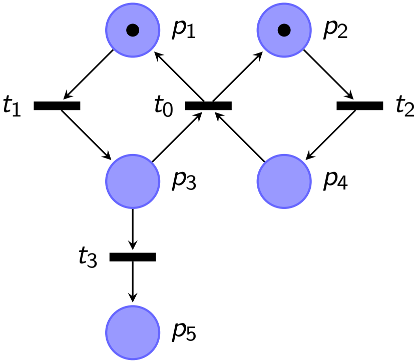
Symbolic Unfolding of Time Petri Nets

Didier Lime

École Centrale de Nantes – IRCCyN

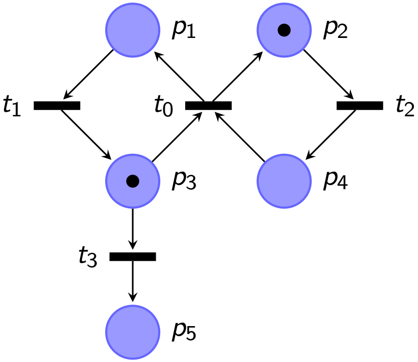
Réunion AFSEC Concurrence
Cachan
19 November 2013

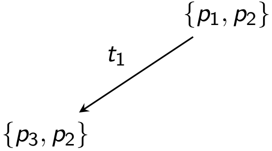
Petri Nets, Sequentiality, and Concurrency



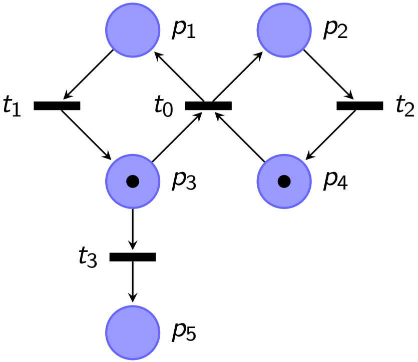
$\{p_1, p_2\}$

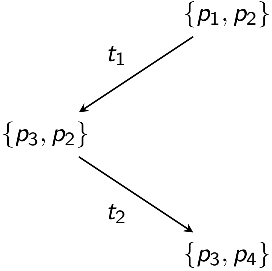
Petri Nets, Sequentiality, and Concurrency



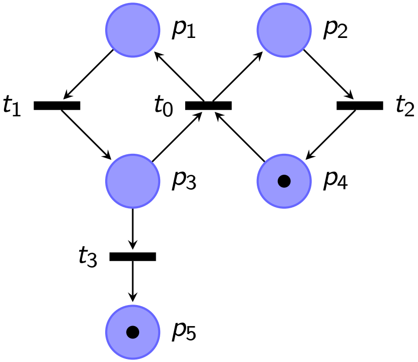


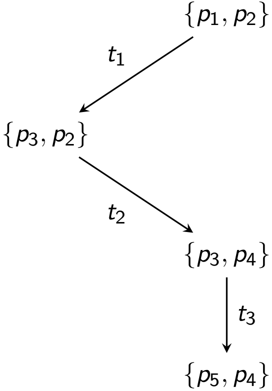
Petri Nets, Sequentiality, and Concurrency



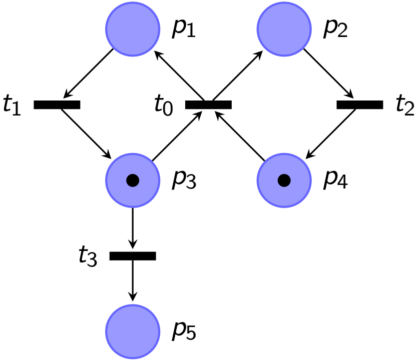


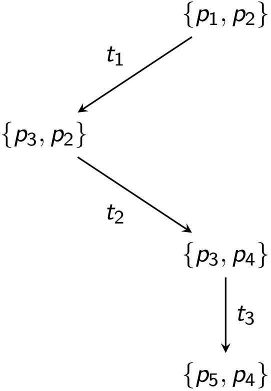
Petri Nets, Sequentiality, and Concurrency



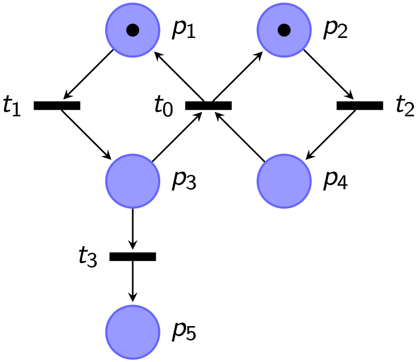


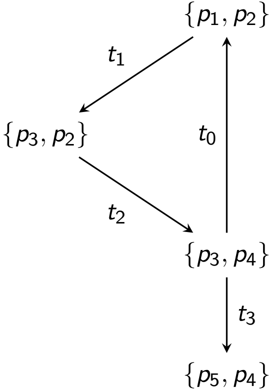
Petri Nets, Sequentiality, and Concurrency



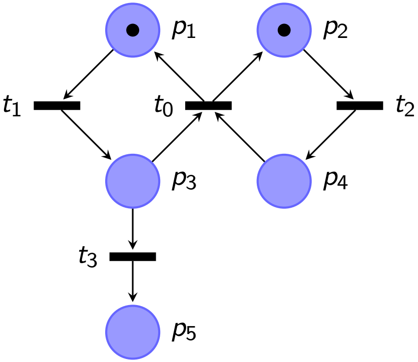


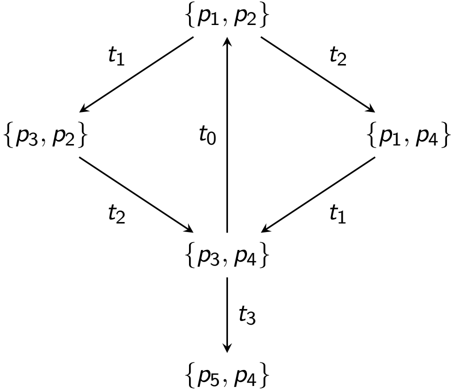
Petri Nets, Sequentiality, and Concurrency





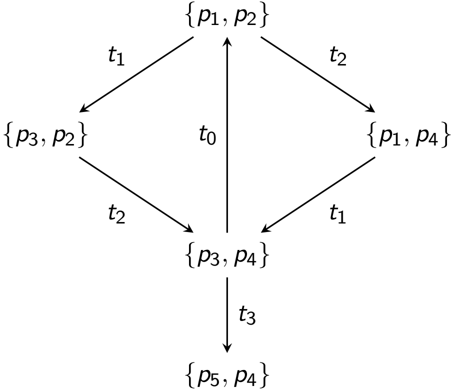
Petri Nets, Sequentiality, and Concurrency



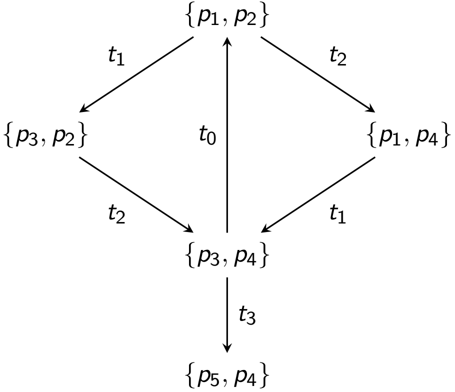


Petri Nets, Sequentiality, and Concurrency

- Are t_1 and t_2 concurrent?
- Can we avoid the enumeration of interleavings.



Petri Nets, Sequentiality, and Concurrency

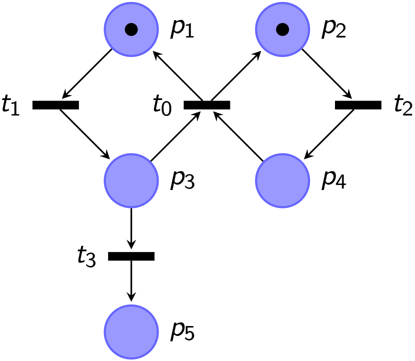


- Are t_1 and t_2 concurrent?
- Can we avoid the enumeration of interleavings.

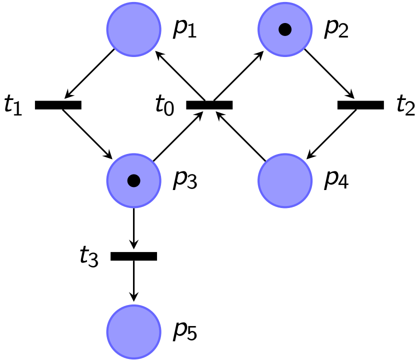
Preserve the structural relations between events

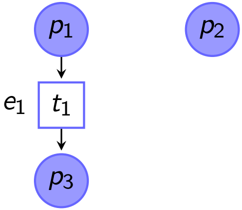
- run $\rightarrow$ process;
- set of runs $\rightarrow$ branching processes;
- marking graph $\rightarrow$ unfolding.

Processes and Branching Processes [McM92]

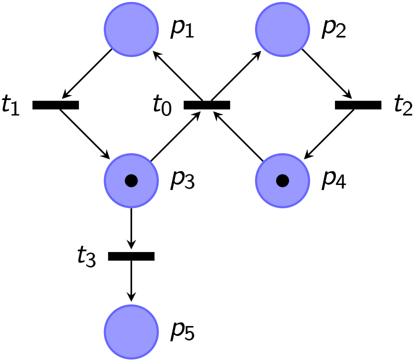


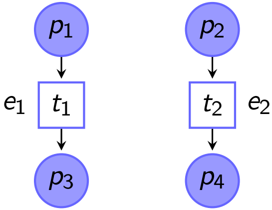
Processes and Branching Processes [McM92]



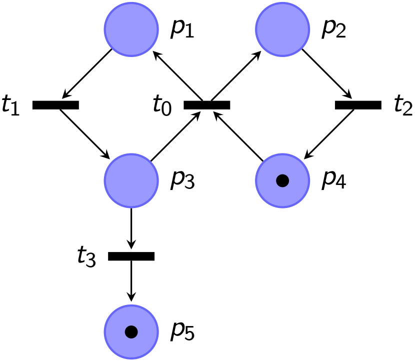


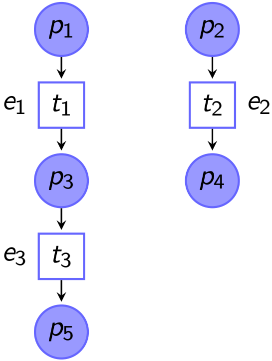
Processes and Branching Processes [McM92]



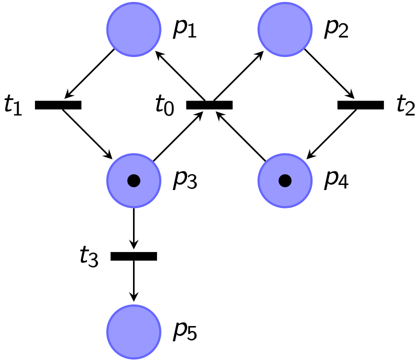


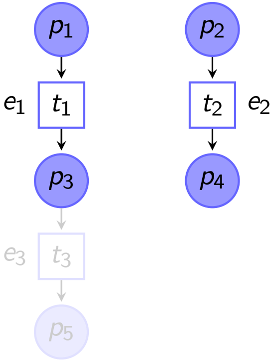
Processes and Branching Processes [McM92]



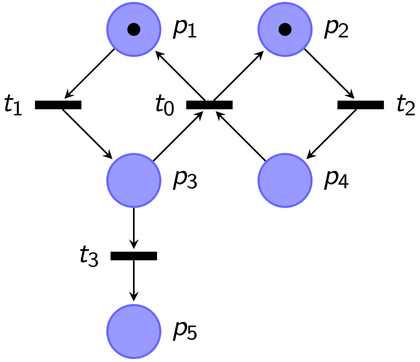


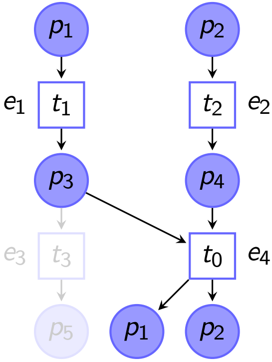
Processes and Branching Processes [McM92]



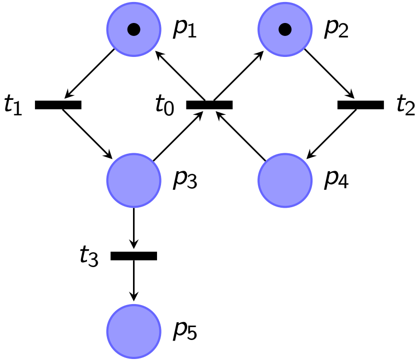


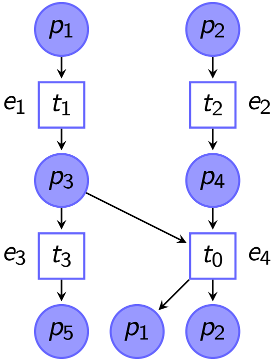
Processes and Branching Processes [McM92]



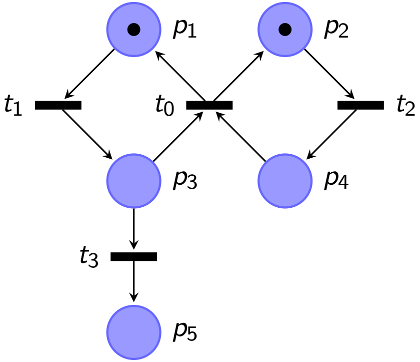


Processes and Branching Processes [McM92]





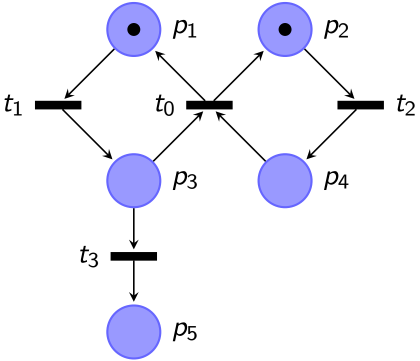
Processes and Branching Processes [McM92]

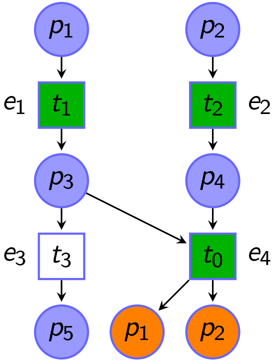


The unfolding is the union of all branching processes.

The exists of a finite complete prefix

Processes and Branching Processes [McM92]



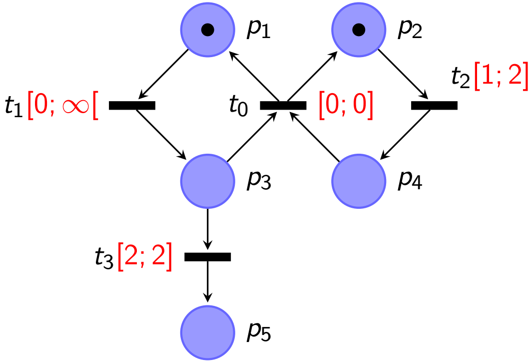


Definition (Cut-off event)

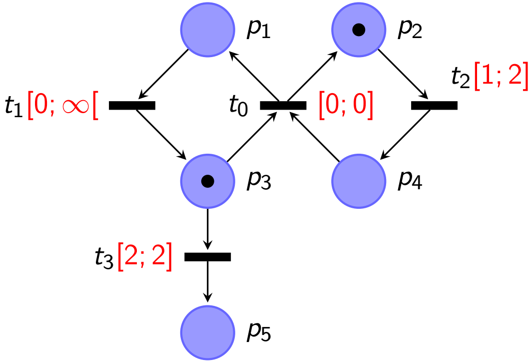
e is a cut-off event if there exists e' s.t.:

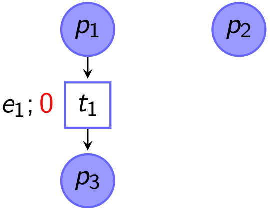
- The marking created by the causal past of e and e' is the same.
- The causal past of e' is less than that of e (adequate order);

Time Processes [AL00]

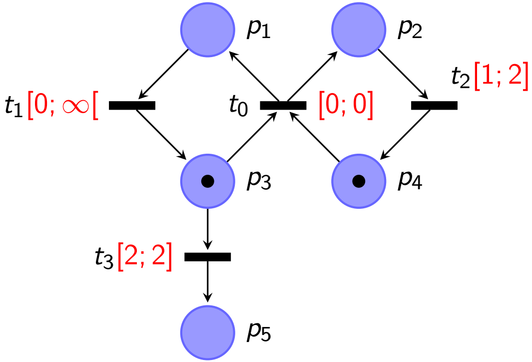


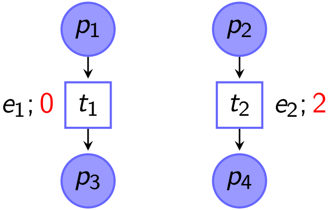
Time Processes [AL00]



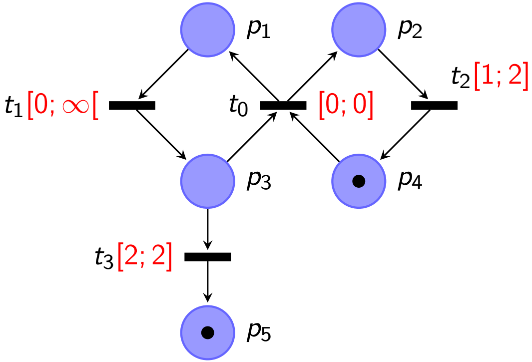


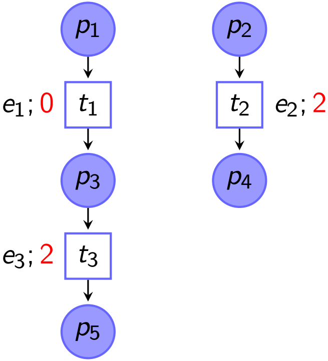
Time Processes [AL00]



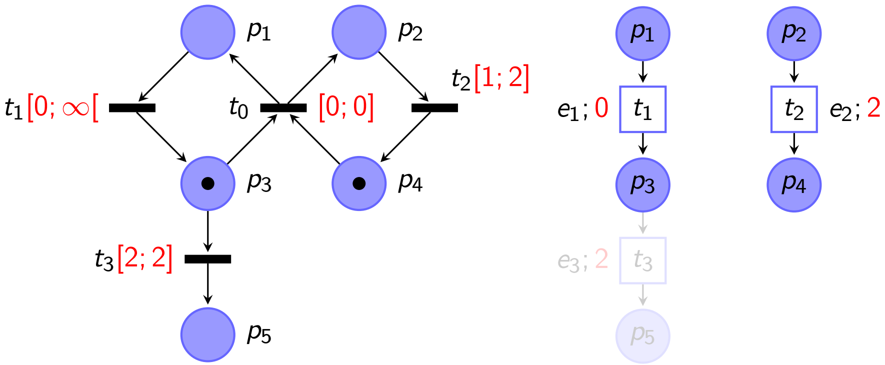


Time Processes [AL00]

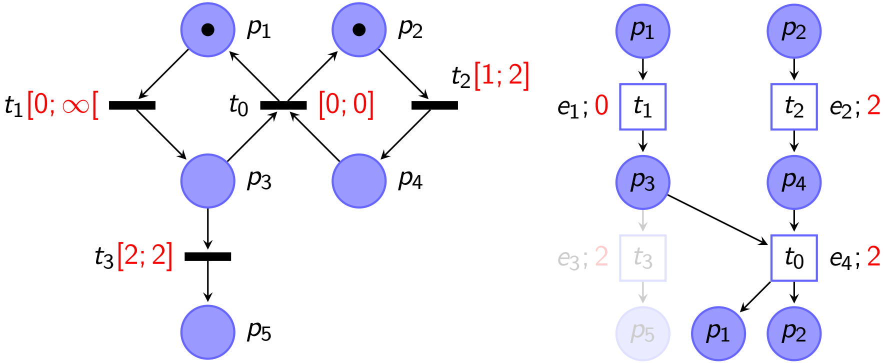




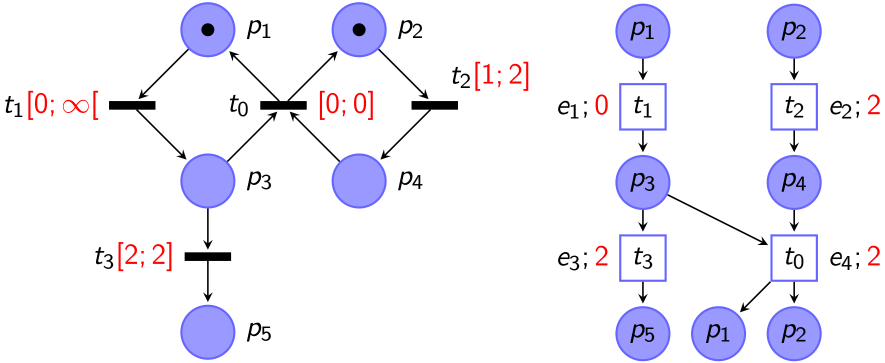
Time Processes [AL00]



Time Processes [AL00]

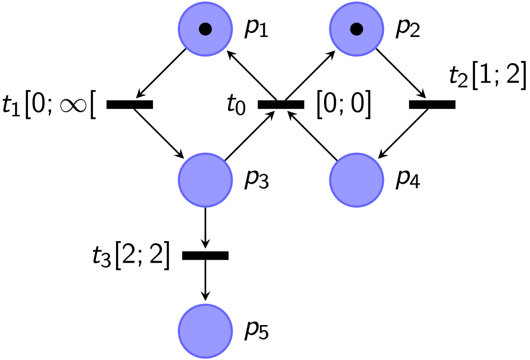


Time Processes [AL00]

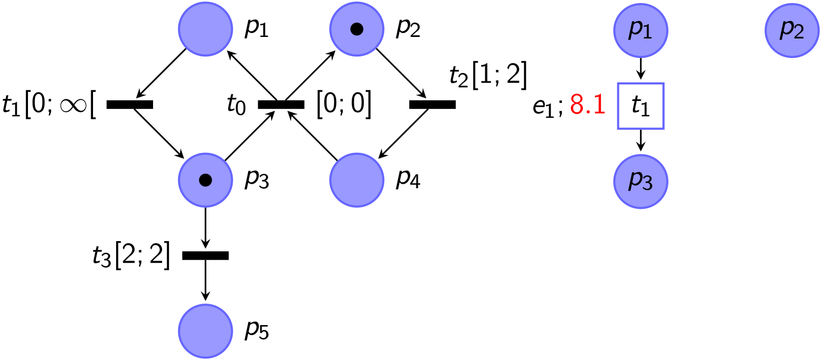


Time branching process?

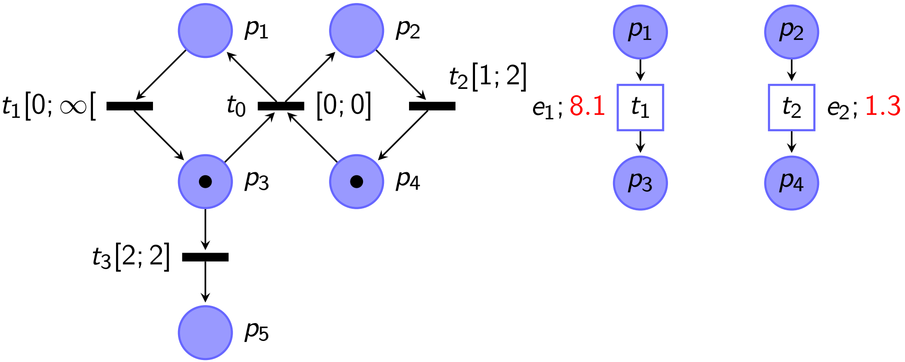
Time Branching Process



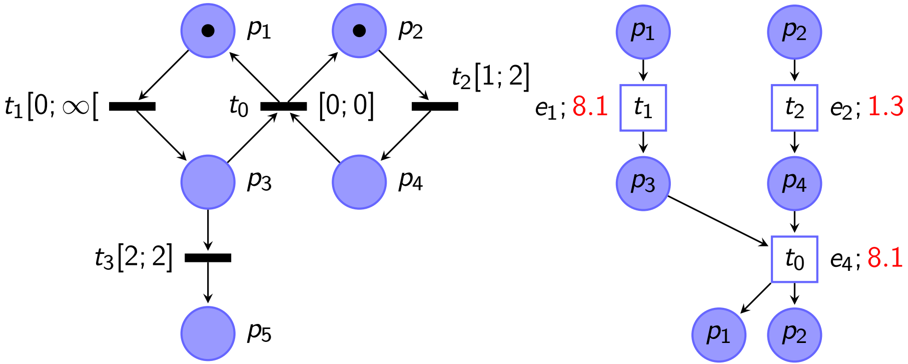
Time Branching Process



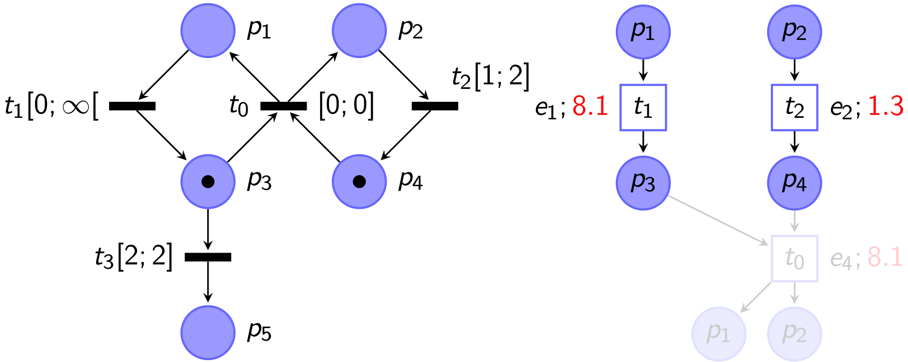
Time Branching Process



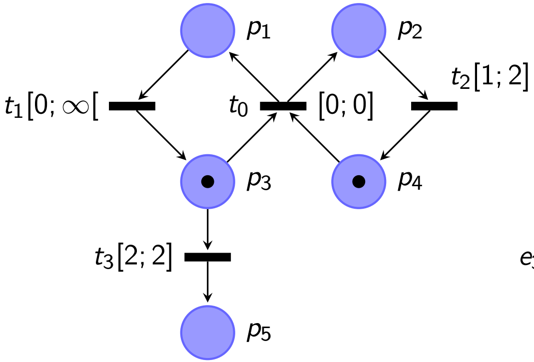
Time Branching Process

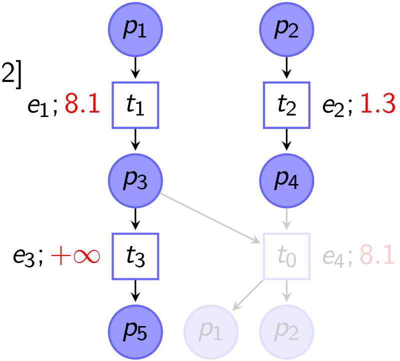


Time Branching Process

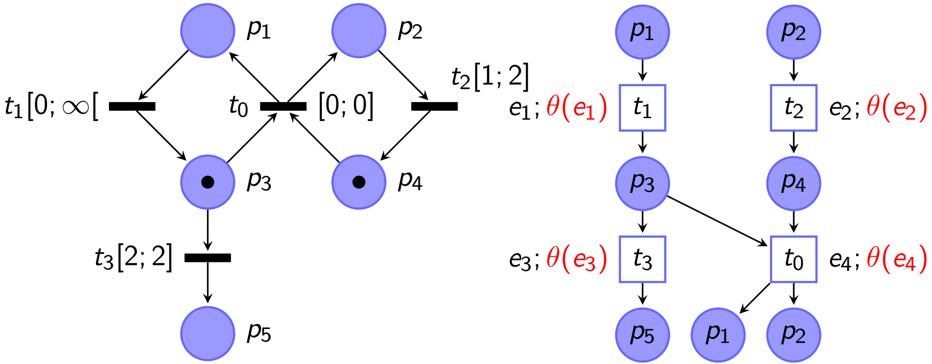


Time Branching Process

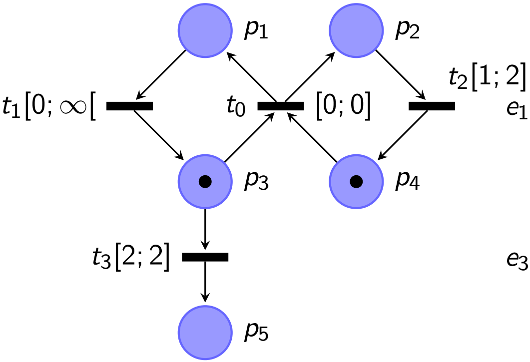


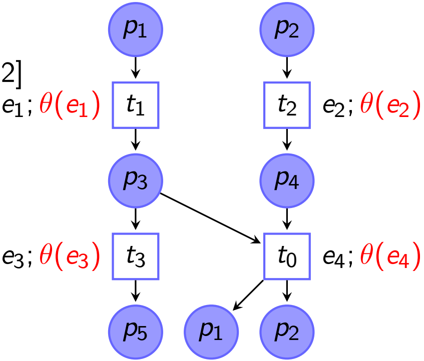


Time Branching Process



Time Branching Process

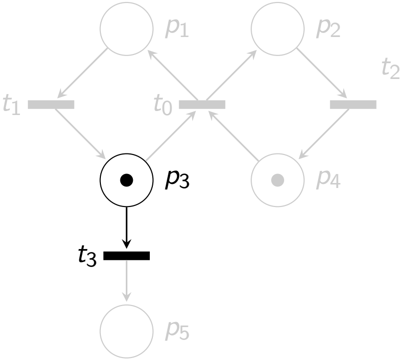




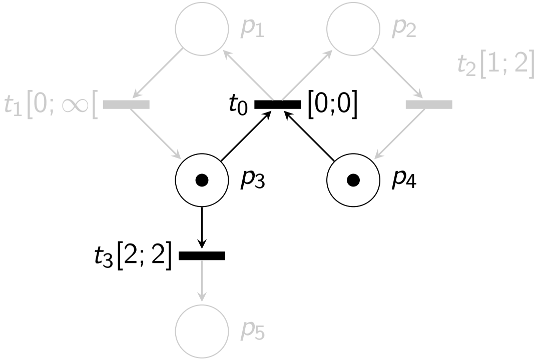
the symbolic unfolding is the union of all valid time branching processes.

$$\left\{ \begin{array}{l} \theta(e_1) = 0, \\ \theta(e_2) = 2, \\ \theta(e_3) = 2, \\ \theta(e_4) = +\infty \end{array} \right. \quad \text{ou} \quad \left\{ \begin{array}{l} 0 \leq \theta(e_1), \\ 1 \leq \theta(e_2) \leq 2, \\ \theta(e_3) = +\infty, \\ \theta(e_4) = \max(\theta(e_1), \theta(e_2)) \end{array} \right.$$

Locality

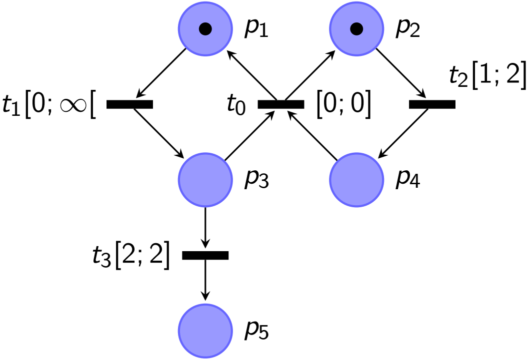


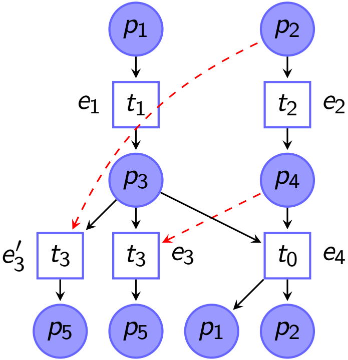
Locality



Conflicts and urgency break the locality of the firing rule.

Locality: A solution from Chatain and Jard [CJ06]

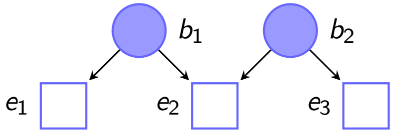




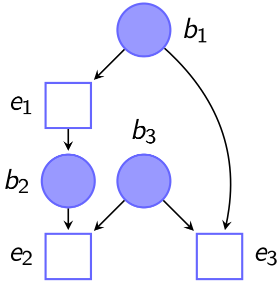
Add read arcs to the unfolding.

$$\begin{cases} 0 \leq \theta(e_1), \\ 1 \leq \theta(e_2) \leq 2, \\ \theta(e_3) = 2, \\ \theta(e'_3) = \theta(e_1) + 2, \\ \theta(e_4) = \max(\theta(e_1), \theta(e_2)) \end{cases}$$

Locality: our approach – strucural analysis of conflicts



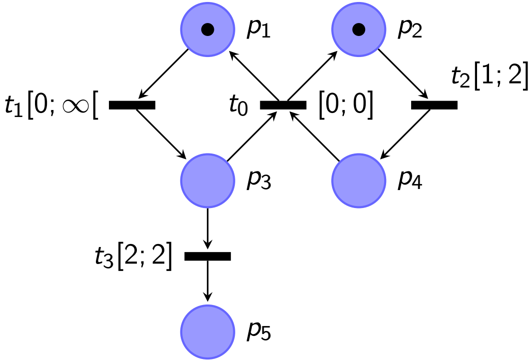
e_1 conf e_2 and e_2 conf e_3

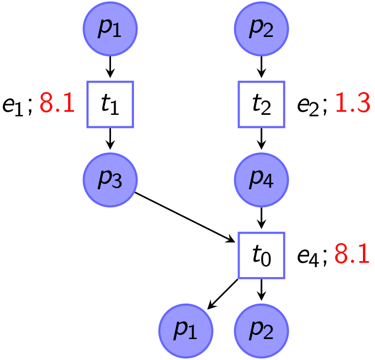


not $e_2 \text{conf} e_3$

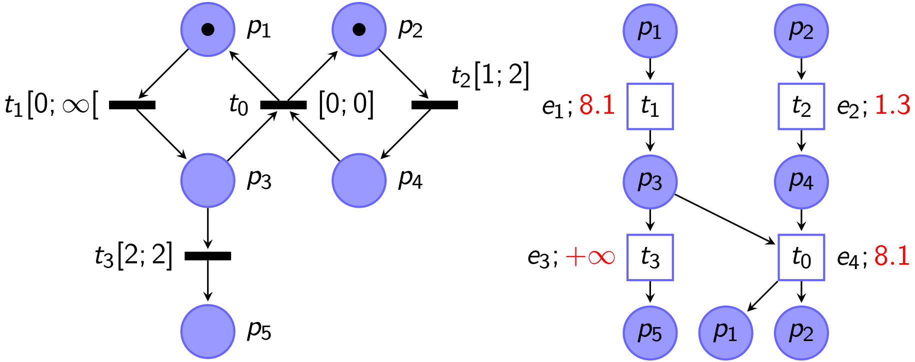
e_1 and e_2 are in direct conflict ($e_1 \text{conf} e_2$) iff they share a precondition and all their preconditions are concurrent.

conf-complete Time Branching Processes





conf-complete Time Branching Processes



Add all the events that are in direct conflict

Valid Time Branching Process

valid = conf-complete + constraints on the occurrence dates of events:
$\forall e \in E$:

$$\Big[\big[\theta(e) \neq +\infty \text{ and } \theta(e) - \mathrm{TOE}({}^\bullet e, l(e)) \in I_s(l(e)) \tag{1}$$

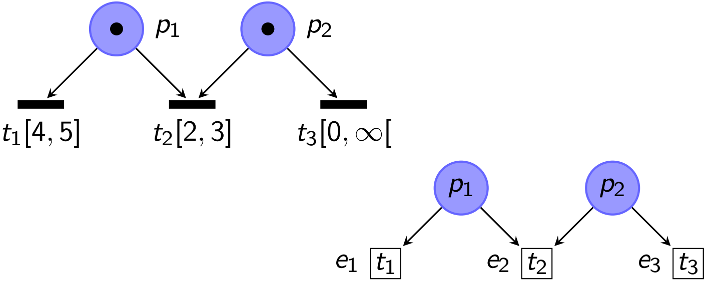
$$\text{and } \forall e' \in E \text{ s.t. } e \,\mathrm{conf}\, e', \theta(e') = +\infty \tag{2}$$

$$\text{or } \big[\theta(e) = +\infty \text{ and } \exists b \in {}^\bullet e, \theta({}^\bullet b) = +\infty\big] \tag{3}$$

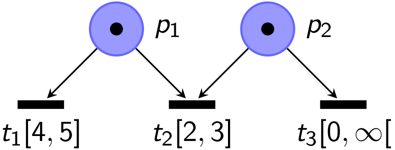
$$\text{or } \big[\theta(e) = +\infty \text{ and } \exists e' \in E \text{ s.t. } e \,\mathrm{conf}\, e' \text{ and } \theta(e') \neq +\infty \text{ and } \theta(e') - \mathrm{TOE}({}^\bullet e, l(e)) \in I_s(l(e))^{\downarrow}\big]\Big] \tag{4}$$

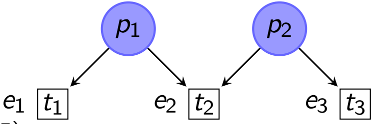
TOE = enabling date of an event
I_s = static firing interval of a transition

Valid Time Branching Process: Example



Valid Time Branching Process: Example

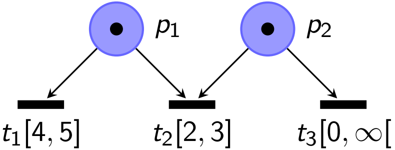




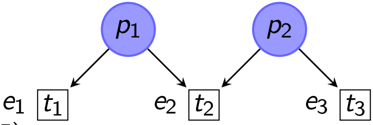
$$\begin{cases} 4 \le \theta(e_1) \le 5 \\ \text{and } \theta(e_2) = +\infty \end{cases}$$

or $(\theta(e_1) = \infty$ and $\theta(e_2) \le 5)$

Valid Time Branching Process: Example

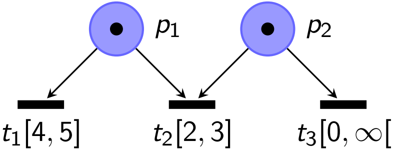


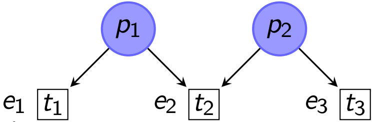
$$\left\{\begin{array}{l} 4 \leq \theta(e_1) \leq 5 \\ \text{and } \theta(e_2) = +\infty \end{array}\right.$$
$$\text{or } (\theta(e_1) = \infty \text{ and } \theta(e_2) \leq 5)$$



$$\left\{\begin{array}{l} 2 \leq \theta(e_2) \leq 3 \\ \text{and } \theta(e_1) = +\infty \\ \text{and } \theta(e_3) = +\infty \end{array}\right.$$
$$\text{or } \left\{\begin{array}{l} \theta(e_2) = +\infty \\ \text{and } (\theta(e_1) \leq 3 \text{or } \theta(e_3) \leq 3) \end{array}\right.$$

Valid Time Branching Process: Example



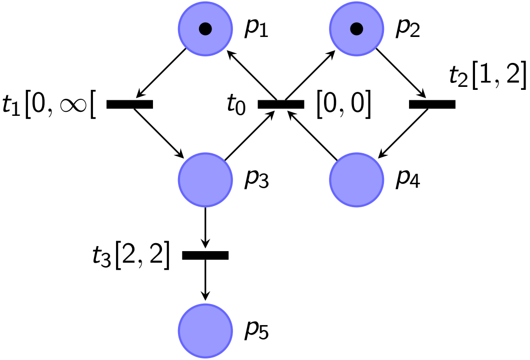


$$\left\{ \begin{array}{l} 4 \leq \theta(e_1) \leq 5 \\ \text{and } \theta(e_2) = +\infty \end{array} \right.$$
$$\text{or } (\theta(e_1) = \infty \text{ and } \theta(e_2) \leq 5)$$

$$\left\{ \begin{array}{l} 0 \leq \theta(e_3) \\ \text{and } \theta(e_2) = +\infty \end{array} \right.$$
$$\vee \theta(e_3) = +\infty$$

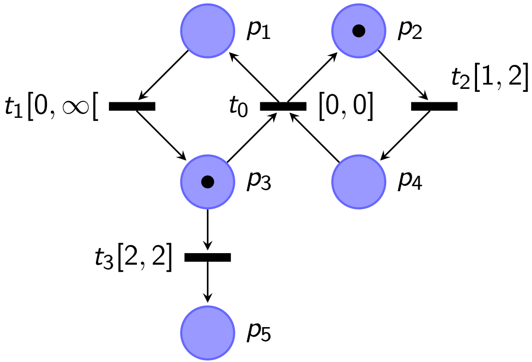
$$\left\{ \begin{array}{l} 2 \leq \theta(e_2) \leq 3 \\ \text{and } \theta(e_1) = +\infty \\ \text{and } \theta(e_3) = +\infty \end{array} \right.$$
$$\text{or } \left\{ \begin{array}{l} \theta(e_2) = +\infty \\ \text{and } (\theta(e_1) \leq 3 \text{or } \theta(e_3) \leq 3) \end{array} \right.$$

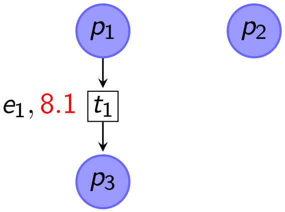
Temporally Complete Time Branching Process



The firing date of all events in the TBP should be less or equal than the latest firing date of all possible extensions.

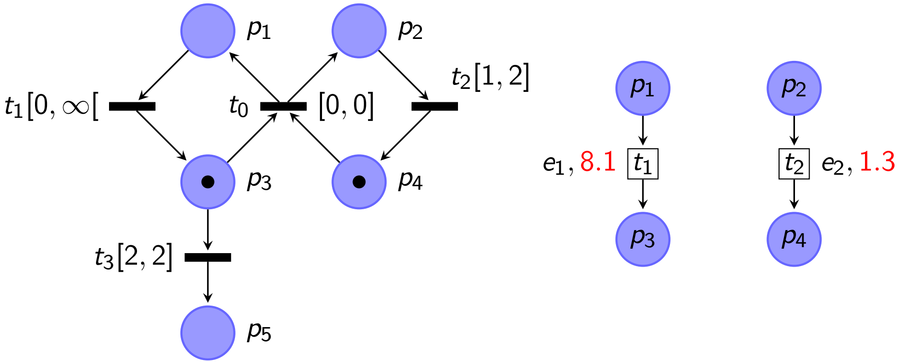
Temporally Complete Time Branching Process





The firing date of all events in the TBP should be less or equal than the latest firing date of all possible extensions.

Temporally Complete Time Branching Process



The firing date of all events in the TBP should be less or equal than the latest firing date of all possible extensions.

Soundness, Completeness

Theorem (Soundness)

For all valid time branching processes (temporally complete), its events with a finite occurrence date form a valid time process.

Theorem (Completeness)

By adding all the events in direct conflict to a valid time process, we obtain a valid time branching complete (which is temporally complete).

Finite Complete Prefix

Theorem (Finite Complete Prefix)

For any time Petri net, there exists a finite prefix of its symbolic unfolding such that: for all valid time process in the unfolding, there exists a valid time process in the prefix that has the same future behaviors.

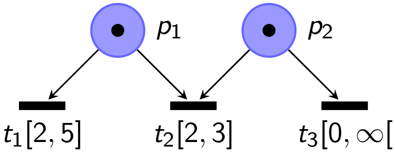
Definition (Cut-off event)

e is a cut-off event if there exists e' s.t.:

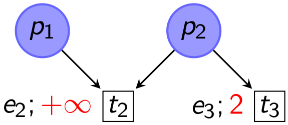
- The marking created by the causal past of e and e' is the same.
- The causal past of e' is less than that of e (adequate order);
- Equality between the (reduced) ages of the tokens in the markings of all the smallest valid processes containing the causal past of e and e' respectively.

  finite unions of zones

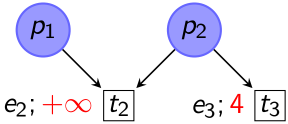
Valid Time Branching Process again



Two processes containing the causal past of e_3.

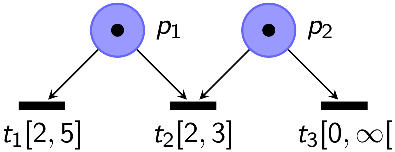


Valid

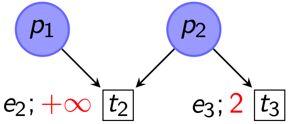


Not valid

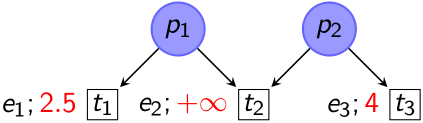
Valid Time Branching Process again



Two processes containing the causal past of e_3.

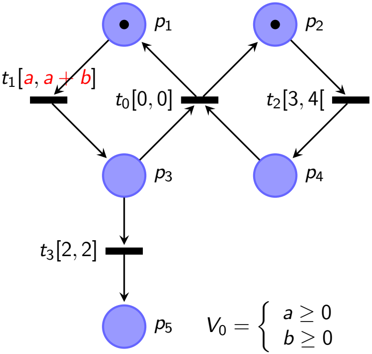


Valid

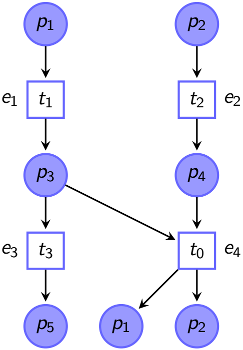


Valid

Parametric Time Petri Nets



$$V_0 = \begin{cases} a \geq 0 \\ b \geq 0 \end{cases}$$

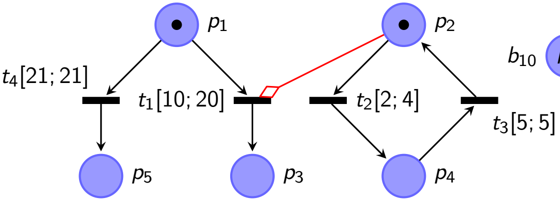


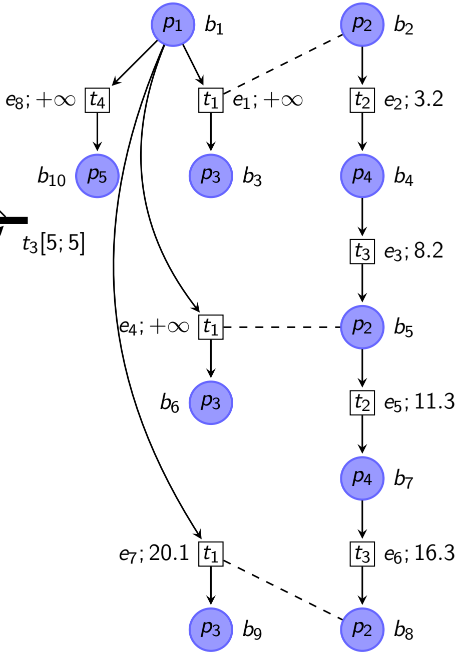
$$\begin{cases} \nu(a) \geq 1 \\ \nu(b) \geq 0 \\ \nu(a) \leq \theta(e_1) \leq \nu(a) + \nu(b) \\ 3 \leq \theta(e_2) < 4 \\ \theta(e_3) = +\infty \\ \theta(e_4) = \max\{\theta(e_1), \theta(e_2)\} \\ \theta(e_4) \leq \theta(e_1) + 2 \end{cases}$$

or

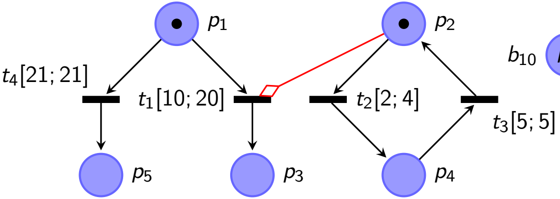
$$\begin{cases} \nu(a) \geq 0 \\ \nu(b) \geq 0 \\ \nu(a) + \nu(b) < 2 \\ \theta(e_1) \leq \nu(a) + \nu(b) \\ 3 \leq \theta(e_2) < 4 \\ \theta(e_3) = \theta(e_1) + 2 \\ \theta(e_3) \leq \max\{\theta(e_1), \theta(e_2)\} \\ \theta(e_4) = +\infty \end{cases}$$

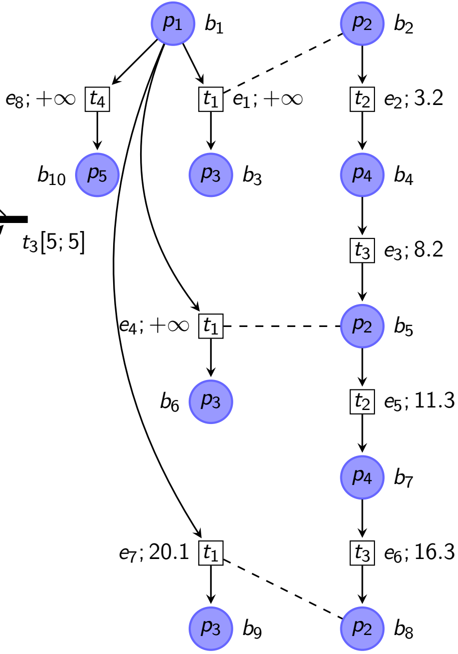
Stopwatch Petri Nets





Stopwatch Petri Nets





e_1 and e_4 correspond to "missed opportunities" of firing t_1 because it was not active for long enough:

- $\mathrm{DOA}(\{b_1\}, t_1, \theta(e_2)) = 3.2 < 10$,
- $\mathrm{DOA}(\{b_1\}, t_1, \theta(e_5)) = (11.3 - 8.2) + (3.2 - 0) = 6.3 < 10$.

DOA = sum of durations during which the transition is active

SwPNs: Valid Time Branching Processes

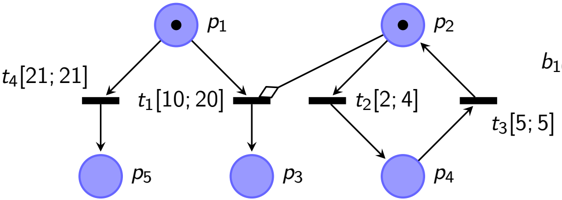
$$\forall E' \in \mathrm{RCycles}(E), \exists e' \in E' \text{ s.t. } \theta(e') = +\infty$$

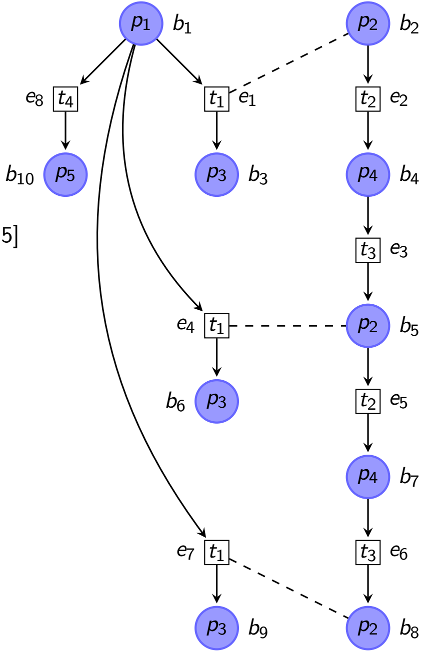
and $\forall e \in E$:

$$\Big[\big[\theta(e) \neq +\infty \text{ and } \theta(e) \geq \max_{b \in {}^\bullet e \cup {}^\circ e} \theta({}^\bullet b)$$
$$\text{and } \mathrm{DOA}({}^\star e, I(e), \theta(e)) \in v(I_s(I(e)))$$
$$\text{and } \forall e' \in E \text{ s.t. } e \,\mathrm{conf}\, e', \theta(e') = +\infty$$
$$\text{and } \forall e' \in E \text{ s.t. } e \nearrow e', \theta(e) \leq \theta(e')\big]$$
$$\text{or } \big[\theta(e) = +\infty \text{ and } \exists b \in {}^\bullet e \cup {}^\circ e, \theta({}^\bullet b) = +\infty\big]$$
$$\text{or } \big[\theta(e) = +\infty \text{ and } \exists e' \in E \text{ s.t. } (e \,\mathrm{conf}\, e' \text{ or } e \nearrow e') \text{ and } \theta(e') \neq +\infty$$
$$\text{and } \mathrm{DOA}({}^\star e, I(e), \theta(e')) \in v(I_s(I(e)))^{\downarrow}\big]\Big]$$

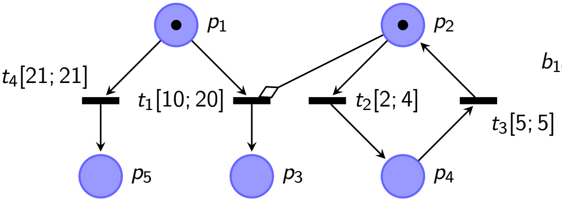
conf and $\nearrow$ are interpreted on the underlying Petri net
w/ additional read arcs for the activator arcs

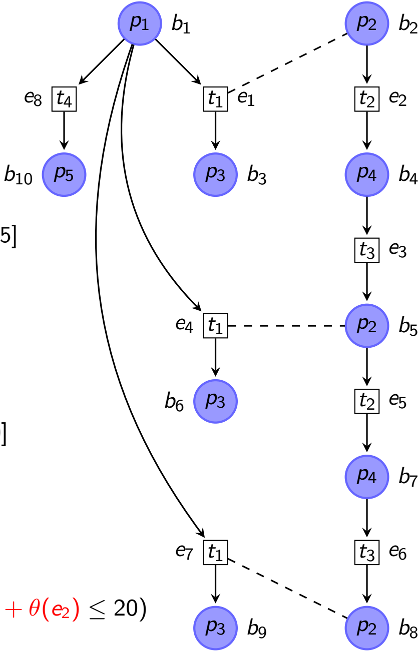
SwPNs: Valid TBPs





SwPNs: Valid TBPs





Constraints for e_4:

$$\begin{cases} \theta(e_4) \geq \theta(e_3) \\ \text{and } \theta(e_4) - \theta(e_3) + \theta(e_2) \in [10, 20] \\ \text{and } \theta(e_1) = +\infty \\ \text{and } \theta(e_8) = +\infty \\ \text{and } \theta(e_4) \leq \theta(e_5) \end{cases}$$

or

$$\begin{cases} \theta(e_4) = +\infty \\ \text{and } (\theta(e_8) - \theta(e_3) + \theta(e_2) \leq 20 \text{ or } \theta(e_5) - \theta(e_3) + \theta(e_2) \leq 20) \end{cases}$$

Conclusion

- Summary:

Conclusion

- Summary:
  - Symbolic unfoldings for time Petri nets

Conclusion

- Summary:
  - Symbolic unfoldings for time Petri nets
  - Can be extended to:
    - Read arcs;
    - Parameters;
    - Stopwatches.

Conclusion

- Summary:
  - Symbolic unfoldings for time Petri nets
  - Can be extended to:
    - Read arcs;
    - Parameters;
    - Stopwatches.
  - Existence of a finite complete prefix for TPNs with read arcs

Conclusion

- Summary:
  - Symbolic unfoldings for time Petri nets
  - Can be extended to:
    - Read arcs;
    - Parameters;
    - Stopwatches.
  - Existence of a finite complete prefix for TPNs with read arcs
- Perspectives:
  - Efficient implementation;
  - Extension to non-safe bounded models.

References

T. Aura and J. Lilius.
A causal semantics for time Petri nets.
Theoretical Computer Science, 243(2):409–447, 2000.

T. Chatain and C. Jard.
Complete finite prefixes of symbolic unfoldings of safe time Petri nets.
In *Proceedings of ICATPN*, volume 4024 of *LNCS*, pages 125–145. Springer, 2006.

K. L. McMillan.
Using unfolding to avoid the state space explosion problem in the verification of asynchronous circuits.
In *Proceedings of Computer Aided Verification (CAV'92)*, volume 663 of *LNCS*, pages 164–177. Springer, 1992.