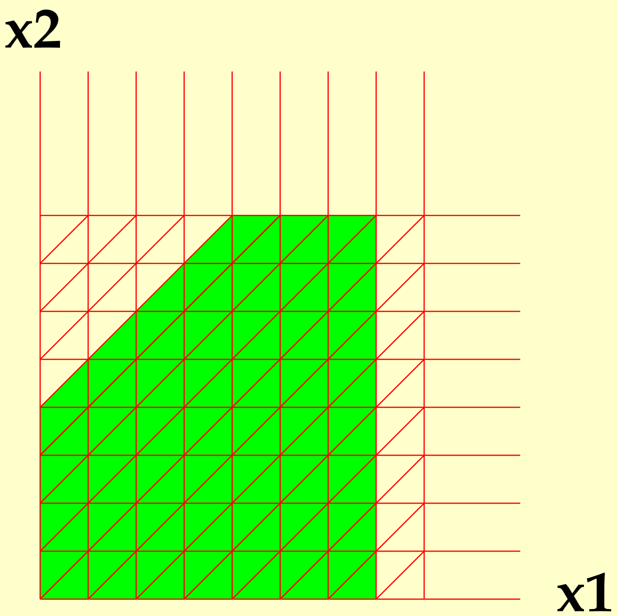
Solution: Use existential zones !!

Zones

- finite number of clocks:
  e.g. timed automata

Z :

$$0 \leq x_1 \leq 8$$
$$\wedge$$
$$0 \leq x_2 \leq 8$$
$$\wedge$$
$$x_2 - x_1 \leq 4$$



- not sufficiently powerful for timed Petri nets

Existential Zones

$$E:$$
$$\exists x_1, \ldots, x_n.\ Z(x_1, \ldots, x_n)\ \wedge\ P(x_1, \ldots, x_n)$$

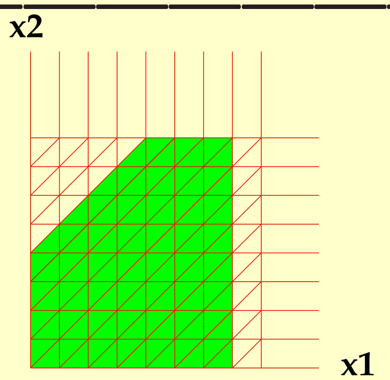
- $x_1, \ldots, x_n$: tokens
- $Z(x_1, \ldots, x_n)$: zone
- $P(x_1, \ldots, x_n)$: assign tokens to places

- E: minimal set of conditions

Existential Zones – Example

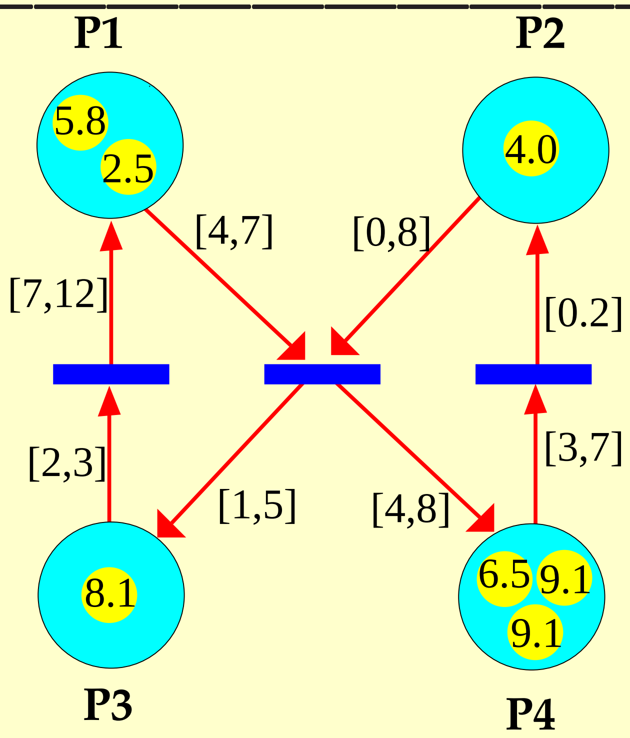
$E: \quad \exists x_1, x_2.\ Z(x_1, x_2) \ \wedge \ P(x_1, x_2)$

$$Z(x_1, x_2): \quad \begin{array}{c} 0 \leq x_1 \leq 8 \\ \wedge \\ 0 \leq x_2 \leq 8 \\ \wedge \\ x_2 - x_1 \leq 4 \end{array}$$



$P(x_1, x_2)$: x_1 **in** P_2 , x_2 **in** P_4

M :



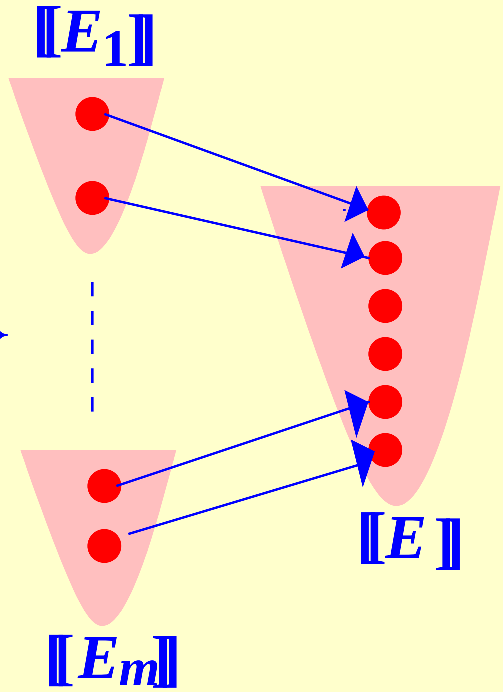
$\in \ [\![E]\!]$

if $M \leq M'$ **then** $M' \in [\![E]\!]$

Pre

E: existential zone

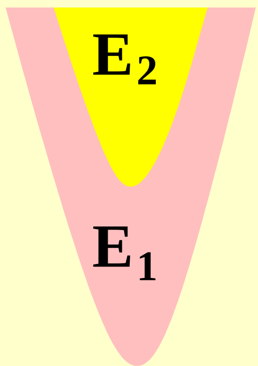
$Pre(E) = \{E_1, \ldots, E_m\}$



$\sqsubseteq$: "Stronger than"

E_1, E_2 : existential zones

$E_1 \sqsubseteq E_2$ **iff** $[\![E_2]\!] \subseteq [\![E_1]\!]$



Backward Reachability Algorithm:
M_{init} , E_{final}

- start with E_{final}, apply Pre repeatedly

$E_{final} = E_0 \, , \, E_1 \, , \, E_2 \, , \, \ldots$

---

iteration i : E_{final} reachable within i steps

Termination : new existential zones $\sqsupseteq$ previous ones

---

Reachability : membership of M_{init} in generated existential zones

Backward Reachability Algorithm:

M_{init} , E_{final}

- start with E_{final}, apply Pre repeatedly

$E_{final} = E_0$, E_1 , E_2 , $\ldots$

---

iteration i : E_{final} reachable within i steps

Termination : new existential zones $\sqsupseteq$ previous ones

---

Reachability : membership of M_{init} in generated existential zones

Termination

= well quasi-ordering (WQO) of existential zones under $\sqsubseteq$:

E_0 , E_1 , E_2 , ...

$\exists\, i\,,\, j\,.\,(i < j)$ and $(E_i \sqsubseteq E_j)$

Existential zones are built:

- starting from a finite domain

and

- repeatedly building finite sets, bags, strings, and disjunctions

---

However:

- WQOs not closed under disjunction !!

Better Quasi-Orderings (BQO)

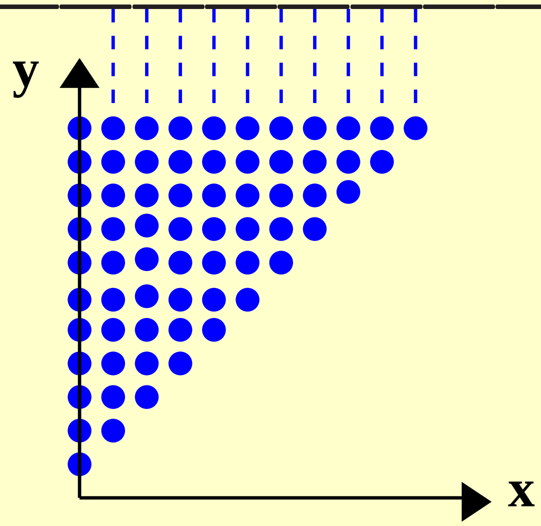
- BQO implies WQO
- equality on a finite domain is a BQO
- BQOs are preserved when building:

  finite sets, strings, bags, and
  disjunctions

Consequence: Existential zones are BQO

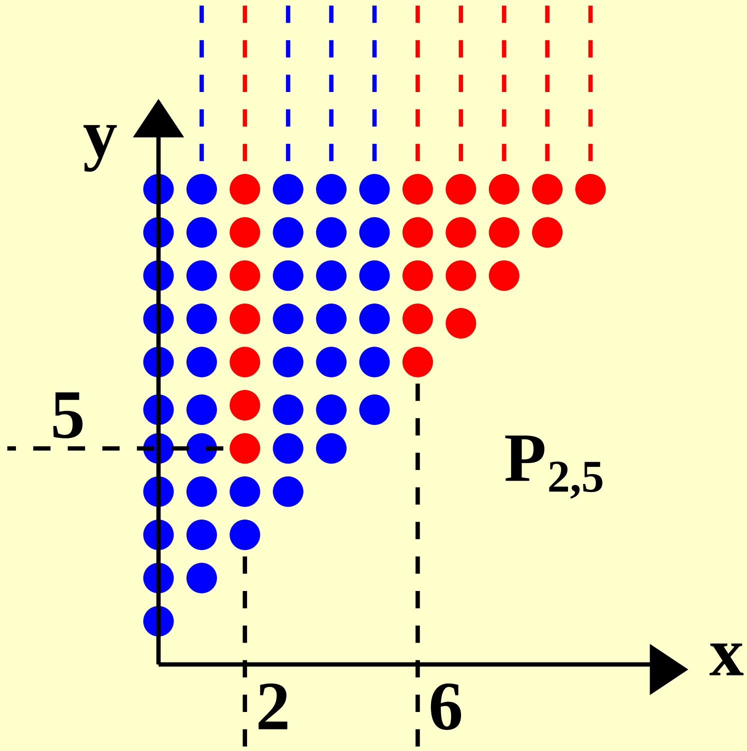
WQO not closed under disjunction !!

$Z \ = \{(x,y) \mid x \ < \ y\}$



$(x,y) \in Z$: $\quad [\![P_{x,y}]\!] \subseteq Z$

$$P_{x,y}(a,b) \ = \left(\begin{array}{c} (a > y) \\ \textit{or} \\ \left(\begin{array}{c} (a = x) \\ \textit{and} \\ (b \geq y) \end{array} \right) \end{array} \right)$$



$$P_{x,y}(a,b) \;=\; \left(\begin{array}{c} (a > y) \\ \mathit{or} \\ \left(\begin{array}{c} (a = x) \\ \mathit{and} \\ (b \geq y) \end{array} \right) \end{array} \right)$$

$$P_{x_1,y_1} \sqsubseteq P_{x_2,y_2} \;=\; \left(\begin{array}{c} (x_2 > y_1) \\ \mathit{or} \\ \left(\begin{array}{c} (x_2 = x_1) \\ \mathit{and} \\ (y_2 \geq y_1) \end{array} \right) \end{array} \right)$$

$\sqsubseteq$ **is WQO:**

$P_{x_1,y_1} \quad P_{x_1,y_1} \quad P_{x_1,y_1} \quad \cdots$

$P_{a,z_1} \quad P_{a,z_2} \quad P_{a,z_3} \quad \cdots$

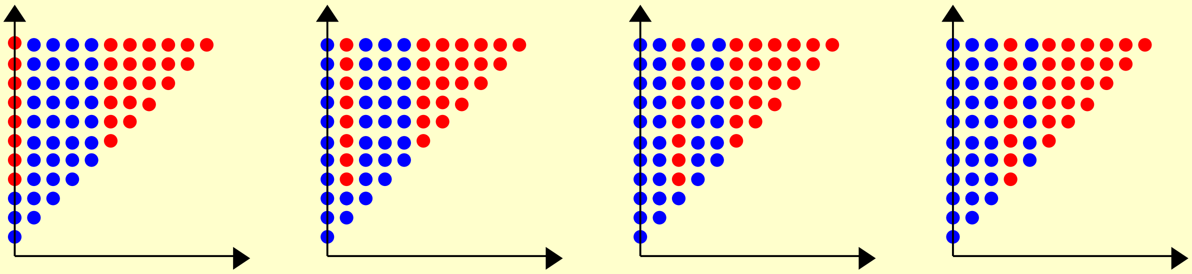
$\exists i, j : \; z_i \leq z_j$

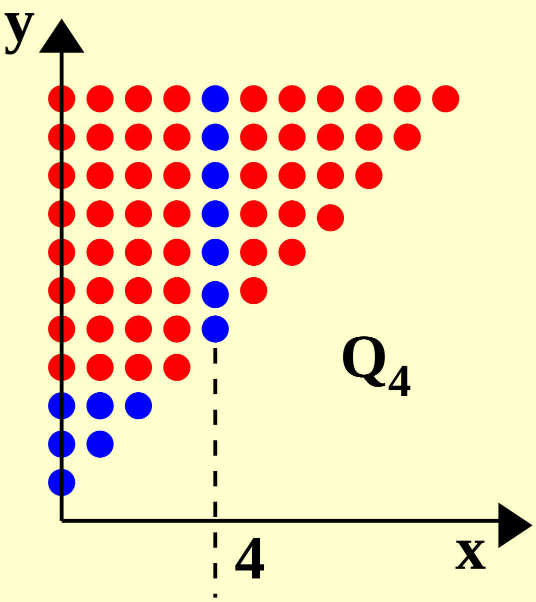
$P_{a,z_i} \sqsubseteq P_{a,z_j}$

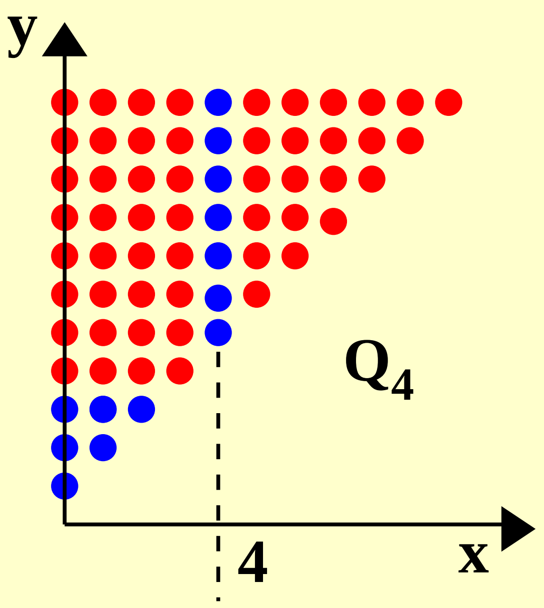
Disjunctions of $P_{x,y}$

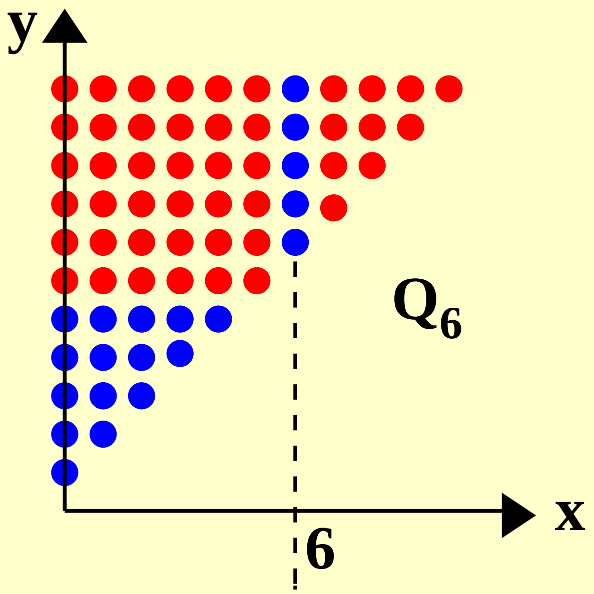
$$Q_y \;=\; P_{0,y} \;\vee\; P_{1,y} \;\vee\; \cdots \;\vee\; P_{y-1,y}$$

$$Q_4 \;=\; P_{0,4} \;\vee\; P_{1,4} \;\vee\; P_{3} \;\vee\; P_{3,4}$$









$\sqsubseteq$ not wqo on Q_y: Q_1 Q_2 Q_3 $\cdots$

Termination

$=$ well quasi-ordering (WQO) of existential zones under $\sqsubseteq$:

E_0 , E_1 , E_2 , ...

$\exists\ i\ ,\ j\ .\ (i < j)$ and $(E_i \sqsubseteq E_j)$

---

1. Existential regions are WQO
   - start from a finite domain
   - repeatedly build finite sets, bags, and strings
2. existential zone $=$ finite disjunction of existential regions
3. existential zones BQO ?

Problem:

- WQOs not closed under disjunction !!

Better Quasi-Orderings (BQO)

- BQO implies WQO
- equality on a finite domain is a BQO
- BQOs are preserved when building:

  finite sets, strings, bags, and
  <u>disjunctions</u>

Consequence: Existential zones are BQO

Conclusions and Future Work

- Parametrized Systems of (Timed) Processes
  - unbounded number of real-valued clocks
  - more powerful than timed automata
- application of symbolic model checking
- using BQOs in design of symbolic representation
- Future Directions
  - parametrized multi-clock processes
  - more experimental results