# Non-Reachability in Priority Duration Petrinets

Matthias Werner
Communication and Operating Systems Group
Department for Electrical Engineering and Computer Science
TU Berlin
mwerner@cs.tu-berlin.de

Louchka Popova-Zeugmann
Automata and System Theory Group
Department of Computer Science
Humboldt University
popova@informatik.hu-berlin.de

Jan Richling
Computer Architecture and Communication Group
Department of Computer Science
Humboldt University
richling@informatik.hu-berlin.de

June 26, 2003

**Abstract**

Times and priorities are important concepts that are frequently used to model real-world systems. Thus, there exist extensions for Petrinets which allow to model times and priorities. In contrast, many proving techniques are based on classical (time-less and priority-less) Petrinets. However, this approach fails frequently for timed and prioritized Petrinets.

In this paper, we present an approach to prove non-reachability in a Priority Duration Petrinet. We use for this proofing technique a state equation as well as conditions for firing that include a priority rule and a maximal step rule. Our approach leads to a system of equations and in-equations, which provide us with a sufficient condition of non-reachability. We demonstrate the application of our approach with an example.

# 1 Introduction

## 1.1 Motivation

Times and priorities are important concepts which are frequently used in real-world systems. Such systems can be build with the *Message Scheduled System*

(MSS) architecture [7] that we have developed. MSS supports composability of real-time systems. It ensures that every component meets its contracted specification on its real-time behavior. The MSS architecture relies on standard priority-based scheduling methods, e.g., [1]. In order to prove the formal correctness of the MSS architecture we need a way to deal with priorites and times.

The correctness of an MSS system can be mapped to the non-reachability of certain states. In [6] and [5] we presented a formal specification of MSS' behavior based on prioritized Duration Petrinets (DPN), and a tool-supported way to generate the specification for a desired system instance, respectively. In [3], we showed how a non-reachability proof can be conducted in a DPN. As the next step, we present in this paper the extension of our method to systems with priorities.

Frequently, non-reachability proofs in extended Petrinets are done by proving the non-reachability in the underlying classic Petrinet. However, this approach fails in cases like MSS where the system's correctness relies on the restriction introduced by time and priorities.

In this paper we present an approach that allows to prove non-reachability in the actual Priority Duration Petrinet (PDPN). For that purpose, we give a state equation and a number of firing conditions that lead to a system of equations and inequations. This system provides a sufficient condition to prove non-reachability.

The remainder of this paper is organized as follows: The rest of this section names the state of art. Section 2 provides the needed definitions. In Section 3, we derive from the definitions a state equation, priority conditions and conditions for maximal steps that support an algebraic reasoning about PDPN. We show in Section 4 how to apply our methods and prove a non-reachability in a example net. Finally, the paper concludes with some final remarks.

## 1.2 Related Work

The question of reachability and non-reachability raises for several problems which can be described by Petrinets. In general, the state space of a Petrinet is infinite. Different methods have been developed in order to prove certain properties without computing resp. knowing the whole state space of the net.

One approache in classical Petrinetse is the computing of invariants. There, it is relatively easy to obtain place or transition invariants using the state equation of the net (cf. [8]).

But, when the Petrinet is a time dependent one or uses priorities, the state space becomes smaller. In this case, the use of the state equation of the skeleton is not very reasonable, because this state equation does not take into account the additional constrains of the net.

There exist quite a range of possibilities to represent times in Petrinets. Times can be assigned to transitions, places and tokens (cf. [9]); for each case exist several semantics. In this work we consider an extension to Duration Petrinets (also called Timed Petrinets). Duration Petrinet were defined by

Ramchandani [4]. Here, times are assigned to transitions and describe a delay in the process of firing.

Also, priorities are an often used concept in Petrinets. Usually, priorities will be assigned to transitions or to tokens. We use the first alternative.

There exist approaches to analytically deal with time and priorities in stochastic Petrinets, cf. e.g., [2]. The reachability graph of stochastic Perinet is the same as the graph of the underlying classical Petrinet and therefore reachability analysis for this kind of Petrinets is purchased on the reachability graph of the classical reachability graph preferably. In the non-stochastic area, there exist quite a few simulation tools, that consider time and priorities.

However, to our best knowledge, there exists no analytical approach to evaluate non-reachability in non-stochastic priorized time-depended Petrinets.

# 2 Definitions

## 2.1 Notation

This subsection introduces the basic notations we use in our paper. $\mathbb{N}$ and $\mathbb{R}$ denote the set of natural numbers and rational numbers, respectively. $\mathbb{N}^+ = \mathbb{N}\backslash\{0\}$ denotes the set of natural numbers without 0, and $\mathbb{Q}_0^+$ denotes the set of nonnegative rational numbers.

$\mathcal{M}(m,n)$ is the set of all matrices with $m$ rows and $n$ columns. A superscript in parentheses distinguishes different matrices. For the arbitrary matrix $A^{(k)} \in \mathcal{M}(m,n)$, $A_i^{(k)}$ is the $i$-th row and $A_{.j}^{(k)}$ is the $j$-th column the matrix.

Let $M$ be a finite set. $|M|$ is the number of elements of $M$.

Let $Q$ be a finite multiset (bag) in $M$. $\kappa_Q(m)$ with $m \in M$ denotes the multiplicity of $m$, i.e., how many instances of $m$ are in $Q$. $E_n = (e_{i,j}) \in \mathcal{M}(n,n)$ denotes the (unit-)matrix with $e_{i,j} = \begin{cases} 1 & i = j \\ 0 & \text{else} \end{cases}$ and $\mathcal{O}_n = (o_{i,j}) \in \mathcal{M}(n,n)$ the (zero-)matrix with $o_{i,j} = 0\ \forall i,j$. The relation $r^{(1)} \not\geq r^{(2)}$ of the two vectors $r^{(1)}, r^{(2)} \in \mathcal{M}(m,1)$ means, that there exists at least one $i,\ i \in \{1,\ldots,m\}$ with $r_i^{(1)} < r_i^{(2)}$.

## 2.2 Structural Descriptions

**Definition 2.1 (Petrinet)** *The structure $N = (P,T,F,V,m_o)$ is called a Petrinet (PN) iff*

1. *$P,T,F$ are finite sets with $P \cap T = \emptyset$, $P \cup T \neq \emptyset$, $F \subseteq (P \times T) \cup (T \times P)$ and $dom(F) \cup cod(F) = P \cup T$*
2. *$V : F \longrightarrow \mathbb{N}^+$ (weight of the arcs)*
3. *$m_o : P \longrightarrow \mathbb{N}$ (initial marking)*

A marking of a PN is a function $m : P \longrightarrow \mathbb{N}$, such that $m(p)$ denotes the number of tokens at the place $p$. The pre- and post-sets of a transition $t$ are given by $Ft = \{p \mid p \in P \wedge (p,t) \in F\}$ and $tF = \{p \mid p \in P \wedge (t,p) \in F\}$, respectively. Each transition $t \in T$ induces the markings $t^-$ and $t^+$, defined as follows:

$$t^-(p) = \begin{cases} V(p,t) & \text{iff} \quad (p,t) \in F \\ 0 & \text{iff} \quad (p,t) \notin F \end{cases} \qquad t^+(p) = \begin{cases} V(t,p) & \text{iff} \quad (t,p) \in F \\ 0 & \text{iff} \quad (t,p) \notin F \end{cases}$$

A transition $t \in T$ is enabled (may fire) at a marking $m$ iff $t^- \leq m$ (e.g., $t^-(p) \leq m(p)$ for every place $p \in P$). When an enabled transition $t$ at a marking $m$ fires, this yields a new marking $m'$ given by $m'(p) := m(p) + t^+(p) - t^-(p)$.

**Definition 2.2 (Duration Petrinet (DPN))** *The structure $Z = (N, D)$ is called a Duration Petrinet*[1] *(DPN) iff:*

1. *$S(Z) = N$ is a PN (Skeleton of $Z$).*
2. *$D : T \longrightarrow \mathbb{Q}_0^+$ (duration function).*

$d_i := D(t_i)$ is the duration of transition's $t_i$ firing. It is easy to see, that without loss of generality we may consider DPNs with $D : T \longrightarrow \mathbb{N}$. Therefore, only such time functions $D$ will be considered subsequently.

**Definition 2.3 (time dimension)** $d := \max\limits_{t \in T}\{D(t)\} + 1$ *is call the time dimension of the DPN.*

**Definition 2.4 (Pritoriy Duration Petrinets, (PDPN))** *The structure $Z = (N, \Theta)$ is called a Priority Duration Petrinet (PDPN) iff:*

1. *$S(Z) = N$ a DPN*
2. *$\Theta : T \longrightarrow \mathbb{N}$ (priority function).*

$\theta_i = \Theta(t_1)$ denotes the priority of transition $t_i$. Without loss of generality we assume that a higher priority value means that the transition is preferred to a transition with a lower priority value.

For PDPN (as for DPN in [3]), a *time marking* is defined.

**Definition 2.5 (time marking)** *Let $Z$ be a PDPN. A matrix $m$ with $m \in \mathcal{M}(|P|, d)$ is a time marking in $Z$.*

**Definition 2.6 (initial time marking)** $m^{(0)}$ *is an initial time marking, iff $m^{(0)}_{\cdot 1} = m_0$ and $m^{(0)}_{i,j} = 0$ for $i = 1 \ldots |P|$ and $j = 2 \ldots d$.*

Each column of the time marking matrix represents a (partial) marking of a place for different delays. The first column represents the present. The second column represents tokens which are on their way to the place and will arrive in one time unit. The same is true for the third column with two time units, etc.

[1] Also called Timed Petrinet.

## 2.3 Dynamics

A Petrinet has a dynamical behavior that leads to a change of the marking. The notation for a change from marking $m^{(1)}$ to marking $m^{(2)}$ is $m^{(1)} \rightarrow m^{(2)}$. In general, two kinds of changing actions have to be distinguished:

- *Firing of transitions.* Firing transitions is similar to classical Petrinets, however, we allow a firing of maximal sets of transitions only.

  We denote firing of the set $\{t_1, \ldots, t_k\}$ by $m^{(1)} \xrightarrow{\{t_1,\ldots,t_k\}} m^{(2)}$. When there is a need for distinction, we denote a marking that is reached by firing with a hat: $m^{(1)} \xrightarrow{\{t_1,\ldots,t_k\}} \hat{m}^{(2)}$
- *Elapsing of time.* A DPN (and thus a PDPN) may change its marking by elapsing of time. The time elapsing happens syncronously for all transitions in the net.

  We denote elapsing of $\tau$ time units by $m^{(1)} \underset{\tau}{\rightarrow} m^{(2)}$. When there is a need for distinction, we denote a marking that is reached be time elapsing by a tilde: $m^{(1)} \underset{\tau}{\rightarrow} \tilde{m}^{(2)}$.

In the following, we define the changing actions in detail. We start with the elapsing of time. It is equivalent to DPN, cf. [3]. To allow consideration about time, we define a transition clock vector:

**Definition 2.7 (transition clock vector)** *Let $Z$ be a PDPN. Then, the vector $h \in \mathcal{M}(|T|, 1)$ is called transition clock vector of $Z$, iff*
$\forall i\, (1 \leq i \leq |T| \rightarrow h_i \leq D(t))$

$h_i = 0$ means, that transition $t_i$ does not fire, whereas $h_i > 0$ denotes that $t_i$ is firing and $h_i$ shows remaining time until the firing is finished. The pair $(m, h)$ describes the state of the PDPN.

Now we are ready to define time elapsing:

**Definition 2.8 (time elapsing)** *Let $Z$ be a PDPN and $m^{(1)}$ and $m^{(2)}$ time markings in $Z$. The time marking $m^{(2)}$ is yield from $m^{(1)}$ by time elapsing, iff*

$$m^{(2)}_{i,j} := \begin{cases} m^{(1)}_{i,1} + m^{(1)}_{i,2} & , j = 1 \\ m^{(1)}_{i,j+1} & , 2 \leq j \leq d-1 \\ 0 & , j = d \end{cases} \quad \textit{and } h^{(2)}_i := \max(0, h^{(1)}_i - 1)$$

In other words, all tokens in the time marking move one column to the left, except the first column, that accumulates the token from the frist and second column, and the last column, which is filled with zero. In addition, all non-zero clocks are decreased.

Firing is equivalent to the firing in DPN too, as long as the selection of transitions to fire is not considered:

**Definition 2.9 (firing)** *Let $Z$ be a PDPN and $m^{(1)}$ and $m^{(2)}$ time markings in $Z$. The time marking $m^{(2)}$ is yield from $m^{(1)}$ by firing the set of transitions $\mathcal{B}$, iff*

$$m^{(2)}_{i,j} := \begin{cases} m^{(1)}_{i,j} - \sum\limits_{t_s \in \mathcal{B}} V(P_i, t_s) + \sum\limits_{\substack{t_s \in \mathcal{B},\\ d_s = 0}} V(t_s, P_i) & , j = 1 \\ m^{(1)}_{i,j} + \sum\limits_{\substack{t_s \in \mathcal{B},\\ d_s = j-1}} V(T_s, P_i) & , j > 1 \end{cases}$$

*and*

$$h^{(2)}_i := \begin{cases} D(t_i) & , t_i \in \mathcal{B} \\ h^{(1)}_i & , else \end{cases}$$

In other words, firing a transition removes a number of tokens from the first column of all places in the firing transition's pre-set and adds a number of tokens to a certain column of all places in the transition's post-set. The column to add corresponds to delay of the transition (0: first column, 1: second column, etc.) and the numbers of tokens correspond to the weight of arcs form and to the transition, respectively.

$h_i$ is working like an egg-timer: When a transition $t_i$ starts to fire, then its clock is set to $d_i$, i.e., $h_i := d_i$. After then, $h_i$ is decreased by each time elapsing.

Until here, the definition of a PDPN does not differ of the definition of a DPN.[2] The impact of the priorities is in the notion of a step.

**Definition 2.10 (prioritized maximal step)** *Let $Z$ be an PDPN. $\mathcal{B} \subseteq T$ is called a prioritized maximal step on the time marking $m$ with the transition clock vector $h$ iff*

1. $\mathcal{B} \subseteq T$
2. $\sum\limits_{t \in \mathcal{B}} t^- \leq m_{.1}$
3. $\forall t (t \in \mathcal{B} \rightarrow h(t) = 0)$
4. $\forall t \forall t_1 \big( \big(t \in \mathcal{B} \wedge t_1 \notin \mathcal{B} \ \wedge \ Ft \cap Ft_1 \neq \emptyset \ \wedge \ t_1^- \leq m_{.1} \ \wedge \ h(t_1) = 0\big) \quad \rightarrow \left( \Theta(t) \geq \Theta(t_1) \vee m_{.1} - \sum\limits_{\substack{t \in \mathcal{B} \\ \Theta(t) \geq \Theta(t_1)}} t^- \not\geq t_1^- \right) \big)$
5. $\neg \exists \mathcal{B}^* \left( (\mathcal{B}^* \supset \mathcal{B}) \ \wedge \ (\mathcal{B}^* \text{ satisfies 1. – 4.}) \right)$

In other words, Definition 2.10 describes a maximal (5) set of transitions (1) which are enabled (2) and not in the process of firing (3), that contains no lower prioritized transition as long it could contain a higher prioritized transition instead (4).

[2]However, a DPN as defined in [3] does not allow zero-time delays. But—as also discussed there—it is easy to extend the definition in the way used in the current paper.

Since we allow zero-time transitions (i.e. $d_i = 0$), it is possible that more than one prioritized maximal step takes place before a time unit may elapse. Thus, we define a global step that includes all firing actions that take place before time elapses.

**Definition 2.11 (global step)** *Let $Z$ be an PDPN with the time marking $m$. $\mathcal{G}$ is a multiset (bag) that is constructed in the following way:*

1. *$\mathcal{G} = \emptyset$*
2. *If there exists a prioritized maximal step $\mathcal{B} \neq \emptyset$, then $\mathcal{G} := \mathcal{G} + \mathcal{B}$; else the construction is ready.*
3. *$m$ and $h$ are changed according to Definition 2.9 by firing the set $\mathcal{B}$. Continue with 2*

A global step $\mathcal{G}$ is a multiset yield by addition of the prioritized maximal steps $\mathcal{B}_1, \ldots, \mathcal{B}_r$ where $m^{(*)} \xrightarrow{\mathcal{B}_1} m^{(1)} \xrightarrow{\mathcal{B}_2} \cdots \xrightarrow{\mathcal{B}_r} m^{(r)}$. Since $\mathcal{G}$ is a multiset, it may include more than one instances of a certain transition. However, this is only true, if this transition has a zero-time delay. Obviously, a global step may be an empty set.

The dynamical behavior of a PDPN is marked by a strict alternation of firing with global steps and time elapsing:

$$m^{(0)} \xrightarrow{\mathcal{G}_1} \hat{m}^{(1)} \underset{1}{\rightarrow} \tilde{m}^{(1)} \xrightarrow{\mathcal{G}_2} \cdots \xrightarrow{\mathcal{G}_n} \hat{m}^{(n)} \underset{1}{\rightarrow} \tilde{m}^{(n)}$$

Without loss of generality, we use one time unit for the time elapsing. However, each common factor of all transition delays would be possible.

Since the number of elapsed time units after a firing is constant for a PDPN and in our considerations always 1, we skip in the following the notion of the elapsed time. I.e., a firing sequence $(\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3)$ means the alternating sequence of firing and time elapsing $(\mathcal{G}_1, 1, \mathcal{G}_2, 1, \mathcal{G}_3)$ or $(\mathcal{G}_1, 1, \mathcal{G}_2, 1, \mathcal{G}_3, 1)$.

**Definition 2.12 (reachability)** *Let $Z$ be a PDPN. A time marking $m'$ is reachable in $Z$ iff there exists a sequence $\sigma = (\mathcal{G}_1, \ldots, \mathcal{G}_\alpha)$ of global steps such that*

$$m^{(0)} \xrightarrow{\mathcal{G}_1} \hat{m}^{(1)} \underset{1}{\rightarrow} \tilde{m}^{(1)} \xrightarrow{\mathcal{G}_2} \hat{m}^{(2)} \underset{1}{\rightarrow} \tilde{m}^{(2)} \ldots \rightarrow m'$$

*$\sigma$ may end either with firing, or with time elapsing.*

# 3 State Equation and Firing Conditions

In this section we introduce some further concepts that support an algebraic reasoning about PDPN.

The structure of a PDPN as given by Definition 2.4 may be described by an incidence matrix.

**Definition 3.1 (incidence matrix)** *Let $Z$ be a PDPN. The matrix $C \in \mathcal{M}(|P|, d{\cdot}|T|)$ is called the incidence matrix of $Z$, iff $C := (C^{(1)}, C^{(2)}, \ldots, C^{(|T|)})$ with $C^{(k)} \in \mathcal{M}(|P|, d)$,$k \in \{1, \ldots, |T|\}$ and $C^{(k)} = (c^{(k)}_{i,j})$ where*

$$c^{(k)}_{i,j} := \begin{cases} V(t_k, P_i) - V(P_i, t_k) & , d_k = 0, j = 1 \\ -V(P_i, t_k) & , d_k > 0, j = 1 \\ V(t_k, P_i) & , (d_k > 0), 0 < j - 1 = d_k \\ 0 & , else \end{cases}$$

I.e., a submatrix $C^{(i)}$ describes, how the transition $t_i$ is connected with places. If the transition has a zero-delay ($d_i = 0$), only the first column $C^{(i)}_{.1}$ is used. It includes difference of the weights of all arces *to* the places and these *from* the places. If the transition has a delay ($0 < d_i < d$), the first column includes the weights *from* the places and the $d_i + 1$-th column the weights *to* the places.

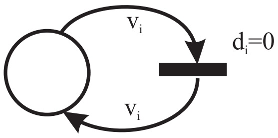


Figure 1: A loop in a Petrinet

Please note, that—similar to a classic Petrinet—a loop (i.e., two arces $(p, t)$ and $(t, p)$ with the same weight, cf. Figure 1) will not appear in the incidence matrix, if the transition has a zero-time delay. However, if the transition in the loop has a non-zero delay ($d_i > 0$) both arces will be represented in the incidence matrix.

As the next element we define a bag matrix to represent global steps.

**Definition 3.2 (bag matrix)** *Let $\mathcal{G}$ be a (maximal or global) step and $\kappa_{\mathcal{G}}(t_i)$ the multiplicity of transition $t_i$ in $\mathcal{G}$. The matrix $G \in \mathcal{M}(d \cdot |T|, d)$ is called the bag matrix of $\mathcal{G}$ iff*

$$G = \begin{pmatrix} G^{(1)} \\ G^{(2)} \\ \vdots \\ G^{(|T|)} \end{pmatrix} \quad \textit{and } G^{(s)} = \kappa_{\mathcal{G}_s} \cdot E_d$$

Obviously, the submatrix $G^{(s)}$ is the zero-matrix if the transition $t_s$ does not belong to the global step $\mathcal{G}$.

Next, we define a progress matrix that allow us to describe the impact of time elapsing to the time marking.

**Definition 3.3 (progress matrix)** *Let $Z$ be a PDPN. The matrix $R \in \mathcal{M}(d,d)$ is called the progress matrix of $Z$, iff*

$$r_{i,j} := \begin{cases} 1 & \text{if } (i=j=1) \text{ or } (i=j+1) \\ 0 & \text{else} \end{cases}$$

Finally, we define a Parikh-Matrix that represents a sequence of steps and time units.

**Definition 3.4 (Parikh-matrix)** *The matrix $\Psi \in \mathcal{M}(|P|, d)$ is called Parikh-matrix of the sequence $\sigma = (\mathcal{G}_1, \ldots, \mathcal{G}_n)$, iff*

$$\Psi_\sigma := \sum_{i=1}^{n} G^{(i)} \cdot R^{n-i}$$

Using the introduced elements, we can formulate a state equation for PDPNs:

**Theorem 3.1 (state equation)** *Let $Z$ be a PDPN, $\sigma = (\mathcal{G}_1, \ldots, \mathcal{G}_n)$ a firing sequence in $Z$, $m^{(0)}$ the initial time marking of $Z$ and*
$m^{(0)} \xrightarrow{\mathcal{G}_1} \hat{m}^{(1)} \underset{1}{\longrightarrow} \tilde{m}^{(1)} \xrightarrow{\mathcal{G}_2} \hat{m}^{(2)} \underset{1}{\longrightarrow} \ldots \xrightarrow{\mathcal{G}_n} m^{(n)}$. *Then it holds:*

$$m^{(n)} = m^{(0)} \cdot R^{n-1} + C \cdot \Psi_\sigma \tag{1}$$

**Proof:**
The proof is analogously to the proof of Theorem 3.1 in [3]. □

**Corollary 3.1 (from Theorem 3.1)** *Let $Z$ be a PDPN, $\sigma = (\mathcal{G}_1, \ldots, \mathcal{G}_n)$ a firing sequence in $Z$, $m^{(0)}$ the initial time marking of $Z$ and*
$m^{(0)} \xrightarrow{\mathcal{G}_1} \hat{m}^{(1)} \underset{1}{\longrightarrow} \tilde{m}^{(1)} \xrightarrow{\mathcal{G}_2} \hat{m}^{(2)} \underset{1}{\longrightarrow} \ldots \underset{1}{\longrightarrow} m^{(n)}$. *Then it holds:*

$$m^{(n)} = m^{(0)} \cdot R^{n} + C \cdot \Psi_\sigma R \tag{2}$$

**Corollary 3.2** *Let $m^{(1)} \underset{\tau}{\longrightarrow} m^{(2)}$, $\tau \in \mathbb{N}^+$. The following holds:*

$$\forall j \left( (1 \le j \le |P|) \rightarrow \sum_{i=1}^{d} m^{(1)}_{j,i} = \sum_{i=1}^{d} m^{(2)}_{j,i} \right) \tag{3}$$

The following three remarks conclude directly from the Definitions 2.10 and 2.11:

**Remark 3.1 (maximality condition for prioritized maximal steps)**
*Let $m^{(1)} \xrightarrow{\mathcal{B}} m^{(2)}$. Then it is true, that*

$$\forall t \left( (t \in T \wedge h(t) = 0) \rightarrow m_{.1} - \sum_{\hat{t} \in \mathcal{B}} \hat{t}^- \not\geq t^- \right) \tag{4}$$

**Remark 3.2 (maximality condition for global steps)** *Let $m^{(1)} \xrightarrow{\mathcal{G}} m^{(2)}$. Then the following holds:*

$$\forall t \left( (t \in T, h(t) = 0) \to m^{(2)}_{\cdot 1} \ngeq t^- \right) \tag{5}$$

**Remark 3.3 (priority rule)** *Let $Z$ be an PDPN with $t_1, t_2 \in T$, $t_1^- \leq t_2^-$ $\Theta(t_1) \geq \Theta(t_2)$ and $D(t_1) \leq D(t_2)$. Then the following holds:*

$$\forall \sigma \left( (\sigma = \{\mathcal{G}_1, \ldots, \mathcal{G}_n\}) \to \sum_{i=1}^{n} \kappa_{\mathcal{G}_i}(t_1) \geq \sum_{i=1}^{n} \kappa_{\mathcal{G}_i}(t_2) \right) \tag{6}$$

# 4 An Example

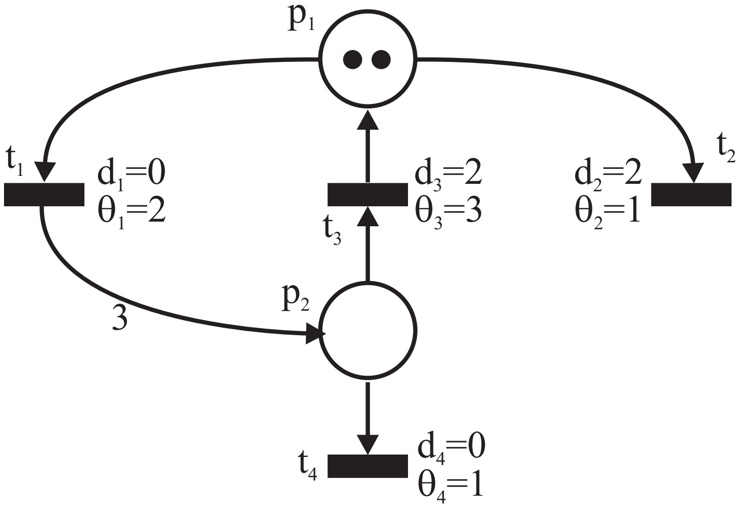


Figure 2: A example PDPN

In this section, we show the application of our approach. Please, consider the PDPN from Figure 2.

We want to examine the following proposition:

**Proposition 4.1** *The PDPN $Z$ in Figure 2 with the initial time marking $m^{(0)} = \left(\begin{smallmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$ will never reach the time marking $m^* = \left(\begin{smallmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$.*

For a DPN (i.e., in case the priorities would be ignored) the marking $m^*$ is reachable, i.e., the Proposition 4.1 does not hold: Then, the sequence $\left(\begin{smallmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) \xrightarrow{\{t_1,t_2\},\{t_3,t_4\},\{t_4\}} \left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{smallmatrix}\right) \underset{1}{\to} \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) \xrightarrow{\emptyset} \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) \underset{1}{\to} \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) \xrightarrow{\{t_2\}} \left(\begin{smallmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$ leads to $m^*$.

We prove Proposition 4.1 by falsification of the converse.

**Proof:**
Assume Proposition 4.1 is wrong. Then, there exist a sequence $\sigma = \{\mathcal{G}_1, \mathcal{G}_2, \dots, \mathcal{G}_n\}$ with $m^{(0)} \xrightarrow{\sigma} m^*$. However, we will show that each sequence that leads to $\left(\begin{smallmatrix}0&0&0\\0&0&0\end{smallmatrix}\right)$ has to start from $\left(\begin{smallmatrix}0&0&0\\0&0&0\end{smallmatrix}\right)$.

It is sufficient to consider the last action in the sequence only. We have to consider two cases. Case A: the last action of the sequence is a elapsing of time, and case B: the last action of the sequence is a firing.

In case A, i.e., $\hat{m}^{(n)} \underset{1}{\rightarrow} m^*$, it is easy to see that $\hat{m}^{(n)}$ has to be $\left(\begin{smallmatrix}0&0&0\\0&0&0\end{smallmatrix}\right)$, because of Corollary 3.2 and because a time marking can not contain any element smaller than zero.

To considering case B, we define:

- $x_i = \sum_{j=1}^{n-1} \kappa_{\mathcal{G}_j}(t_i)$ , i.e., $x_i$ is the number of firing of the transition $t_i$ within the sequence $\{\mathcal{G}_1, \dots, \mathcal{G}_{n-1}\}$.
- $\alpha_i = \kappa_{\mathcal{G}_n}(t_i)$, i.e., $\alpha_i$ is the number of firing of the transition $t_i$ within $\mathcal{G}_n$.
- $y_i = \sum_{i=j}^{n-2} \kappa_{\mathcal{G}_j}(t_i)$, i.e., $y_i$ is the number of firing of the transition $t_i$ within the sequence $\{\mathcal{G}_1, \dots, \mathcal{G}_{n-2}\}$.
- $\beta_i = \kappa_{\mathcal{G}_{n-1}}(t_i)$, i.e., $\beta_i$ is the number of firing of the transition $t_i$ within $\mathcal{G}_{n-1}$.

And of course, the following is true:

$$x_i = y_i + \beta_i \tag{7}$$

From Remark 3.3 we know:

$$x_1 \geq x_2, y_1 \geq y_2, \alpha_1 \geq \alpha_2, \text{ and } \beta_1 \geq \beta_2 \tag{8}$$

We want to apply the state equation. In our example,
$C = \left( \begin{matrix} -1 & 0 & 0 \\ 3 & 0 & 0 \end{matrix} \quad \begin{matrix} -1 & 0 & 0 \\ 0 & 0 & 0 \end{matrix} \quad \begin{matrix} 0 & 0 & 1 \\ -1 & 0 & 0 \end{matrix} \quad \begin{matrix} 0 & 0 & 0 \\ -1 & 0 & 0 \end{matrix} \right)$, $R = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$
and $R^i = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ for all $i > 1$.

Insert in (1), we get:

$$\begin{aligned} m^* = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} &= m^{(0)} R^{n-1} + C \cdot \Psi \\ &= m^{(0)} R^{n-1} + C \left( \sum_{i=1}^{n} G^{(i)} R^{n-i} \right) \\ &= \left(\begin{smallmatrix}2&0&0\\0&0&0\end{smallmatrix}\right) \left(\begin{smallmatrix}1&0&0\\1&0&0\\1&0&0\end{smallmatrix}\right) + C \left( \sum_{i=1}^{n-2} G^{(i)} \left(\begin{smallmatrix}1&0&0\\1&0&0\\1&0&0\end{smallmatrix}\right) + G^{(n-1)} \left(\begin{smallmatrix}1&0&0\\1&0&0\\0&1&0\end{smallmatrix}\right) + G^{(n)} \right) \end{aligned}$$

$$= \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + C \left( \begin{pmatrix} y_1 & 0 & 0 \\ y_1 & 0 & 0 \\ y_1 & 0 & 0 \\ y_2 & 0 & 0 \\ y_2 & 0 & 0 \\ y_2 & 0 & 0 \\ y_3 & 0 & 0 \\ y_3 & 0 & 0 \\ y_3 & 0 & 0 \\ y_4 & 0 & 0 \\ y_4 & 0 & 0 \\ y_4 & 0 & 0 \end{pmatrix} + \begin{pmatrix} \beta_1 & 0 & 0 \\ \beta_1 & 0 & 0 \\ 0 & \beta_1 & 0 \\ \beta_2 & 0 & 0 \\ \beta_2 & 0 & 0 \\ 0 & \beta_2 & 0 \\ \beta_3 & 0 & 0 \\ \beta_3 & 0 & 0 \\ 0 & \beta_3 & 0 \\ \beta_4 & 0 & 0 \\ \beta_4 & 0 & 0 \\ 0 & \beta_4 & 0 \end{pmatrix} + \begin{pmatrix} \alpha_1 & 0 & 0 \\ 0 & \alpha_1 & 0 \\ 0 & 0 & \alpha_1 \\ \alpha_2 & 0 & 0 \\ 0 & \alpha_2 & 0 \\ 0 & 0 & \alpha_2 \\ \alpha_3 & 0 & 0 \\ 0 & \alpha_3 & 0 \\ 0 & 0 & \alpha_3 \\ \alpha_4 & 0 & 0 \\ 0 & \alpha_4 & 0 \\ 0 & 0 & \alpha_4 \end{pmatrix} \right)$$

$$= \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + C \begin{pmatrix} y_1 + \beta_1 + \alpha_1 & 0 & 0 \\ y_1 + \beta_1 & \alpha_1 & 0 \\ y_1 & \beta_1 & \alpha_1 \\ & \vdots & \\ y_4 + \beta_4 + \alpha_4 & 0 & 0 \\ y_4 + \beta_4 & \alpha_4 & 0 \\ y_4 & \beta_4 & \alpha_4 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} -y_1 - \beta_1 - \alpha_1 - y_2 - \beta_2 - \alpha_2 + y_3 & \beta_3 & \alpha_3 \\ 3y_1 + 3\beta_1 + 3\alpha_1 - y_3 - \beta_3 - \alpha_3 - y_4 - \beta_4 - \alpha_4 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 - y_1 - \beta_1 - \alpha_1 - y_2 - \beta_2 - \alpha_2 + y_3 & \beta_3 & \alpha_3 \\ 3y_1 + 3\beta_1 + 3\alpha_1 - y_3 - \beta_3 - \alpha_3 - y_4 - \beta_4 - \alpha_4 & 0 & 0 \end{pmatrix}$$

We get $\beta_3 = 0$ and therefore by (7): $x_3 = y_3$. In addition, we get $\alpha_3 = 0$. $\alpha_3 = \beta_3 = 0$ means that $t_3$ does not fire during the last step $\mathcal{G}_n$ or during the step before $\mathcal{G}_{n-1}$. Thus, after $\mathcal{G}_n$

$$h(t_3) = 0 \tag{9}$$

Also $t_4$ does not fire during $\mathcal{G}_n$, since $t_4$ has the same pre-condition as $t_3$, but a lower priority, i.e., $\alpha_4 = 0$

Assume, $t_1$ does fire during $\mathcal{G}_n$. Since $d_1 = 0$, $\alpha_3 = 0$, and (9), maximality condition (5) is not met. Therefore, $t_1$ does not fire during $\mathcal{G}_n$, thus $\alpha_1 = 0$.

Following, because of (8), $\alpha_2 = 0$.

We have shown, that none of the transitions $t_1, \ldots, t_4$ belong to $\mathcal{G}_n$, i.e., $\mathcal{G}_n = \emptyset$. Thus, regarding the state equation (1) for $\tilde{m}^{(n-1)} \xrightarrow{\mathcal{G}_n} m^{(*)}$

$$\begin{aligned} m^* = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} &= \tilde{m}^{(n-1)} \cdot R^0 + C \cdot \begin{pmatrix} \mathcal{O}_d \\ \mathcal{O}_d \\ \mathcal{O}_d \\ \mathcal{O}_d \end{pmatrix} \\ &= \tilde{m}^{(n-1)} \cdot E_d + \mathcal{O}_d \\ &= \tilde{m}^{(n-1)} \end{aligned}$$

i.e.

$$\tilde{m}^{(n-1)} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

That concludes the proof. $\square$

# 5 Conclusions and Future Work

Within this paper, we have provided an approach that allows for reasoning about Priority Duration Petrinets. We have given sufficient conditions to prove non-reachablity, and presented an example.

Currently, we are working on a big-scale application of our approach: the correctness proof of the Message Scheduled System architecture.

In order to reach this goal it is not sufficient to apply our technique just to one specific net, we have to apply it to a class of nets describing generic MSS instances. These nets can be automatically composed out of basic building blocks using the technology presented in [5].

To proof correctness of the MSS architecture we must show that in this class of nets a specific error state is not reachable if the MSS configuration specified by the net is valid according to the rules of MSS.

# References


[1] C. L. Lui and J. W. Layland. Scheduling algorithms for multiprogramming in a hard-real-time enviroment. *JACM*, 20(1):46–61, January 1973.

[2] M. Ajmone Marsan, G. Balbo, G. Conte, S. Donatelli, and G. Franceschinis. *Modelling with Generalized Stochastic Petri Nets*. John Wiley and Sons, 1996.

[3] L. Popova-Zeugmann, M. Werner, and J. Richling. Using state-equation to prove non-reachability in timed petrinets. *Fundamenta Informaticae*, 2003.

[4] C. Ramchandani. Analysis of asynchronous concurrent systems by Timed Petri Nets. *Project MAC-TR 120, MIT*, February 1974.

[5] J. Richling, M.Werner, and L. Popova-Zeugmann. Automatic composition of timed petrinet specifications for a real-time architecture. In *Proceedings of 2002 IEEE International Conference on Robotics and Automation*, Washington DC, May 2002.

[6] J. Richling, L. Popova-Zeugmann, and M. Werner. Verification of non-functional properties of a composable architecture with petrinets. *Fundamenta Informaticae*, 51:185–200, 2002.

[7] Jan Richling. Message Scheduled System - A Composable Architecture for Embedded Real-Time-Systems. In *Prooceedings of 2000 Int. Conference on Parallel and Distributed Processing techniques and Applications (PDPTA 2000)*, volume 4, pages 2143–2150, Jun 2000.

[8] Peter H. Starke. *Analyse von Petri-Netz-Modellen*. B.G. Teubner, Stuttgart, 1990.

[9] Peter H. Starke. A memo on time constraints in petri nets. Informatik-Bericht 46, Humboldt University of Berlin, 1995.