From Continuous Petri nets to Petri nets and Back

Serge Haddad

LSV ENS Paris-Saclay & CNRS & Inria

Centre Fédéré en Vérification, Bruxelles, the 24th February 2017

(1) Laura Recalde, SH and Manuel Silva.
Continuous Petri Nets: Expressive Power and Decidability Issues. IJFCS 21(2), 2010

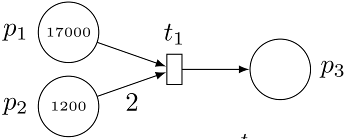
(2) Estibaliz Fraca and SH.
Complexity Analysis of Continuous Petri Nets. FI 137(1), 2015

(3) Michaël Blondin, Alain Finkel, Christoph Haase and SH.
Approaching the Coverability Problem Continuously, TACAS'16, 2016

A Production System

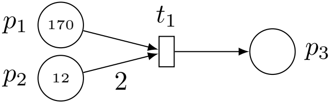
Two products can be combined to form a third one: $P_1 + 2P_2 \rightarrow P_3$

A possible Petri net modelling with 17000 P_1 and 1200 P_2 is:



$$17000p_1 + 1200p_2 \xrightarrow{t_1} 16999p_1 + 1198p_2 + p_3$$

Allowing fractional firings (here 0.01) another possible modelling is:



$$170p_1 + 12p_2 \xrightarrow{0.01t_1} 169.99p_1 + 11.98p_2 + 0.01p_3$$

The state space is no more discrete.

Fluidification

Fluidification "approximates" a discrete space system by a continuous one.

- **Optimisation.**
  - when the constraints and utility are linear;
  - one considers the integer variables (NP-complete problem) as real ones;
  - and one computes in polynomial time a bound of the optimal value.

- **Mean Field Analysis.**
  - when populations of species randomly evolve;
  - one substitutes their number by their proportion
    and introduces appropriate differential or recurrence equations;
  - whose behaviour is the asymptotic behaviour of the discrete system.

Plan

1. Continuous Petri Nets

2. Characterisation of Properties

3. Complexity of the Problems

4. Coverability in Petri Nets

5. Back to Continuous Petri Nets

Plan

1. Continuous Petri Nets
2. Characterisation of Properties
3. Complexity of the Problems
4. Coverability in Petri Nets
5. Back to Continuous Petri Nets

Continuous Petri Nets: Syntax and Semantics (1)

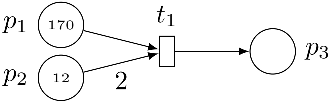
A continuous Petri net is a Petri net $\mathcal{N} = \langle P, T, \mathbf{Pre}, \mathbf{Post} \rangle$
whose markings are *real* vectors over places.

The firing rule allows a fractional firing of transitions $\boldsymbol{m} \xrightarrow{\alpha t} \boldsymbol{m}'$.

- The *enabling degree* of t w.r.t. $\boldsymbol{m}$, $enab(t, \boldsymbol{m}) \in \mathbb{R}_{\geq 0} \cup \infty$, is defined by:

$$enab(t, \boldsymbol{m}) \overset{\text{def}}{=} \min\{\frac{\boldsymbol{m}[p]}{\mathbf{Pre}[p,t]} \mid \mathbf{Pre}[p,t] > 0\}$$

- t is *enabled* in $\boldsymbol{m}$ if $enab(t, \boldsymbol{m}) > 0$.



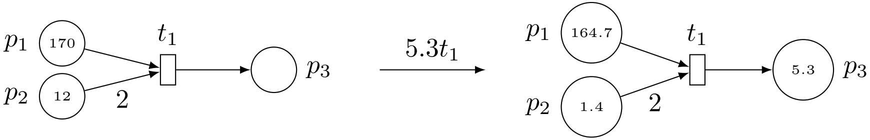
$enab(t_1, m) = 6$

Continuous Petri Nets: Syntax and Semantics (2)

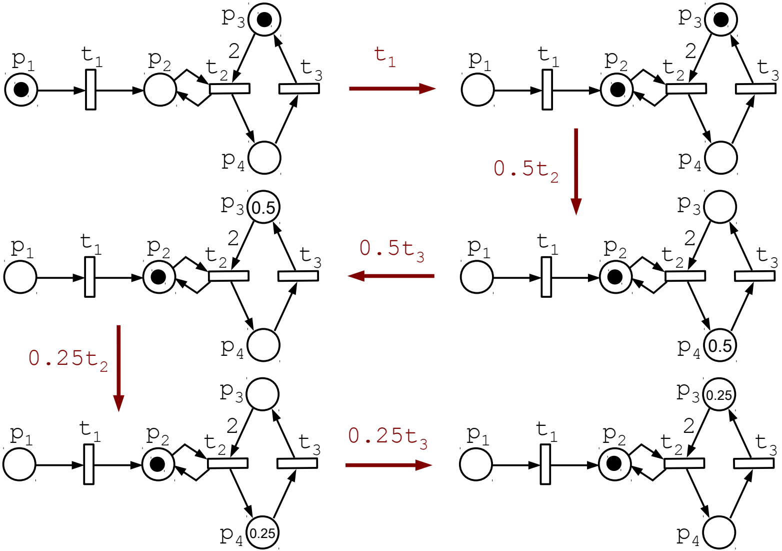
Transition t can be *fired* by any amount $\alpha \in \mathbb{R}$ such that $0 \leq \alpha \leq enab(t, \boldsymbol{m})$ and its firing leads to marking $\boldsymbol{m}'$ defined by:

$$\text{for all } p \in P \qquad \boldsymbol{m}'[p] \overset{\text{def}}{=} \boldsymbol{m}[p] + \alpha\mathbf{C}[p,t]$$

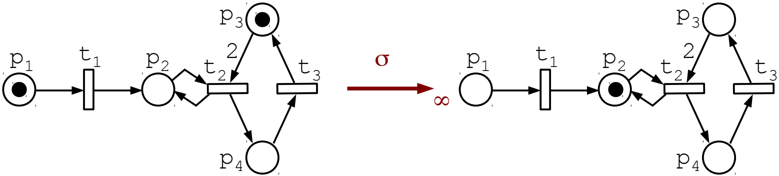
where $\mathbf{C} \overset{\text{def}}{=} \mathbf{Post} - \mathbf{Pre}$



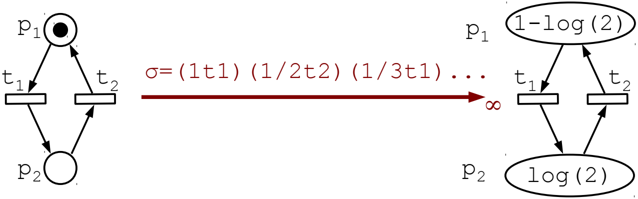
A Finite Firing Sequence



Infinite Firing Sequences



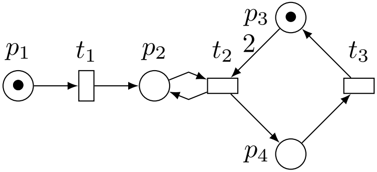
with Parikh image $\vec{\sigma} = \vec{t}_1 + \vec{t}_2 + \vec{t}_3$

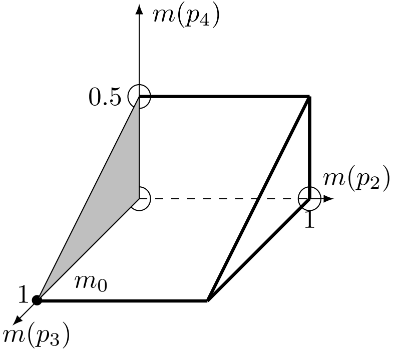


with Parikh image $\vec{\sigma} = \infty\vec{t}_1 + \infty\vec{t}_2$

Reachability Set

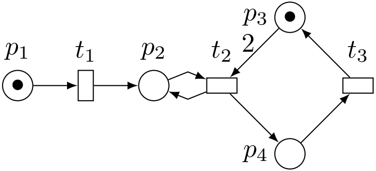
The reachability set $\mathrm{RS}(\mathcal{N}, \boldsymbol{m}_0)$ is defined by:
$\mathrm{RS}(\mathcal{N}, \boldsymbol{m}_0) \overset{\text{def}}{=} \{\boldsymbol{m} \mid \text{there exists a finite sequence } \boldsymbol{m}_0 \xrightarrow{\sigma} \boldsymbol{m}\}$.

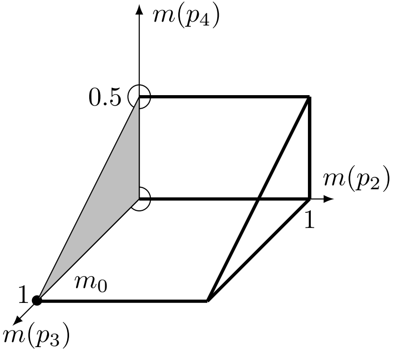




Lim-Reachability Set

The lim-reachability set, $\mathtt{lim}{-}\mathrm{RS}(\mathcal{N},\boldsymbol{m}_0)$, is defined by:
$\mathtt{lim}{-}\mathrm{RS}(\mathcal{N},\boldsymbol{m}_0) \overset{\text{def}}{=} \{\boldsymbol{m} \mid$ there exists an infinite sequence $\boldsymbol{m}_0 \xrightarrow{\sigma}_\infty \boldsymbol{m}\}$.





The lim-reachability set is not necessarily closed.

$p_1+p_3 \xrightarrow{\varepsilon t_1} (1-\varepsilon)p_1+\varepsilon p_2+p_3 \rightarrow_\infty (1-\varepsilon)p_1+\varepsilon p_2 \ldots$ but $p_1 \notin \mathtt{lim}{-}\mathrm{RS}(\mathcal{N},\boldsymbol{m}_0)$

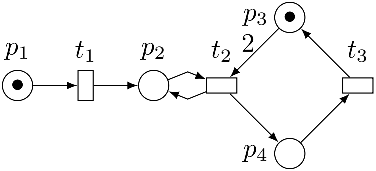
State Problems for Petri Nets

Reachability and coverability. Given a system $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$ and a marking $\boldsymbol{m}$, $\boldsymbol{m}$ is *reachable* (resp. *coverable*) in $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$ if $\boldsymbol{m} \in \mathrm{RS}(\mathcal{N}, \boldsymbol{m}_0)$ (resp. $\exists \boldsymbol{m}' \geq \boldsymbol{m}\ \boldsymbol{m}' \in \mathrm{RS}(\mathcal{N}, \boldsymbol{m}_0)$).

Boundedness. A system $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$ is *bounded* if there exists $b \in \mathbb{R}_{\geq 0}$ such that for all $\boldsymbol{m} \in \mathrm{RS}(\mathcal{N}, \boldsymbol{m}_0)$ and all $p \in P$, $\boldsymbol{m}[p] \leq b$.

Reachability set inclusion. Given systems $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$ and $\langle \mathcal{N}', \boldsymbol{m}'_0 \rangle$ with $P = P'$, $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$ is *included* in $\langle \mathcal{N}', \boldsymbol{m}'_0 \rangle$ if $\mathrm{RS}(\mathcal{N}, \boldsymbol{m}_0) \subseteq \mathrm{RS}(\mathcal{N}', \boldsymbol{m}'_0)$.

A marking $\boldsymbol{m}$ is a *home state* if $\mathrm{RS}(\mathcal{N}, \boldsymbol{m}_0) \subseteq \mathrm{RS}(\mathcal{N}^{-1}, \boldsymbol{m})$.



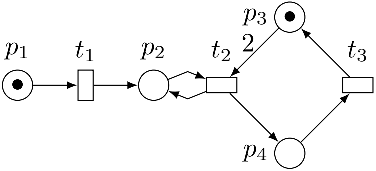
Marking $p2$ is not reachable.

This system is bounded and does not admit a home state.

Transition Problems for Petri Nets

Deadlock-freeness. A system $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$ is *deadlock-free* if for all $\boldsymbol{m} \in \mathrm{RS}(\mathcal{N}, \boldsymbol{m}_0)$, there exists $t \in T$ such that t is enabled at $\boldsymbol{m}$.

Liveness. A system $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$ is *live* if for all transition t and for all marking $\boldsymbol{m} \in \mathrm{RS}(\mathcal{N}, \boldsymbol{m}_0)$ there exists $\boldsymbol{m}' \in \mathrm{RS}(\mathcal{N}, \boldsymbol{m})$ such that t is enabled at $\boldsymbol{m}'$.



This net is deadlock-free but not live.

All properties can be considered at the limit with $\texttt{lim}-\mathrm{RS}$ instead of RS.

This net is not lim-deadlock-free and the dead marking p_2 is a lim-home state.

Plan

1. Continuous Petri Nets

2. Characterisation of Properties

3. Complexity of the Problems

4. Coverability in Petri Nets

5. Back to Continuous Petri Nets

Necessary Conditions for Reachability

Let $\boldsymbol{m}_0 \xrightarrow{\sigma} \boldsymbol{m}$ with $\sigma = \alpha_1 t_1 \ldots \alpha_k t_k$

1. State equation

$$\boldsymbol{m} - \boldsymbol{m}_0 = \mathbf{C}\vec{\sigma}$$

2. Firing set

- $[\![\overrightarrow{\sigma}]\!] \in FS(\mathcal{N}, \boldsymbol{m}_0)$
- $[\![\overrightarrow{\sigma}]\!] \in FS(\mathcal{N}^{-1}, \boldsymbol{m})$

where the *firing set* $FS(\mathcal{N}, \boldsymbol{m}_0) \subseteq 2^T$ is defined by:

$$FS(\mathcal{N}, \boldsymbol{m}_0) = \{[\![\overrightarrow{\sigma}]\!] \mid \boldsymbol{m}_0 \xrightarrow{\sigma} \}$$

Siphons and Firing Set

Some definitions

Let X a subset of transitions or places,
${}^\bullet X$ (resp. $X^\bullet, {}^\bullet X^\bullet$) is the set of predecessors (resp. successors, neighbours) of X.

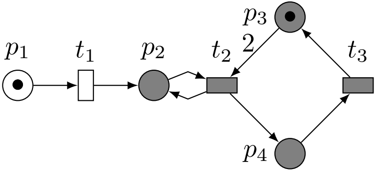
$\mathcal{N}_U$ is the net restricted to set of transitions U and set of places ${}^\bullet U^\bullet$.

A non empty subset of places Q is a siphon if ${}^\bullet Q \subseteq Q^\bullet$

A siphon is *empty* in a marking if the marking of all its places is null.

Observation

By construction, if $\mathcal{N}_U$ has an empty siphon in $\boldsymbol{m}_0$ then $U \notin FS(\mathcal{N}, \boldsymbol{m}_0)$.



p_2 is an empty siphon of $\mathcal{N}_{\{t_2,t_3\}}$

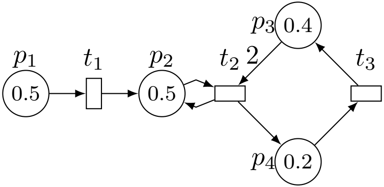
Characterisation of the Firing Set

Let $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$ be a CPN system and U be a subset of transitions. Then:

$$U \in FS(\mathcal{N}, \boldsymbol{m}_0) \text{ iff } \mathcal{N}_U \text{ has no empty siphon in } \boldsymbol{m}_0.$$

Furthermore if $U \in FS(\mathcal{N}, \boldsymbol{m}_0)$ then there exists $\sigma = \alpha_1 t_1 \ldots \alpha_k t_k$ with $U = \{t_1, \ldots, t_k\}$, $\alpha_i > 0$ for all i and a marking $\boldsymbol{m}$ such that:

- $\boldsymbol{m}_0 \xrightarrow{\sigma} \boldsymbol{m}$;
- for all place p, $\boldsymbol{m}(p) > 0$ iff $\boldsymbol{m}_0(p) > 0$ or $p \in {}^\bullet U^\bullet$.

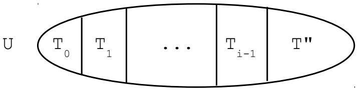


$$p_1 + p_3 \xrightarrow{0.5t_1 0.4t_2 0.2t_3} 0.5p_1 + 0.5p_2 + 0.4p_3 + 0.2p_2$$

Proof of the Characterisation (1)

Suppose that $\mathcal{N}_U$ has no empty siphon in $\boldsymbol{m}_0$.

We inductively prove for increasing values of i that there exists a partition of U (with T'' possibly empty):



$$\boldsymbol{m}_0 \xrightarrow{\sigma_0} \boldsymbol{m}_1 \ldots \boldsymbol{m}_{i-1} \xrightarrow{\sigma_{i-1}} \boldsymbol{m}_i \text{ with } [\![\overrightarrow{\sigma_j}]\!] = T_j$$

$$\boldsymbol{m}_i[p] > 0 \text{ iff } \boldsymbol{m}_0[p] > 0 \text{ or } p \in {}^\bullet(\bigcup_{j<i} T_j)^\bullet$$

There is nothing to prove for the basis case $i = 0$.

Suppose that the assertion holds until i. If $T'' = \emptyset$ then we are done.

Proof of the Characterisation (2)

- Let $T_i = \{t \text{ enabled in } \boldsymbol{m}_i \mid t \in T''\}$.

We claim that T_i is not empty.

Otherwise for all $t \in T''$, there exists an empty place p_t in $\boldsymbol{m}_i$.

Due to the inductive hypothesis, $\boldsymbol{m}_0(p_t) = 0$ and ${}^\bullet p_t \cap (\bigcup_{j<i} T_j) = \emptyset$.

So the union of places p_t is an empty siphon of $\langle \mathcal{N}_{T'}, \boldsymbol{m}_0 \rangle$

which contradicts our hypothesis.

- Let us denote $T_i = \{t_{i,1}, \ldots, t_{i,k_i}\}$.

Choose α enough small.

The sequence $\sigma_i = \alpha t_{i,1} \ldots \alpha t_{i,k_i}$ is fireable from $\boldsymbol{m}_i$

and leads to a marking $\boldsymbol{m}_{i+1}$ fulfilling the inductive hypothesis.

A Sufficient Condition for Reachability

Let $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$ be a system, $\boldsymbol{m}$ be a marking and $\mathbf{v} \in \mathbb{R}^T_{\geq 0}$ that fulfill:

- $\boldsymbol{m} = \boldsymbol{m}_0 + \mathbf{C}\mathbf{v}$;
- $\forall p \in {}^{\bullet}[\![\mathbf{v}]\!]\ \boldsymbol{m}_0[p] > 0$;
- $\forall p \in [\![\mathbf{v}]\!]^{\bullet}\ \boldsymbol{m}[p] > 0$.

Then there exists a finite sequence σ such that $\boldsymbol{m}_0 \xrightarrow{\sigma} \boldsymbol{m}$ and $\overrightarrow{\sigma} = \mathbf{v}$.

Sketch of proof.

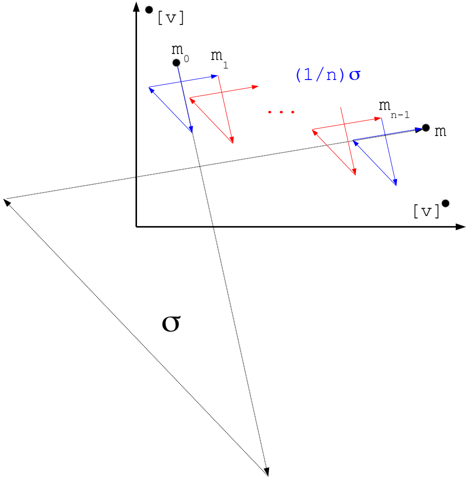
Let σ be an arbitrary sequence such that $\overrightarrow{\sigma} = \mathbf{v}$.

Let $\mathbf{m}_i = \frac{n-i}{n}\mathbf{m}_0 + \frac{i}{n}\mathbf{m}$.

Then for large n, $\mathbf{m}_0 \xrightarrow{\frac{1}{n}\sigma} \mathbf{m}_1$ and $\mathbf{m}_{n-1} \xrightarrow{\frac{1}{n}\sigma} \mathbf{m}$.

By convexity, $\mathbf{m}_0 \xrightarrow{(\frac{1}{n}\sigma)^n} \mathbf{m}$.

Illustration



Characterisation of Reachability

Let $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$ be a CPN system and $\boldsymbol{m}$ be a marking.

Then $\boldsymbol{m} \in \mathrm{RS}(\mathcal{N}, \boldsymbol{m}_0)$ iff there exists $\mathbf{v} \in \mathbb{R}^{|T|}_{\geq 0}$ such that:

1. $\boldsymbol{m} = \boldsymbol{m}_0 + \mathbf{C}\mathbf{v}$
2. $[\![\mathbf{v}]\!] \in FS(\mathcal{N}, \boldsymbol{m}_0)$
3. $[\![\mathbf{v}]\!] \in FS(\mathcal{N}^{-1}, \boldsymbol{m})$

Proof

Since $\llbracket \mathbf{v} \rrbracket \in FS(\mathcal{N}, \boldsymbol{m}_0)$, there exists a sequence σ_1 such that $\llbracket \mathbf{v} \rrbracket = \llbracket \overrightarrow{\sigma_1} \rrbracket$ and for all $0 < \alpha_1 \leq 1$, $\boldsymbol{m}_0 \xrightarrow{\alpha_1 \sigma_1} \boldsymbol{m}_1$ with $\boldsymbol{m}_1(p) > 0$ for $p \in {}^\bullet\llbracket \mathbf{v} \rrbracket^\bullet$.

Since $\llbracket \mathbf{v} \rrbracket \in FS(\mathcal{N}^{-1}, \boldsymbol{m})$, there exists a sequence σ_2 such that $\llbracket \mathbf{v} \rrbracket = \llbracket \overrightarrow{\sigma_2} \rrbracket$ and for all $0 < \alpha_2 \leq 1$, $\boldsymbol{m} \xrightarrow{\alpha_2 \sigma_2} \boldsymbol{m}_2$ in $\mathcal{N}^{-1}$ with $\boldsymbol{m}_2(p) > 0$ for $p \in {}^\bullet\llbracket \mathbf{v} \rrbracket^\bullet$.

Choose α_1 and α_2 enough small such that $\mathbf{v}' = \mathbf{v} - \alpha_1 \overrightarrow{\sigma_1} - \alpha_2 \overrightarrow{\sigma_2}$ is non negative and $\llbracket \mathbf{v}' \rrbracket = \llbracket \mathbf{v} \rrbracket$. This is possible since $\llbracket \mathbf{v} \rrbracket = \llbracket \overrightarrow{\sigma_1} \rrbracket = \llbracket \overrightarrow{\sigma_2} \rrbracket$.

Since $\boldsymbol{m}_1$ and $\boldsymbol{m}_2 = \boldsymbol{m}_1 + \mathbf{C}\mathbf{v}'$ fulfill the sufficient condition for reachability, there exists a sequence σ_3 such that $\mathbf{v}' = \overrightarrow{\sigma_3}$ and $\boldsymbol{m}_1 \xrightarrow{\sigma_3} \boldsymbol{m}_2$.

Let $\sigma \overset{\text{def}}{=} (\alpha_1 \sigma_1) \sigma_3 (\alpha_2 \sigma_2)^{-1}$ then $\boldsymbol{m}_0 \xrightarrow{\sigma} \boldsymbol{m}$.

Maximal Firing Set

Let $\boldsymbol{m}_0 \xrightarrow{\sigma_1}$ and $\boldsymbol{m}_0 \xrightarrow{\sigma_2}$

Then $0.5\boldsymbol{m}_0 \xrightarrow{0.5\sigma_1}$ and $0.5\boldsymbol{m}_0 \xrightarrow{0.5\sigma_2}$

Entailing $\boldsymbol{m}_0 \xrightarrow{0.5\sigma_1 0.5\sigma_2}$

So $FS(\mathcal{N}, \boldsymbol{m}_0)$ is closed by union.

Its maximal item is denoted $\mathtt{maxFS}(\mathcal{N}, \boldsymbol{m}_0)$.

Characterisation of Boundedness

Let $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$ be a system. Then $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$ is unbounded iff:

There exists $\mathbf{v} \in \mathbb{R}^T_{\geq 0}$ such that $\mathbf{Cv} \gneq \mathbf{0}$ and $[\![\mathbf{v}]\!] \subseteq \mathtt{maxFS}(\mathcal{N}, \boldsymbol{m}_0)$.

Proof of sufficiency.

Assume there exists $\mathbf{v} \in \mathbb{R}^T_{\geq 0}$ such that $\mathbf{Cv} \gneq \mathbf{0}$ and $[\![\mathbf{v}]\!] \subseteq \mathtt{maxFS}(\mathcal{N}, \boldsymbol{m}_0)$.

Denote $U \overset{\text{def}}{=} \mathtt{maxFS}(\mathcal{N}, \boldsymbol{m}_0)$. Using the characterisation of the firing set, there exists $\boldsymbol{m}_1 \in RS(\mathcal{N}, \boldsymbol{m}_0)$ such that for all $p \in {}^\bullet U^\bullet$, $\boldsymbol{m}_1(p) > 0$.

Define $\boldsymbol{m}_2 \overset{\text{def}}{=} \boldsymbol{m}_1 + \mathbf{Cv}$, thus $\boldsymbol{m}_2 \gneq \boldsymbol{m}_1$.
Since $[\![\mathbf{v}]\!] \subseteq U$, $\boldsymbol{m}_1$ and $\boldsymbol{m}_2$ fulfill the *sufficient* condition for reachability.

Applying it, yields a firing sequence $\boldsymbol{m}_1 \xrightarrow{\sigma} \boldsymbol{m}_2$.
Iterating this sequence establishes the unboundedness of $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$.

Proof of Necessity

- Assume there exists $p \in P$ and a family of firing sequences $\{\sigma_n\}_{n\in\mathbb{N}}$ such that $\boldsymbol{m}_0 \xrightarrow{\sigma_n} \boldsymbol{m}_n$ and $\boldsymbol{m}_n[p] > \max(n, \boldsymbol{m}_{n-1}[p])$.
W.l.o.g. we can assume that all these sequences have the same support U.

- Let $\mathbf{v}_n \overset{\text{def}}{=} \mathbf{C}\overrightarrow{\sigma}_n$ and $\mathbf{w}_n \overset{\text{def}}{=} \frac{\mathbf{v}_n}{\|\mathbf{v}_n\|_1}$.
For all $p' \in P$, $\mathbf{w}_n[p'] = \frac{\boldsymbol{m}_n[p'] - \boldsymbol{m}_0[p']}{\|\mathbf{v}_n\|_1} \geq \frac{-\boldsymbol{m}_0[p']}{\|\mathbf{v}_n\|_1}$.
$\|\mathbf{v}_n\|_1 \geq \mathbf{v}_n[p] = \boldsymbol{m}_n(p) - \boldsymbol{m}_0[p] \geq n - \boldsymbol{m}_0[p]$.
So for $n > \boldsymbol{m}_0[p]$, $\mathbf{w}_n[p'] \geq \frac{-\boldsymbol{m}_0[p']}{n - \boldsymbol{m}_0[p]}$.

- There exists a subsequence $\{\mathbf{w}_{\alpha(n)}\}_{n\in\mathbb{N}}$ converging to some $\mathbf{w} \neq \mathbf{0}$.
Applying the inequality to $\alpha(n)$ and letting n go to infinity yields $\mathbf{w} \geq \mathbf{0}$.

- Due to polyhedra theory, $\{\mathbf{C}_{P\times U}\mathbf{u} \mid \mathbf{u} \in \mathbb{R}^U_{\geq 0}\}$ is closed.
So there exists $\mathbf{u} \in \mathbb{R}^U_{\geq 0}$ such that $\mathbf{w} = \mathbf{C}_{P\times U}\mathbf{u}$.
Adding null components for $T \setminus U$ yields the required vector.

Plan

1. Continuous Petri Nets
2. Characterisation of Properties
3. Complexity of the Problems
4. Coverability in Petri Nets
5. Back to Continuous Petri Nets

Using the Characterisations

Preliminary observation. One can compute $\mathtt{maxFS}(\mathcal{N}, \boldsymbol{m}_0)$ and decide whether $U \in FS(\mathcal{N}, \boldsymbol{m}_0)$ in polynomial time.

Boundedness in PTIME. Compute $\mathtt{maxFS}(\mathcal{N}, \boldsymbol{m}_0)$ and solve a linear program.

Reachability in NP.

- Guessing a support U, one looks for $\mathbf{v}$ with support U
- such that $\boldsymbol{m} = \boldsymbol{m}_0 + \mathbf{C}\mathbf{v}$ and $U \in FS(\mathcal{N}, \boldsymbol{m}_0) \cap FS(\mathcal{N}^{-1}, \boldsymbol{m})$.

Coverability in NP. Just add "loosing" transitions.

Deadlock freeness in coNP.

- Guessing a support U and a subset of places P' such that for all t, ${}^\bullet t \cap P' \neq \emptyset$
- one looks for $\mathbf{v}$ with support U and marking m null over P'
- such that $\boldsymbol{m} = \boldsymbol{m}_0 + \mathbf{C}\mathbf{v}$ and $U \in FS(\mathcal{N}, \boldsymbol{m}_0) \cap FS(\mathcal{N}^{-1}, \boldsymbol{m})$.

Reachability set inclusion in EXPTIME. Build (and solve) an exponential number of exponentially sized linear programs representing the difference set.

Can we do better?

A PTIME Fixed Point Computation for Reachability

```
If $\boldsymbol{m} = \boldsymbol{m}_0$ then return(true,$\mathbf{0}$)
$T' \leftarrow T$ % $T'$ contains the support of all reachability sequences
While $T' \neq \emptyset$ do
    % Compute a maximal support solution in $T'$ of the state equation
    $nbsol \leftarrow 0$; $\mathbf{sol} \leftarrow \mathbf{0}$
    For $t \in T'$ do
      solve $\exists ?\mathbf{v}\ \mathbf{v} \geq \mathbf{0} \wedge \mathbf{v}[t] > 0 \wedge \boldsymbol{C}_{P\times T'}\mathbf{v} = \boldsymbol{m} - \boldsymbol{m}_0$
      If $\exists \mathbf{v}$ then $nbsol \leftarrow nbsol + 1$; $\mathbf{sol} \leftarrow \mathbf{sol} + \mathbf{v}$
    If $nbsol = 0$ then return(false) else $\mathbf{sol} \leftarrow \frac{1}{nbsol}\mathbf{sol}$ ; $T' \leftarrow [\![\mathbf{sol}]\!]$
    % Potentially restrict the support solution to fulfill the firing set conditions
    $T' \leftarrow T' \cap \mathtt{maxFS}(\mathcal{N}_{T'}, \boldsymbol{m}_0[{}^{\bullet}T'^{\bullet}])$
    $T' \leftarrow T' \cap \mathtt{maxFS}(\mathcal{N}_{T'}^{-1}, \boldsymbol{m}[{}^{\bullet}T'^{\bullet}])$
    % If the support is unchanged return the solution
    If $T' = [\![\mathbf{sol}]\!]$ then return(true,$\mathbf{sol}$)
% $\mathbf{0}$ is not a solution
Return(false)
```

Proof of Correctness

Soundness. Assume that the algorithm returns true at line 12.

By construction, $\mathbf{sol}$ fulfills the first statement of the characterisation.

Since $T' = [\![\mathbf{sol}]\!]$ at line 12,

1. $[\![\mathbf{sol}]\!] = \mathtt{maxFS}(\mathcal{N}_{T'}, \boldsymbol{m}_0[{}^\bullet T'^\bullet]) \in FS(\mathcal{N}, \boldsymbol{m}_0)$ (line 10)
2. $[\![\mathbf{sol}]\!] = \mathtt{maxFS}(\mathcal{N}^{-1}_{T'}, \boldsymbol{m}[{}^\bullet T'^\bullet]) \in FS(\mathcal{N}^{-1}, \boldsymbol{m})$ (line 11)

Thus $\boldsymbol{m}$ is reachable in $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$.

Completeness.

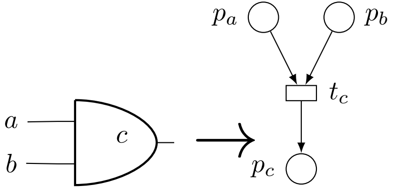
Follows from the following loop invariant: for any $\boldsymbol{m}_0 \xrightarrow{\sigma} \boldsymbol{m}$, $[\![\overrightarrow{\sigma}]\!] \subseteq T'$

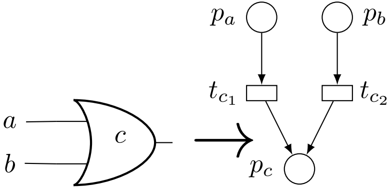
Reachability is PTIME-complete.

Reduction from the boolean circuit value problem.

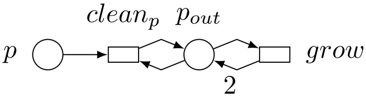
Two places $p_{\mathbf{true}}$ and $p_{\mathbf{false}}$.

One place per gate and one subnet per gate.





An additional subnet (one transition $clean_p$ per place p).

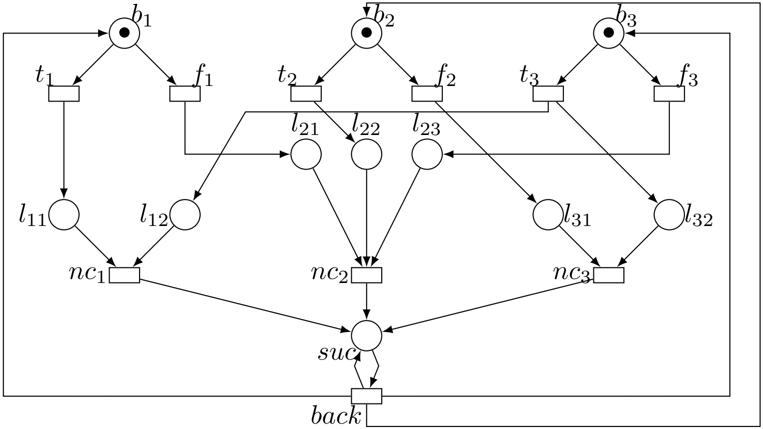


Is $1p_{out}$ reachable from $1p_{\mathbf{true}}$?

Deadlock freeness is coNP-complete.

Reduction from 3SAT.

$$\varphi = (\neg x_1 \vee \neg x_3) \wedge (x_1 \vee \neg x_2 \vee x_3) \wedge (x_2 \vee \neg x_3)$$



Proof of Correctness.

φ is satisfiable.

Fire one unit of the choice transitions according to the appropriate interpretation.

Then for all clause transition there is an empty place.

So the net is dead.

φ is unsatisfiable.

As long as it remains initial tokens the net is not dead.

Once the there are no more initial tokens, one can define an arbitrary interpretation according to the firing of choice transitions.

Since the interpretation does not satisfy φ, one clause transition is fireable.

Once suc is marked, there can be no more deadlock.

Plan

1. Continuous Petri Nets
2. Characterisation of Properties
3. Complexity of the Problems
4. Coverability in Petri Nets
5. Back to Continuous Petri Nets

Backward Algorithm: Ingredients.

Upward closed sets.

A set of markings **M** is upward closed if $\boldsymbol{m'} \geq \boldsymbol{m} \in \mathbf{M} \Rightarrow \boldsymbol{m'} \in \mathbf{M}$.

Given **M** a set of markings,
$\uparrow\mathbf{M} = \{\boldsymbol{m'} \mid \exists \boldsymbol{m} \in \mathbf{M}\ \boldsymbol{m'} \geq \boldsymbol{m}\}$ is the upward closure of $\mathbf{M}$.

Given an upward closed set **M**, $base(\mathbf{M})$ the basis of **M**
is the minimal (finite) subset of **M** such that $\mathbf{M} = \bigcup_{\boldsymbol{m} \in base(\mathbf{M})} \uparrow\{\boldsymbol{m}\}$.

Let $\{\mathbf{M}_n\}_{n\in\mathbb{N}}$ be a family of upward closed sets such that for all n, $\mathbf{M}_n \subseteq \mathbf{M}_{n+1}$ then there exists n_0 such that for all $n \geq n_0$, $\mathbf{M}_n = \mathbf{M}_{n_0}$.

Petri nets.

Let $pred(\mathbf{M})$ be the set of markings that reach $\mathbf{M}$ after a transition firing.

If $\mathbf{M}$ is upward closed then $pred(\mathbf{M})$ is upward closed.

Let $\mathbf{B}$ be the basis of $\mathbf{M}$ then one can compute $pb(\mathbf{B})$ the basis of $pred(\mathbf{M})$.

Let $\mathbf{m}$ be a marking. Define $\mathbf{M}_0 = \uparrow\{\boldsymbol{m}\}$ and $\mathbf{M}_{n+1} = \mathbf{M}_n \cup pred(\mathbf{M}_n)$.

Then $\bigcup_{n\in\mathbb{N}} \mathbf{M}_n$ is the set of markings from which one covers $\boldsymbol{m}$.

Backward Algorithm

```
$\mathbf{B} \leftarrow \{\boldsymbol{m}\}$
While $\boldsymbol{m}_0 \notin \uparrow\mathbf{B}$ do
  $\mathbf{newB} \leftarrow pb(\mathbf{B}) \setminus \uparrow\mathbf{B}$
  If $\mathbf{newB} = \emptyset$ then return false
  $\mathbf{B} \leftarrow minbase(\mathbf{B} \cup \mathbf{newB})$
return true
```

Correctness and termination follow from properties of upward closed sets.

Improved Backward Algorithm

```
If not $ContCover(\boldsymbol{m}_0, \boldsymbol{m})$ then return false

$\mathbf{B} \leftarrow \{\boldsymbol{m}\}$

While $\boldsymbol{m}_0 \notin \uparrow\mathbf{B}$ do

  $\mathbf{newB} \leftarrow pb(\mathbf{B}) \setminus \uparrow\mathbf{B}$

  $\mathbf{newB} \leftarrow \{\boldsymbol{m}' \in \mathbf{newB} \mid ContCover(\boldsymbol{m}_0, \boldsymbol{m}')\}$

  If $\mathbf{newB} = \emptyset$ then return false

  $\mathbf{B} \leftarrow minbase(\mathbf{B} \cup \mathbf{newB})$

return true
```

Related Work

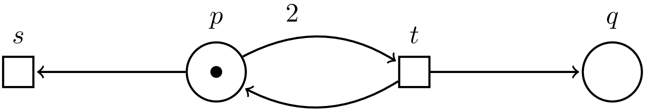
Another necessary condition for reachability in Petri nets.

A *trap* is a non empty set of places Q such that ${}^{\bullet}Q \subseteq Q^{\bullet}$.

- $\exists \mathbf{v}\ \boldsymbol{m} = \boldsymbol{m}_0 + \mathbf{C}\mathbf{v}$;
- For all trap Q marked in $\boldsymbol{m}_0$, Q is marked in $\boldsymbol{m}$.

(An SMT-Based Approach to Coverability Analysis. Esparza & al. CAV 2014)

$\mathbb{Q}$-reachability strictly implies this condition.



Marking $\boldsymbol{m} = 1q$ is not reachable in this CPN.

However $\boldsymbol{m} = \boldsymbol{m}_0 + \mathbf{C}\mathbf{1}_t$ and the single trap q is unmarked in $\boldsymbol{m}_0$.

A Logical Approach to Reachability in Continuous PN

Observation

- While reachability is checkable in PTIME in continuous Petri nets,
- an efficient alternative consists to express the characterisation in a logical way
- and provide an *existential* formula to a SMT solver ...
- ... since repeated calls to a solver are optimised.

The state equation can be directly provided as an input to the solver.

How to express the firing set constraints to a solver?

A Logical Formula for a Firing Set

Input variables

- For all $p \in P$, $x(p)$ is the initial marking;
- For all $t \in T$, $y(t)$ is the t-component of the Parikh image of the sequence.

Auxiliary variables

- For all $p \in P$, $z(p)$, when non null, is the first instant p is marked;
- For all $t \in T$, $z(t)$, when non null, is the firing instant of t.

Auxiliary formulas

- $\varphi_{\mathcal{N},1} = \bigwedge_{t \in T} \left(y(t) > 0 \Rightarrow \bigwedge_{p \in {}^\bullet t} 0 < z(p) \leq z(t) \right)$
- $\varphi_{\mathcal{N},2} = \bigwedge_{p \in P} \left(z(p) > 0 \Rightarrow \left(x(p) > 0 \vee \bigvee_{t \in {}^\bullet p} y(t) > 0 \wedge 0 < z(t) < z(p) \right) \right)$

$\varphi_{\mathcal{N}} = \exists \mathbf{z}\, \varphi_{\mathcal{N},1} \wedge \varphi_{\mathcal{N},2}$ $\qquad \varphi_{\mathcal{N},\boldsymbol{m}_0}[\mathbf{w},\mathbf{y}] = \mathbf{w} - \boldsymbol{m}_0 = \mathbf{C}\mathbf{y} \wedge \varphi_{\mathcal{N}}[\boldsymbol{m}_0/\mathbf{x}] \wedge \varphi_{\mathcal{N}^{-1}}[\mathbf{w}/\mathbf{x}]$

The size of $\psi_{\mathcal{N},\boldsymbol{m}_0}[\mathbf{w}] = \exists \mathbf{y}\ \varphi_{\mathcal{N},\boldsymbol{m}_0}$ is linear w.r.t. the size of $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$.

Plan

1. Continuous Petri Nets
2. Characterisation of Properties
3. Complexity of the Problems
4. Coverability in Petri Nets
5. Back to Continuous Petri Nets

Reachability Set Inclusion belongs to Π_2^{P}

Let $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$ and $\langle \mathcal{N}', \boldsymbol{m}'_0 \rangle$ be two continuous Petri nets.

The formula below expresses the reachability set inclusion:

$$\forall \mathbf{w}\ \neg\psi_{\mathcal{N},\boldsymbol{m}_0} \vee \psi_{\mathcal{N}',\boldsymbol{m}'_0}$$

This formula can be written as $\forall \ldots \exists \ldots \theta$
where θ is a quantifier-free formula of FO$(\mathbb{Q}, +, <)$.

So the complexity of the reachability set inclusion belongs to Π_2^{P}.
(Eduardo D. Sontag. Real Addition and the Polynomial Hierarchy. 1985.)

Can we do better?

Reachability Set Inclusion belongs to coNP

Polyhedra theory.

- Let $\varphi[\mathbf{x}] = \exists \mathbf{y} \theta[\mathbf{x}, \mathbf{y}]$ where θ is a quantifier-free formula of FO$(\mathbb{Q}, +, <)$.

Then there exists a quantifier free-formula $\psi[\mathbf{x}]$
whose size is polynomial w.r.t. size of φ such that $\forall \mathbf{x}\ \varphi \Leftrightarrow \psi$.

- Assume $\exists \mathbf{x}\ \psi$ is true.

Then there exists a witness $\mathbf{v}$ whose size is polynomial w.r.t. size of ψ
such that $\psi[\mathbf{v}/\mathbf{x}]$ is true.

Application to reachability set inclusion.

$\forall \mathbf{w}\ \forall \mathbf{y}\ \exists \mathbf{y}'\ \neg\varphi_{\mathcal{N},\boldsymbol{m}_0} \vee \varphi_{\mathcal{N}',\boldsymbol{m}'_0}[\mathbf{y}'/\mathbf{y}]$
express the reachability set inclusion.

This formula is equivalent to some $\forall \mathbf{w}\ \forall \mathbf{y}\ \theta$ where θ is quantifier-free,
and when false admits a polynomially sized witness.

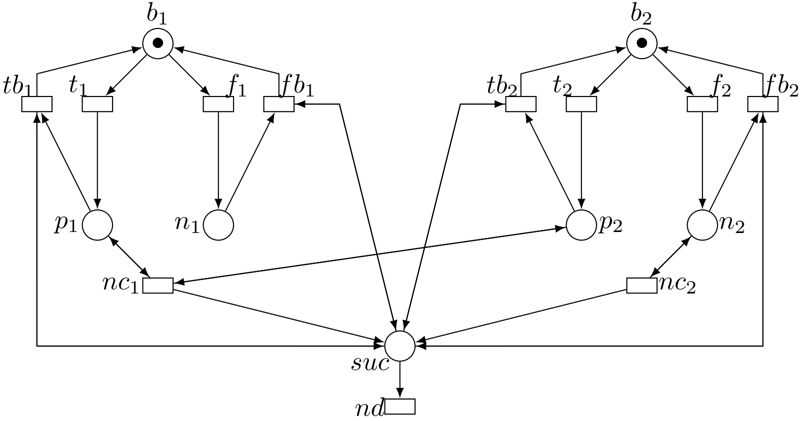
So one guesses a polynomially sized marking $\boldsymbol{m}$
and checks whether $\boldsymbol{m}$ is reachable in $\langle \mathcal{N}, \boldsymbol{m}_0 \rangle$ and unreachable in $\langle \mathcal{N}', \boldsymbol{m}'_0 \rangle$.

Reachability Set Inclusion is coNP-complete

A net is *reversible* if the initial marking is a home state.

Reduction from 3SAT to reversibility.

$$\varphi = (\neg x_1 \vee \neg x_2) \wedge x_2$$



Summary of the Results

A full characterisation for problems complexity.

Problems	**Complexity**
(lim-)reachability	PTIME-complete
(lim-)boundedness	PTIME-complete
(lim-)deadlock-freeness and (lim-)liveness	coNP-complete
(lim-)reachability set inclusion	coNP-complete

A relevant improvement for Petri nets coverability.

Perspectives

Temporal logic

- In Petri nets, model checking is at the border of decidability/undecidability depending on: branching versus linear, propositional versus evenemential;
- Goal: in CPNs, investigation of decidability and complexity issues.

Hybrid Petri nets

- Combination of Petri nets and continuous Petri nets
- Goal: establishing the border decidability/undecidability of standard problems for this formalism.