UNIVERSITÉ LIBRE DE BRUXELLES
Faculté des Sciences
Département d'Informatique

The Coverability problem for parametric Petri nets

Alexis Reynouard

Promotor : Prof. Gilles Geeraerts

Master Thesis in Computer Sciences

Academic year 2018 - 2019

Contents

Chapter 1

Introduction

Petri nets (PNs) are a mathematical and graphical model introduced by Carl Adam Petri in 1962 [7]. It was successfully used to analyse systems in a wide range of domains, especially for the formal verification of asynchronous systems.

In their standard definition, PNs are instantiated through many natural numbers which may represent, for example, the amount of resource needed for a given action to be carried out.

The introduction of parameters into the model to avoid the need to state these values explicitly[1] may have several benefits: it may allow to perform analysis of a whole family of PNs in an efficient way, like in [1]; or to model dynamic changes in the system, as introduced by [2] as a subclass of reconfigurable nets.

The use of parameters increases the modelling power of PNs but also make some basic coverability problems undecidable in the general case [4].

We adopt the parametric Petri net model introduced by [4], which seems the most general, and study the existing results and algorithms for conventional Petri nets to determine if they still hold or how to adapt them to the parametric model.

The rest of the document is as follows: We define the classical Petri net model and the parametric model. We then briefly motivate our study and give concrete examples of applications. Third, we recall, first, the results already obtained for the parameterized Petri net as we have defined them, second, the classical results that we will study on this new model.

1.1 Definitions

Definition 1 (Petri net)**.** A Petri net (PN) $\mathcal{N}$ is a weighted oriented bipartite graph, whose the two subsets of vertices define a tuple $\langle P, T\rangle$ where:

- P is a finite set of places,
- T is a finite set of transitions.

[1] One can find in the literature many other way to use parameters in PNs. For example, place and / or transitions may also be parameters in order to dynamically change the network structure, like in [3].

For each transition $t \in T$ are defined (exactly) these two functions:

- $I_t : P \mapsto \mathbb{N}$ associates to each place the weight of the edge to t *(input weight)*,
- $O_t : P \mapsto \mathbb{N}$ associates to each place the weight of the edge from t *(output weight)*.

It is denoted by $t = \langle I_t, O_t \rangle$. Because these functions define the edges of the graph, a PN is completely defined by the tuple $\langle P, T \rangle$ and so is denoted by $\mathcal{N} = \langle P, T \rangle$.

Definition 2 (marking)**.** Given a set of place P, a marking over P is a function $\mathbf{m} : P \mapsto \mathbb{N}$ that associates $\mathbf{m}(p)$ tokens to each place $p \in P$.

An order on the markings is essential for the analysis of Petri nets. The order we will define is a well quasi order and a partial order.

Definition 3 (quasi order)**.** A quasi order on a set $\mathcal{E}$ is a binary relation R that is:

$$\begin{aligned} &\text{reflexive:} && \forall x \in \mathcal{E},\ x\ R\ x \\ &\text{transitive:} && \forall (x, y, z) \in \mathcal{E}^3,\ (x\ R\ y \wedge y\ R\ z) \Rightarrow x\ R\ z \end{aligned}$$

Definition 4 (well quasi order)**.** A well quasi order $\sqsubseteq$ on a set $\mathcal{E}$ is a quasi order on $\mathcal{E}$ such that, for any infinite sequence $s = e_0, e_1, e_2, \ldots$ of elements from $\mathcal{E}$, there exist indices $i < j$ with $e_i \sqsubseteq e_j$. That is, there is no infinite antichain in $\mathcal{E}$ for this relation.

Definition 5 (partial order)**.** A partial order on a set $\mathcal{E}$ is a quasi order R that is

$$\text{antisymmetric:} \qquad \forall (x, y) \in \mathcal{E}^2,\ (x\ R\ y \wedge y\ R\ x) \Rightarrow x = z$$

Definition 6 (partial order $\preccurlyeq$ on the markings)**.** Given a set of places P, the partial order $\preccurlyeq \subseteq \mathbb{N}^{|P|} \times \mathbb{N}^{|P|}$ is such that for all pair of markings $(\mathbf{m}_1, \mathbf{m}_2) \in \mathbb{N}^{|P|} \times \mathbb{N}^{|P|}$ we have that $\mathbf{m}_1 \preccurlyeq \mathbf{m}_2$ if and only if for all place $p \in P : \mathbf{m}_1(p) \leq \mathbf{m}_2(p)$.

In this work we will focus on an extension of PNs with parameters as input and output weights.

Definition 7 (parametric Petri net)**.** A parametric Petri net (PPN) $\mathcal{S} = \langle P, T, \mathbb{P} \rangle$ is a weighted oriented bipartite graph with a finite set $\mathbb{P}$ of parameters. The two subsets of vertices are:

- P: a finite set of places,
- T: a finite set of transitions,

For each transition $t \in T$ are defined the following functions:

- $I_t : P \mapsto \mathbb{N} \cup \mathbb{P}$ associates to each place the weight of the edge to t *(input weight)*,
- $O_t : P \mapsto \mathbb{N} \cup \mathbb{P}$ associates to each place the weight of the edge from t *(output weight)*.

Definition 8 (parametric marking)**.** Given a set of place P, a parametric marking over P is a function $\mathbf{m} : P \mapsto \mathbb{N} \cup \mathbb{P}$ that associates $\mathbf{m}(p)$ tokens to each place $p \in P$.

A marking of a PN $\mathcal{N} = \langle P, T \rangle$ is a marking over P. A marking of a PPN $\mathcal{S} = \langle P, T, \mathbb{P} \rangle$ is a *parametric* marking over P. Note that a marking $\mathbf{m}$ is a parametric marking where $\mathbf{m}(p) \in \mathbb{N}$ for all $p \in P$.

Definition 9 (initialized (parametric) Petri net)**.** An initialized PN $\mathcal{N} = \langle P, T, \mathbf{m}_0 \rangle$ (resp. PPN $\mathcal{S} = \langle P, T, \mathbb{P}, \mathbf{m}_0 \rangle$) is a PN (resp. PPN) with an initial marking $\mathbf{m}_0$.

This is sometimes called a *marked (parametric) Petri net*. We will often refer to an initialized (parametric) Petri net loosely as a (parametric) Petri net.

The figure 1.1 shows an example of PPN with an initial marking $\mathbf{m}_0$ such that $\mathbf{m}_0(p_1) = 0$, $\mathbf{m}_0(p_2) = a$ and $\mathbf{m}_0(p_3) = 0$. The circles represent the places, the rectangles are the transitions and the dots are the tokens. An arrow from a place p and to a transition t denotes that $I_t(p) = 1$. If there is no arrow from p to t, $I_t(p) = 0$. If $I_t(p) \notin \{0, 1\}$, a label with the value of $I_t(p)$ is added to the arrow. Symmetrically, the arrows from the transitions to the places indicate the output weights.

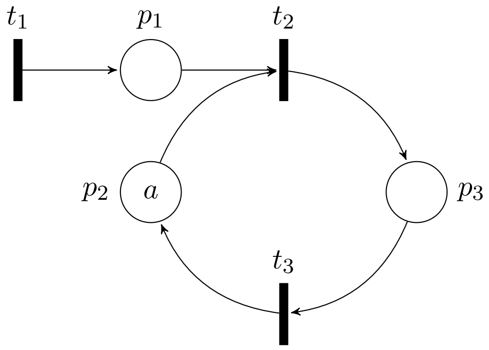

Figure 1.1: An initialized PPN

We usually set an order on the places. This allows to view the markings as vectors (here, $\mathbf{m}_0$ is the column vector $(0, a, 0)^T$, where $\cdot^T$ is the transpose operator) as well as the I and O functions. Likewise, we define an order on the transitions. Therefore, I_t and O_t denote respectively the I and O functions defined for the t^{th} transition (here, $I_1 = (0, 0, 0)^T$ and $O_1 = (1, 0, 0)^T$). Given a PPN $\mathcal{S} = \langle P, T, \mathbb{P} \rangle$, the backward and forward incidence matrices $\mathbf{I}_\mathcal{S} \in (\mathbb{N} \cup \mathbb{P})^{|P| \times |T|}$ and $\mathbf{O}_\mathcal{S} \in (\mathbb{N} \cup \mathbb{P})^{|P| \times |T|}$ are naturally defined by $\mathbf{I}_\mathcal{S}(p, t) = I_t(p)$ and $\mathbf{O}_\mathcal{S}(p, t) = O_t(p)$. ($\mathcal{S}$ is omitted when it is obvious from the context.) This allows to use linear algebra to analyse PNs.

$$\mathbf{I} = \begin{array}{c|ccc} & t_1 & t_2 & t_3 \\ \hline p_1 & 0 & 1 & 0 \\ p_2 & 0 & 1 & 0 \\ p_3 & 0 & 0 & 1 \end{array} \qquad \mathbf{O} = \begin{array}{c|ccc} & t_1 & t_2 & t_3 \\ \hline p_1 & 1 & 0 & 0 \\ p_2 & 0 & 0 & 1 \\ p_3 & 0 & 1 & 0 \end{array}$$

Figure 1.2: The incidence matrices of the PN from figure 1.1

1.1.1 Operational semantic of Petri nets

Given a PN $\mathcal{N} = \langle P, T \rangle$ and a marking $\mathbf{m}$ on $\mathcal{N}$, a transition $t \in T$ is said *enabled* by $\mathbf{m}$ if $\forall p \in P : \mathbf{m}(p) \geq I_t(p)$. An enabled transition can be *fired* to produce a new marking $\mathbf{m}'$ such that $\forall p \in P : \mathbf{m}'(p) = \mathbf{m}(p) - I_t(p) + O_t(p)$. This is denoted by $\mathbf{m} \xrightarrow{t} \mathbf{m}'$. It is important to note that the effect of a transition is to add or remove a constant number of tokens at each place and does not depend on the marking from which it is fired. A PN transition is said to have a *constant effect.* [TODO: Note difference when talking about ω-Petri nets]

Here are some additional notations:

- $\mathbf{m} \rightarrow \mathbf{m}'$ denotes that there exists $t \in T$ such that $\mathbf{m} \xrightarrow{t} \mathbf{m}'$.
- $\mathbf{m} \xrightarrow{\sigma} \mathbf{m}'$ where σ is a sequence of transitions $\sigma = (t_1, \dots, t_{n-1}), t_i \in T, i \in \{1, \dots, n-1\}$ denotes that there exists a sequence of markings $\mathbf{m}_1, \dots, \mathbf{m}_n$ such that : $\mathbf{m} = \mathbf{m}_1 \xrightarrow{t_1} \cdots \xrightarrow{t_{n-1}} \mathbf{m}_n = \mathbf{m}'$.
- $\mathbf{m} \xrightarrow{*} \mathbf{m}'$ denotes that there exists a sequence of transition σ such that $\mathbf{m} \xrightarrow{\sigma} \mathbf{m}'$.

All of this applies to PPN through valuations of the parameters:

Definition 10 (Instantiation of parametric Petri nets)**.** Let $\mathcal{S} = \langle P, T, \mathbb{P}, \mathbf{m}_0 \rangle$ be a PPN and $v : \mathbb{P} \mapsto \mathbb{N}$ be a *valuation* on $\mathbb{P}$. Then $v(\mathcal{S})$ is defined as the PN obtained by replacing each parameter $a \in \mathbb{P}$ by $v(a)$. Thus, we have $v(\mathcal{S}) = \langle P, T, \mathbf{m}'_0 \rangle$ such that :

- $\mathbf{I}_{v(\mathcal{S})}(p,t) = \begin{cases} \mathbf{I}_{\mathcal{S}}(p,t) & \text{if } \mathbf{I}_{\mathcal{S}}(p,t) \in \mathbb{N} \\ v(\mathbf{I}_{\mathcal{S}}(p,t)) & \text{if } \mathbf{I}_{\mathcal{S}}(p,t) \in \mathbb{P} \end{cases}$
- $\mathbf{O}_{v(\mathcal{S})}(p,t) = \begin{cases} \mathbf{O}_{\mathcal{S}}(p,t) & \text{if } \mathbf{O}_{\mathcal{S}}(p,t) \in \mathbb{N} \\ v(\mathbf{O}_{\mathcal{S}}(p,t)) & \text{if } \mathbf{O}_{\mathcal{S}}(p,t) \in \mathbb{P} \end{cases}$
- $\mathbf{m}'_0(p) = \begin{cases} \mathbf{m}_0(p) & \text{if } \mathbf{m}_0(p) \in \mathbb{N} \\ v(\mathbf{m}_0(p)) & \text{if } \mathbf{m}_0(p) \in \mathbb{P} \end{cases}$

Given PPN $\mathcal{S}$ and a valuation v, one can thus instantiate a PN $v(\mathcal{S})$ from $\mathcal{S}$ and apply the semantic described above. When the PPN under consideration is clear from the context, $\mathbf{I}_v$ is used to denote $\mathbf{I}_{v(\mathcal{S})}$ and $\mathbf{O}_v$ to denote $\mathbf{O}_{v(\mathcal{S})}$. We write $\mathbf{m} \xrightarrow{t}_v \mathbf{m}'$, $\mathbf{m} \rightarrow_v \mathbf{m}'$, $\mathbf{m} \xrightarrow{\sigma}_v \mathbf{m}'$ and $\mathbf{m} \xrightarrow{*}_v \mathbf{m}'$ to denote $\xrightarrow{t}$, $\rightarrow$, $\xrightarrow{\sigma}$ and $\xrightarrow{*}$ on the classic PN $v(\mathcal{S})$.

This make it possible to formally represent a system and interactions between its components. We will now define some properties that the model may have and that are usually of interest to show that the modelled system meets some requirement.

1.1.2 Behavioural properties of Petri nets

The markings basically indicate the state of the system. Thus, knowing if an initialized PN may reach a given marking, that represents for example a bad state, is essential to check properties of the modelled system. This is the *reachability problem.*

Definition 11 (Reachability)**.** Given an initialized PN $\mathcal{N} = \langle P, T, \mathbf{m}_0 \rangle$ and a marking $\mathbf{m}$ of $\mathcal{N}$, $\mathbf{m}$ is said reachable if $\mathbf{m}_0 \xrightarrow{*} \mathbf{m}$.

However safety properties are more often analysed through the *coverability problem*, that is essentially asking if a PN can reach or exceed a given marking.

Definition 12 (Coverability)**.** Given an initialized PN $\mathcal{N} = \langle P, T, \mathbf{m}_0 \rangle$ and a marking $\mathbf{m}$ of $\mathcal{N}$, $\mathbf{m}$ is said coverable if there exists a marking $\mathbf{m}'$ such that $\mathbf{m} \preccurlyeq \mathbf{m}'$ and $\mathbf{m}_0 \xrightarrow{*} \mathbf{m}'$.

The behaviour of a PPN is defined by the behaviours of all the PNs that can be obtained by a valuation of its parameters. So, for an initialized PPN $\mathcal{S}$, the coverability problem may be declined in an existential and an universal form. The existential coverability problem ($\mathscr{E}$-cov) ask if there exists a valuation v such that $\mathbf{m}$ is coverable. The universal coverability problem ($\mathscr{U}$-cov) ask if $\mathbf{m}$ is coverable for all valuations v.

Definition 13 (Universal and existential coverability problems)**.** Given a PPN $\mathcal{S} = \langle P, T, \mathbb{P} \rangle$ and a marking $\mathbf{m}$ of $\mathcal{S}$

- the *existential coverability problem* ask if there is a valuation v for $\mathbb{P}$ such that $\mathbf{m}$ is coverable,
- the *universal coverability problem* ask if $\mathbf{m}$ is coverable for all valuations of $\mathbb{P}$.

1.2 Motivations

[TODO: motivations: What should we write here? Are the two subtitles below a possible approach? And here or put it before?]

1.2.1 Interests of PPNs

1.2.2 Interest of the coverability problem in PPNs

1.3 Previous work

The use of parameters in formal verification systems is a well developed topic in the literature.

With regard to PN, parameters have been introduced with many different roles. Some works, like [3] use parameters as places or transitions, for example to make it possible to change a place into a more complex subnet and thus allow different levels of abstractions to be considered. In [6], parameters are used on the markings to obtain concise parametrised reachability trees, but not to realize formal verifications on these parametric systems.

[2] introduce parameters as the weight of arcs to model changes in a system. The parameters have a finite valuation domain and verifications are performed on these parametrized systems. Systems with quantitative parameters with infinite valuation domains are analysed in [1].

Our work is in the line with [4] which use discrete parameters as arc weights and in the markings. [4] provide also a proof for the non decidability of $\mathscr{U}$-cov and $\mathscr{E}$-cov, and define several subclasses of PPN for which these problems are decidable.

Other similar approaches are the PNs with parametric initial markings, like in [[TODO: Modeling with Generalized Stochastic Petri Nets, Marsan 94, On parametric P/T nets and their modelling power, Chiola 91]].

[TODO: ω-markings [5]]

1.4 Objectives (should become Contributions)

[TODO: objectives]

Conclusions

The conclusions are to be written with care, because it will be sometimes the part that could convince a potential reader to read the whole document.

Bibliography

[1] Parosh Abdulla, Frédéric Haziza, and Lukáš Holík. All for the price of few: (parameterized verification through view abstraction). volume 7737, pages 476–495, 2013.

[2] Eric Badouel and Javier Oliver. Dynamic changes in concurrent systems: Modelling and verification. 1999.

[3] Søren Christensen and Kjeld Høyer Mortensen. Parametrisation of coloured petri nets. *DAIMI Report Series*, 26(521), March 1997.

[4] Nicolas David. *Discrete Parameters in Petri Nets*. PhD thesis, Université de Nantes, Augustus 2017.

[5] Gilles Geeraerts, Alexander Heussner, M Praveen, and Jean-François Raskin. ω-petri nets: Algorithms and complexity. 137:29–60, 01 2015.

[6] M. Lindqvist. *Parametrized Reachability Trees for Predicate / Transition Nets*, pages 351–372. Springer Berlin Heidelberg, Berlin, Heidelberg, 1991.

[7] Carl Adam Petri. *Kommunikation mit Automaten*. PhD thesis, Universität Hamburg, 1962.