A State Equation for Timed Petrinets

Louchka Popova-Zeugmann* Matthias Werner† Jan Richling*

Abstract

Nonreachability proofs in Timed Petrinets were usually done by proving the non-reachability within the time-less skeleton. However, in many cases this approach fails.

In this paper, we present an approach to prove nonreachability within the actual Timed Petrinet. For this purpose, we introduce a state equation for Timed Petrinets in analogy to time-less nets. Using this state equation, we can express reachability as a systems of equations and inequations, which is solvable in polynomial time.

1 Introduction

1.1 Motivation

The complexity of todays computer systems is increasing every year due to increasing computing power and due to increasing demands of users. This is not only valid for general purpose systems used in offices or at home, but also for embedded systems used inside technical systems such as cars or airplanes. The correct function of such systems does not only depend on functional aspects such as the correctness of a result, but also on nonfunctional properties such as performance, timeliness, configurability or reliability. In most cases (especially if a failure of the system results in danger for humans) it is not sufficient to argue that these properties are fulfilled, it is necessary to prove them.

In order to develope such a proof it is necessary to use a formal description technique to describe the system, and to express the desired properties.

As an example for a composable architecture for embedded real-time systems we have developed a system architecture called *Message Scheduled System* (MSS) [4]. MSS supports composability, which means that one can build a system out of components and put them together in a way that nonfunctional properties such as timeliness are still holding and system properties such as end-to-end-delays can precomputed.

MSS uses scheduling algorithms at three different levels to reach that goal of composability. In order to prove that we meet our objectives, we developed a formal specification of MSS's behavior based on Timed Petrinets [3, 2].

*Humboldt University, {popova|richling}@informatik.hu-berlin.de

†TU Berlin, mwerner@cs.tu-berlin.de

This specification allows modelchecking using the tool INA[5], but proofs for general cases are still an open question. To solve this, we need proving technologies to prove non-reachability in a Timed Petrinet — this will allow us to prove that forbidden (dangerous) states in the MSS-model will never be reached.

A common approach to prove non-reachability in a Timed Petrinet (Duration Net, DPN) is to prove this property in time-less skeleton of the DPN. However, since the nonreachability in the time-less skeleton is a sufficient but not necessary condition for the nonreachability in the DPN, this approach has limits.

In this paper, we present an approach that allows to prove nonreachability in the actual DPN. For that purpose, we have developed a state equation for the DPN that allows to determine the marking of a DPN in analogy to the state equation of timeless nets.

1.2 Related Work

The question of reachability and nonreachability 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 proof certain properties without computing resp. knowing the whole state space of the net. One of the first approaches here is the computing of invariants (comp. [6]). In a classical Petrinet it is relatively easy to obtain place- or transition invariants using the state equation of the net (comp. [6]).

But, when the Petrinet is a time dependent one, the state space becomes smaller. In this case, the use of the state equation of the skeleton - this is a classical Petrinet - is not very reasonable, because this state equation does not take into account the time constrains of the net. Because of the last, in the time dependent net new invariants can be erased, i.e., a reachable state in the skeleton can become unreachable.

Till now, there is no comparable approach for time dependent Petrinets as for the classical nets. In this work we consider Timed Petrinets (also called Duration Petrinets, DPN), defined by Ramchandani (comp. [1]).

The remainder of this paper is organized as follows: Section 2 introduces the needed definitions. In Section 3, we present and prove the state equation for a DPN. In Section 4, we give an example for a nonreachability proof, using the state equation. Finally, the paper ends with some conclusions in Section 5.

2 Basics

2.1 Notation

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

A matrix $A \in \mathcal{M}(m,n)$ is a matrix with m rows and n columns. A superindex in parentheses distinguishes different matrices or vectors, and theire elements, respectively. $A_i^{(k)}$ is the i-th row and $A_{\cdot j}^{(k)}$ is the j-th column of a matrix $A^{(k)}$.

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

$E_n = (e_{i,j}) \in \mathcal{M}(n,n)$ denotes the 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 $r^{(1)} \ngeq r^{(2)}$ 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 Definitions

Definition 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 $Ft = \{p \mid p \in P \wedge pFt\}$ and $tF = \{p \mid p \in P \wedge tFp\}$, respectively. Each transition $t \in T$ induces the marking t^- and t^+, defined as follows:

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

Furthermore, Δt denotes $t^+ - t^-$. 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 $m'(p) := m(p) + \Delta t(p)$. The firing is denoted by $m \xrightarrow{t} m'$.

Definition 2 (Timed Petrinet) *The structure $Z = (N,D)$ is called a Timed Petrinet (DPN) iff:*

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

$D(t_i) = d_i$ is the duration of the firing transition t_i. It is easy to see, that considering DPNs with $D : T \longrightarrow \mathbb{N}$ will not result in a loss of generality. Therefore, only such time functions D will be considered subsequently.

Example 1 *The timed petrinet Z_1 which is used for illustration is shown in Figure 1. Let $d := \max\{d_i | i \in \{1\ldots|T|\}\} + 1$. In the net Z_1: $d = 3$.*

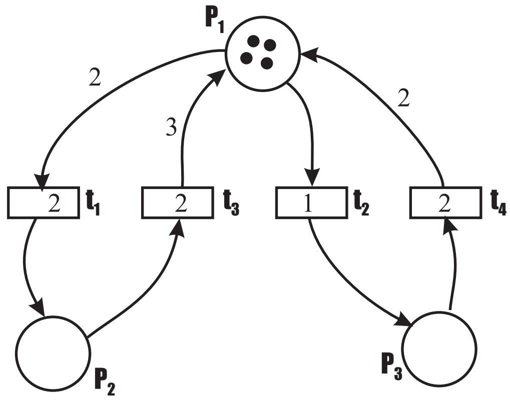

Figure 1: Net from Example 1

Definition 3 (time marking) *Let Z be a DPN. A matrix m with $m \in \mathcal{M}(|P|, d)$ is a time marking in Z.*

Definition 4 (initial time marking) *$m^{(0)}$ is an initial time marking, iff $m^{(0)}_{.1} = m_0$ and $m^{(0)}_{i,j} = 0$ for $i = 1 \dots |P|$ and $j = 2 \dots d$.*

Each column of the time marking matrix represents a (partial) marking of a place for different time steps. The first row represents the present, the second one represents potential[1] changes in the marking one time unit in the future, the third two time units, etc.

Example 2 *The net from Example 1 has the following initial time marking:*

$$m^{(0)} = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Definition 5 (transition clock vector) *Let $Z = (N, D)$ be an DPN. Then, the vector $h : T \longrightarrow \mathbb{N}$ is called transition clock vector of Z, iff*
$\forall t\,(t \in T \to h(t) \leq D(t))$

The so-called initial transition clock vector is the zero-vector.

Definition 6 (maximal step) *Let $Z = (N, D)$ be an DPN. $\mathcal{B} \subset T$ is called a maximal step of the time marking m with the transition clock vector h iff*

1. $\sum\limits_{t \in \mathcal{B}} t^- \leq m_{.1}$

[1]Please note, that a row does not give a full description of future changes, since a transition with a shorter delay may fire later.

2. $\forall t(t \in \mathcal{B} \to h(t) = 0)$

3. $\neg\exists\mathcal{B}^* \left((\mathcal{B}^* \supset \mathcal{B}) \wedge (\mathcal{B} \text{ satisfies 1. and 2.})\right)$

Example 3 *In the net from Example 1, $\mathcal{B}^* = \{t_2\}$ or $\mathcal{B}^+ = \{t_1, t_4\}$ are not maximal steps, but $\mathcal{B} = \{t_1, t_2\}$ is.*

Definition 7 (state change[2]) *Let $Z = (N, D)$ be a DPN and $m^{(1)}$ and $m^{(2)}$ time markings in Z.*

The time marking $m^{(2)}$ is yield from $m^{(1)}$

(a) by firing the maximum step $\mathcal{B} = \{t_{i_1}, \ldots, t_\kappa\}$ ($m^{(1)} \overset{\mathcal{B}}{\mapsto} m^{(2)}$), iff

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

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

(b) by elapsing one time unit ($m^{(1)} \underset{1}{\mapsto} m^{(2)}$), iff

$$m^{(2)}_{i,j} := \begin{cases} m^{(1)}_{i,1} + m^{(1)}_{i,2} & , j = 1 \\ m^{(1)}_{i,j+1} & , 2 \le j \le d-1 \\ 0 & , j = d \end{cases}$$

$$h^{(2)}_i := \max(0, h^{(1)}_i - 1)$$

(a) and (b) happen strictly alternating, beginning with (a) from an initial time marking.

The number of tokens $m_{i,j}$ arrives at place i

Remark 1 *Let $m^{(1)} \overset{\mathcal{B}}{\mapsto} m^{(2)}$. Then, it is easy to see from Definition 6.1 that the following holds*

$$m^{(2)}_{.1} \ngeq t^- \text{ for each } t \in T \backslash \mathcal{B} \tag{1}$$

In case of self concurrency of transitions (1) holds for each $t \in T$.

Remark 2 *Let $m^{(1)} \overset{\mathcal{B}}{\mapsto} m^{(2)}$ and $\forall t(t \in \mathcal{B} \longrightarrow d(t) > 0)$. Then, it follows from Definition 7 that*

$$m^{(2)}_{.1} + \sum_{t \in \mathcal{B}} t^- \le m^{(1)}_{.1}. \tag{2}$$

[2]The pair (m, q) can be considered as a state of a DPN.

For the reader's comfort, we will mark the results of (a) and (b) in different ways, where they need to be distinguished. Variables that are connected with a state transitions of the type (a) will be denoted with a hat (e.g., $\hat{m}$), and variables that are a result of a state transition (b) will be denoted with a tilde (e.g., $\tilde{m}$).

Example 4 *Consider Z_1 again. $\mathcal{B} := \{t_1, t_2\}$ is a maximal step in $m^{(0)}$. Let $m^{(1)}$ be the time marking which the net Z_1 reaches after firing $\mathcal{B}$ at $m^{(0)}$, i.e. $m^{(0)} \xrightarrow{\mathcal{B}} \hat{m}^{(1)}$. It is easy to see that* $\hat{m}^{(1)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix}$ *and* $\hat{q}^{(1)} = \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix}$.

Now, starting from $\hat{m}^{(1)}$ the net obtains the time marking $\tilde{m}^{(1)}$ after elapsing 1 time unit

$$\tilde{m}^{(1)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 1 & 0 & 0 \end{pmatrix} \text{ and the transition clock vector } \tilde{q}^{(1)} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Please note, that the alternating sequence of state changing always starts from initital state (initial time marking, initial transition clock vector) with firing, but may end with one of both, time elapsing or firing.

In order to introduce a state equation for DPN we define an incidence matrix for DPN and a Parikh matrix for DPN.

Definition 8 (incidence matrix) *Let $Z = (N, D)$ be a DPN. 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 $C^{(k)} \in \mathcal{M}(|P|, d)$ and $k \in \{1, \ldots, |T|\}$ and*

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

The matrix C consists of submatrices $C^{(k)}$ representing the transitions t_k of the net. $c_{i,1}^{(k)}$ is the number of tokens that will be changed at place P_i immediately, if the transition t_k is an element of the firing bag. $c_{i,j}^{(k)}$ shows a number of tokens that will arrive at place P_i after $(j-1)$ time units, if the transition t_k is an element of the firing bag.

Example 5 *In the example 1 the incidence matrix of Z_1 is*

$$C = \begin{pmatrix} -2 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \end{pmatrix}$$

Now we define a matrix $B \in \mathcal{M}(d \cdot |T|, d)$ in order to define a Parikh-matrix later. Let us consider a bag $\mathcal{B} = \{t_{i_1}, \ldots, t_{i_\kappa}\}$, $t_{i_j} \in T$.

Definition 9 (bag matrix) *The matrix $B \in \mathcal{M}(d \cdot |T|, d)$ is called the bag matrix of $\mathcal{B}$ iff*

$$B = \begin{pmatrix} B^{(1)} \\ B^{(2)} \\ \vdots \\ B^{(|T|)} \end{pmatrix} \text{ and } B^{(s)} := \begin{cases} E_d & \text{if } s \in \{i_1, \ldots, i_\kappa\} \\ \mathcal{O} & \text{else } (\text{i.e., } s \in \{1, \ldots, |T|\} \backslash \{i_1, \ldots, i_\kappa\}) \end{cases}$$

Example 6 *Let us consider the step $\mathcal{B} = \{t_1, t_2\}$ in Z_1:*

$$B = \begin{pmatrix} B^{(1)} \\ B^{(2)} \\ B^{(3)} \\ B^{(4)} \end{pmatrix} \text{ with } \begin{matrix} B^{(1)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & B^{(2)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ B^{(3)} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} & B^{(4)} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \end{matrix} \text{ i.e.: } B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ & & \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ & & \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ & & \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Next, we define a progress matrix R in order to compute the progress of time.

Definition 10 (progress matrix) *Let $Z = (N, D)$ be a DPN. The matrix $R \in \mathcal{M}(d, d)$ is called the progress matrix of Z, iff*

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

Example 7 *In Example 1 the progress matrix R of the net Z_1 is* $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.

Definition 11 (reachability) *Let $Z = (N, D)$ be a DPN. A time marking m' is reachable in Z iff there exists a sequence $\sigma = (\mathcal{B}_1, \ldots, \mathcal{B}_\alpha)$ of bags such that*

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

3 State Equation

We want to derive a state equation for DPN in analogy to the state equation of time-less nets.

Lemma 1 *Let $Z = (N, D)$ be a DPN, $m^{(1)}$ a reachable time marking in Z and $m^{(1)} \underset{1}{\longrightarrow} m^{(2)}$. Then it holds $m^{(2)} = m^{(1)} \cdot R$.*

Proof: $m^{(2)}_{i,j} = m^{(1)}_{i,j} \cdot R$

Case 1:

$$j = 1 \rightsquigarrow \quad \sum_{s=1}^{d} m^{(1)}_{i,s} \cdot r_{s,1} = m^{(1)}_{i,1} \cdot 1 + m^{(1)}_{i,2} \cdot 1 \underset{acc.def}{=} m^{(2)}_{i,1}$$

Case 2:

$$d > j \geq 2 \rightsquigarrow \quad \sum_{s=1}^{d} m^{(1)}_{i,s} \cdot r_{s,j} = m^{(1)}_{i,j+1} \cdot 1 \underset{acc.def}{=} m^{(2)}_{i,j}$$

Case 3:

$$j = d \rightsquigarrow \quad \sum_{s=1}^{d} m^{(1)}_{i,s} \cdot r_{s,j} = 0 = m^{(2)}_{i,j}$$

□

Example 8 *We consider the timed Petrinet Z_1 and time marking $\hat{m}^{(1)}$ and $\tilde{m}^{(1)}$ from Example 4.*

It is easy to prove that

$$\tilde{m}^{(1)} = m^{(1)} \cdot R$$

and

$$R = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Lemma 2 *Let $Z = (N, D)$ be a DPN and $m^{(1)} \xrightarrow{\mathcal{B}} m^{(2)}$, $\mathcal{B} = \{t_{i_1}, \ldots, t_{i_\kappa}\}$. Then holds: $m^{(2)} = m^{(1)} + C \cdot B$.*

Proof:
We consider $m^{(2)}_{i,j}$.
Case 1: $j = 1$

According to Definition 7 the following is true:

$$m_{i,1}^{(2)} = m_{i,j}^{(1)} - \sum_{t_s \in \mathcal{B}} V(P_{i,j}, t_s) + \sum_{\substack{t_s \in \mathcal{B} \\ d_s = j-1 = 0}} V(t_s, P_i) \quad .$$

Therefore, it is sufficient to show that

$$\sum_{j=1}^{d \cdot |T|} c_{i,j} b_{j,1} = - \sum_{t_s \in \mathcal{B}} V(P_i, t_s) + \sum_{\substack{t_s \in \mathcal{B}, \\ d_s = 0}} V(t_s, P_i) \quad .$$

Now we consider the bag matrix B. The first column $B_{.1}$ of B is $B_{.1} = (b^{(1)}, b^{(2)}, \ldots, b^{(|T|)})^T$, where $b^{(k)}$ is a d-dimensional vector with

$$b^{(k)} = (b_1^{(k)}, \ldots, b_d^{(k)}) \quad k = 1, \ldots, |T|$$

and

$$b_j^{(k)} = \begin{cases} 1 & , j = 1, k \in \{i_1, \ldots, i_\kappa\} \\ 0 & , else \end{cases}$$

That means, $b^{(k)}$ is the d-dimensional vector $(1, 0, \ldots, 0)^T$ if $t_k \in \mathcal{B}$ and the d-dimensional zero-vector else.

Hence,

$$\sum_{j=1}^{d \cdot |T|} c_{i,j} \cdot b_{j,1} = \sum_{t_k \in \mathcal{B}} c_{i,j}^{(k)} \cdot b_j^{(k)} = \sum_{t_k \in \mathcal{B}} c_{i,1}^{(k)} \underset{acc.def}{=} - \sum_{t_k \in \mathcal{B}} V(P_i, t_k) + \sum_{\substack{t_k \in \mathcal{B}, \\ d_k = 0}} V(t_k, P_i)$$

Case 2: $j \geq 2$

Obviously, now we have to show that

$$\sum_{s=1}^{d \cdot |T|} c_{i,s} \cdot b_{s,j} = \sum_{\substack{t_k \in \mathcal{B}, \\ d_k = j-1}} V(t_s, P_i) \quad .$$

We consider the j-th column of the bag matrix B, the vector $B_{.j}$:

$$B_{.j} = (b^{(1)}, b^{(2)}, \ldots, b^{(|T|)})$$

with

$$b^{(k)} = (b_1^{(k)}, \ldots, b_d^{(k)})^T \quad \overset{|T|}{\underset{1}{\forall}} k$$

and

$$b_s^{(k)} = \begin{cases} 1 & , s = k \\ 0 & , else \end{cases}$$

i.e. $b^{(k)} = \underbrace{(0,\ldots,0)}_{d}$ if $t_k \notin \mathcal{B}$ and $b^{(k)} = \underbrace{(0,\ldots,\underset{\uparrow k.}{1},0,\ldots,0)^T}_{d}$, if $t_k \in \mathcal{B}$.

Now we can compute

$$\sum_{s=1}^{d\cdot|T|} c_{i,s}\cdot b_{s,j} = \sum_{\substack{t_k\in\mathcal{B},\\ j\geq 2}} c_{i,j}^{(k)} \underset{acc.def}{=} \sum_{\substack{t_k\in\mathcal{B},\\ d_k=j-1}} V(t_k,P_i)$$

□

Example 9 *Considering Z_1, $m^{(0)}$, $m^{(1)}$ and $\mathcal{B}$ from Example 3 again, we can verify that*

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix}}_{=m^{(1)}} = \underbrace{\begin{pmatrix} 4 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}}_{m^0} + \underbrace{\begin{pmatrix} -2 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \end{pmatrix}}_{=C} \cdot \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}}_{=B}$$

Definition 12 (Parikh-matrix) *The matrix $\Psi \in \mathcal{M}(|P|,d)$ is called Parikh-matrix of the sequence $\sigma = (\mathcal{B}_1,\ldots,\mathcal{B}_n)$, iff*

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

Theorem 1 (state equation) *Let $Z = (N, D)$ be a DPN, all $d_i > 0$, $\sigma = (\mathcal{B}_1,\ldots,B_n)$ a firing sequence in Z, $m^{(0)}$ the initial time marking of Z and $m^{(0)} \xrightarrow{\mathcal{B}_1} \hat{m}^{(1)} \xrightarrow[1]{} \tilde{m}^{(1)} \xrightarrow{\mathcal{B}_2} \hat{m}^{(2)} \xrightarrow[1]{} \ldots \xrightarrow{\mathcal{B}_n} m^{(n)}$.*

Then it holds:

$$m_n = m^{(0)}\cdot R^{n-1} + C\cdot\Psi_\sigma \tag{3}$$

Proof: by induction on n.
Basis: $n = 1$.
We have to show that for $m^{(0)} \xrightarrow{\mathcal{B}_1} m^{(1)}$ holds:

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

with

$$\Psi_\sigma = \sum_{i=1}^{1} B^{(i)} \cdot R^{n-i} = B^{(1)} \cdot R^0 = B^{(1)}$$

Following, we have to proof that $m^{(1)} = m^{(0)} + C \cdot B^{(1)}$. That is true because of Lemma 2.

Step: We consider the firing sequence $\sigma' = (\sigma, \mathcal{B}_{n+1})$ with $m^{(0)} \longrightarrow \hat{m}^{(n)} \underset{1}{\longrightarrow} \tilde{m}^{(n)} \xrightarrow{\mathcal{B}_{n+1}} \hat{m}^{(n+1)}$.

We have to show that

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

and

$$\Psi_{\sigma'} = \sum_{i=1}^{n+1} B^{(i)} \cdot R^{n+1-i}$$

Because of the induction hypothesis it holds:

$$m^{(n)} = m^{(0)} \cdot R^{n-1} + C \cdot \Psi_\sigma = m^{(0)} \cdot R^{n-1} + C \cdot \left(\sum_{i=1}^{n} B^{(i)} \cdot R^{n-1} \right) \tag{4}$$

Because of Lemma 1 and resp. Lemma 2 it holds too:

$$\tilde{m}^{(n)} = \hat{m}^{(n)} \cdot R \tag{5}$$

resp.

$$\hat{m}^{(n+1)} = \tilde{m}^{(n)} + C \cdot B^{(n+1)} \tag{6}$$

From (4), (5) and (6) it follows:

$$\begin{aligned}
\hat{m}^{(n+1)} &= \tilde{m}^{(n)} + C \cdot B^{(n+1)} \underset{(5)}{=} \hat{m}^{(n)} \cdot R + C \cdot B^{(n+1)} \underset{(4)}{=} \\
&= \left(m^{(0)} \cdot R^{n-1} + C \cdot \left(\sum_{i=1}^{n} B^{(i)} R^{n-1} \right) \right) \cdot R + C \cdot B^{(n+1)} \\
&= m^{(0)} \cdot R^n + C \cdot \left(\sum_{i=1}^{n} B^{(i)} R^{n+1-i} \right) + C \cdot B^{(n+1)} \cdot \underbrace{E_d}_{=R^0} \\
&= m^{(0)} \cdot R^n + C \cdot \left(\sum_{i=1}^{n} B^{(i)} R^{n+1-i} + B^{(n+1)} \cdot R^{(n+1)-(n-1)} \right) \\
&= m^{(0)} \cdot R^n + C \cdot \left(\sum_{i=1}^{n+1} B^{(i)} R^{n+1-i} \right) \\
&= m^{(0)} R^n + C \cdot \Psi_{\sigma'}
\end{aligned}$$

□

Please note, that we call Equation 3 a *state equation* in analogy to time-less petrinets. However, in difference to time-less petrinet, the time marking does not constitute the whole state of the DPN.

4 Nonreachability of Time Markings — An Example

We proved already that in a given Timed Petrinet each reachable time marking fulfills the state equation and the maximal step inequalities, i.e. they are necessary conditions for the reachability of the time marking. As expected, the condition is not sufficient.

In this section we consider an example using the necessity of completion the conditions mentioned above in order to prove the nonreachability of a certain time marking in a given net.

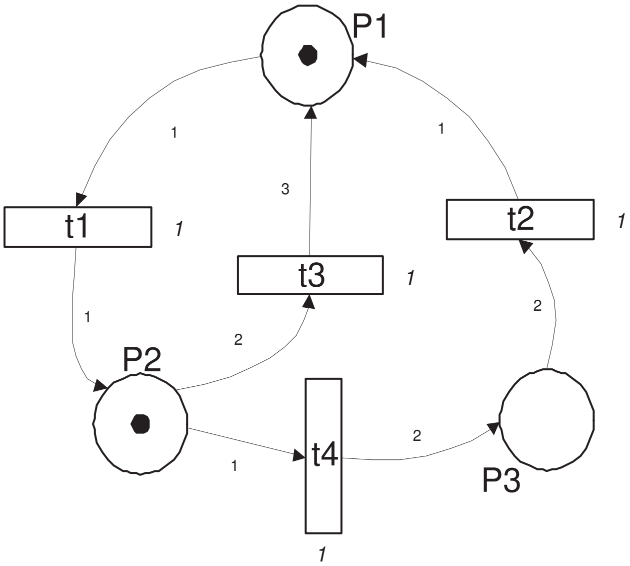

Figure 2: Example net Z_2

Consider Z_2 as in Figure 2. The time marking $m^{(0)}$ is the matrix $m^{(0)} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}$, the incidence matrix C is $C = \begin{pmatrix} -1 & 0 & 0 & 1 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 & -2 & 0 & -1 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$ and the progress matrix R is $R = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$.

Obviously it is true that $R^n = R$ for each $n \geq 1$ ($R^0 = E_2$).

We want to show that the time marking $m^* = \begin{pmatrix} 0 & p^* \\ 2 & q^* \\ 0 & r^* \end{pmatrix}$ is unreachable in Z_2 for each $p^*, q^*, r^* \in \mathbb{R}$. Please note, that this is not true for the time-less net. In the skeleton of Z_2, a firing of $\mathcal{B}_0 = \{t_1\}$ leads immediately to m^*.

Assume that m^* is reachable in Z_2, so it has to fulfill the state equation:

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

for some firing sequence σ and the maximal step inequalities:

$$m_{.1} \not\geq \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \tag{7}$$

$$m_{.1} \not\geq \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix} \tag{8}$$

$$m_{.1} \not\geq \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix} \tag{9}$$

$$m_{.1} \not\geq \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \tag{10}$$

for each reachable time marking, obtained after firing a maximal step, unless the related transition has fired within the last step.

We do not need to consider the whole sequenz σ, but the last marking change. There are two cases: Changing by firing a maximal step and changing by elapsing time. In both cases we consider the last two reached time markings.

Case 1: Last change by time elapsing,
i.e.: $m^{(0)} \xrightarrow{\mathcal{B}_1} \ldots \xrightarrow{\mathcal{B}_n} \hat{m} \underset{1}{\longrightarrow} m^*$.
Then it holds for $\hat{m}$:

$$\begin{aligned} \hat{m} &= m^{(0)} \cdot R^{n-1} + C \cdot \left(\sum_{i=1}^{n} B_i R^{n-i} \right) \\ &= m^{(0)} \cdot \underbrace{R^{n-1}}_{=R} + C \cdot \sum_{i=1}^{n-1} B_i \cdot \underbrace{R^{n-1}}_{=R} + C \cdot B_i \cdot \underbrace{R^0}_{=E_2} \end{aligned}$$

$$= \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} + C \cdot \sum_{i=1}^{n-1} \left(\begin{pmatrix} \alpha_1^i & 0 \\ 0 & \alpha_1^i \\ \alpha_2^i & 0 \\ 0 & \alpha_2^i \\ \alpha_3^i & 0 \\ 0 & \alpha_3^i \\ \alpha_4^i & 0 \\ 0 & \alpha_4^i \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \right) + C \cdot \begin{pmatrix} \kappa & 0 \\ 0 & \kappa \\ \lambda & 0 \\ 0 & \lambda \\ \mu & 0 \\ 0 & \mu \\ \nu & 0 \\ 0 & \nu \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

where

$$\alpha_j^i = \begin{cases} 1 & , t_j \in \mathcal{B}_i, i = 1, \ldots, n \\ 0 & , else \end{cases}$$

and

$$\kappa = \begin{cases} 1 & , t_1 \in \mathcal{B}_n \\ 0 & , else \end{cases} \qquad \lambda = \begin{cases} 1 & , t_2 \in \mathcal{B}_n \\ 0 & , else \end{cases}$$

$$\mu = \begin{cases} 1 & , t_3 \in \mathcal{B}_n \\ 0 & , else \end{cases} \qquad \nu = \begin{cases} 1 & , t_4 \in \mathcal{B}_n \\ 0 & , else \end{cases}$$

$$\hat{m} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix} + C \cdot \begin{pmatrix} x_1 & 0 \\ x_1 & 0 \\ x_2 & 0 \\ x_2 & 0 \\ x_3 & 0 \\ x_3 & 0 \\ x_4 & 0 \\ x_4 & 0 \end{pmatrix} + C \cdot \begin{pmatrix} \kappa & 0 \\ 0 & \kappa \\ \lambda & 0 \\ 0 & \lambda \\ \mu & 0 \\ 0 & \mu \\ \nu & 0 \\ 0 & \nu \end{pmatrix}$$

x_i is the number of occurrences of the transition t_i in the sequence σ at large

$$\hat{m} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} -x_1 + x_2 + 3x_3 & 0 \\ x_1 - 2x_3 - x_4 & 0 \\ -2x_2 + 2x_4 & 0 \end{pmatrix} + \begin{pmatrix} -\kappa & \lambda + 3\mu \\ -2\mu - \nu & \kappa \\ -2\lambda & 2\nu \end{pmatrix} .$$

Hence, we obtain for $\hat{m} = \begin{pmatrix} \hat{\alpha} & \hat{p} \\ \hat{\beta} & \hat{q} \\ \hat{\gamma} & \hat{r} \end{pmatrix}$ for arbitrary $\hat{\alpha}$, $\hat{\beta}$, $\hat{\gamma}$, $\hat{p}$,$\hat{q}$,$\hat{r} \in \mathbb{N}$ that

$$\begin{aligned} \hat{\alpha} &= 1 - x_1 + x_2 + 3x_3 - \kappa \\ \hat{\beta} &= 1 + x_1 - 2x_3 - x_4 - 2\mu - \nu \\ \hat{\gamma} &= -2x_2 + 2x_4 - 2\lambda \\ \hat{p} &= \lambda + 3\mu \\ \hat{q} &= \kappa \\ \hat{r} &= 2\nu \end{aligned} \tag{11}$$

Furthermore, because of $\hat{m} \xrightarrow[1]{} m^*$ it holds $m^* = \hat{m} \cdot R$, i.e.:

$$\begin{pmatrix} 0 & p^* \\ 2 & q^* \\ 0 & r^* \end{pmatrix} = \begin{pmatrix} \hat{\alpha} + \hat{p} & 0 \\ \hat{\beta} + \hat{q} & 0 \\ \hat{\gamma} + \hat{r} & 0 \end{pmatrix} .$$

Following, it is true

$$\hat{\alpha} + \hat{p} = 0$$
$$\hat{\beta} + \hat{q} = 2$$
$$\hat{\gamma} + \hat{r} = 0$$

and therefore

$$\hat{\alpha} = \hat{p} = \hat{\gamma} = \hat{r} = 0$$

Last result, put in (11), leads to $\lambda = \mu = \nu = 0$ and $\kappa = \hat{q} = 1$ or $\kappa = \hat{q} = 0$.
That means:

$$\hat{\beta} = 2 \text{ or } \hat{\beta} = 1 \tag{12}$$

At least, $\tilde{m}$ has to fulfill (7), (8), (9) and (10), i.e.

$$\begin{pmatrix} 0 \\ \hat{\beta} \\ 0 \end{pmatrix} \not\geq \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ \hat{\beta} \\ 0 \end{pmatrix} \not\geq \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix} \quad \begin{pmatrix} 0 \\ \hat{\beta} \\ 0 \end{pmatrix} \not\geq \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ \hat{\beta} \\ 0 \end{pmatrix} \not\geq \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

except those conditions which belong to the transitions including in the step $\mathcal{B}_n$. In case that $\hat{\beta} = 2$ conditions (9) and (10) are not fulfilled. Assuming $\mathcal{B}_n$ includes t_3 and t_4 the conditions (9) and (10) have not to be true. But then it follows that $\mu = \nu = 1$ and this is a contradiction to $\mu = \nu = 0$, computed above. Analogously, in the case that $\hat{\beta} = 1$ the condition (10) is not fulfilled.

Assuming $\mathcal{B}_n$ includes t_4 it follows that $\nu = 1$ and this is a contradiction to $\nu = 0$, as already mentioned.

Therefore, Case 1 can not appear.

Case 2: Last change by firing a maximal step $\mathcal{B}_n$,
i.e. $m^{(0)} \xrightarrow[n-2]{\mathcal{B}_1 \dots \mathcal{B}_{n-1}} \hat{m} \xrightarrow[1]{} \tilde{m} \xrightarrow{\mathcal{B}_n} m^*$.

Analogously to Case 1, we obtain for the time marking $\hat{m} = \begin{pmatrix} \hat{\alpha} & \hat{p} \\ \hat{\beta} & \hat{q} \\ \hat{\gamma} & \hat{r} \end{pmatrix}$ the following:

$$\begin{aligned} \begin{pmatrix} \hat{\alpha} & \hat{p} \\ \hat{\beta} & \hat{q} \\ \hat{\gamma} & \hat{r} \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} -(x_1 - \hat{\kappa}) + (x_2 - \hat{\lambda}) + 3(x_3 - \hat{\mu}) & 0 \\ (x_1 - \hat{\kappa}) - 2(x_3 - \hat{\mu}) - (x_4 - \hat{\nu}) & 0 \\ -2(x_2 - \hat{\lambda}) + 2(x_4 - \hat{\nu}) & 0 \end{pmatrix} + \\ &+ \begin{pmatrix} -\hat{\kappa} & \hat{\lambda} - 3\hat{\mu} \\ -2\hat{\mu} + \hat{\nu} & \hat{\kappa} \\ -2\hat{\lambda} & 2\hat{\nu} \end{pmatrix} \end{aligned} \tag{13}$$

where $\hat{\kappa}, \hat{\lambda}, \hat{\mu}, \hat{\nu} \in \{0,1\}$ are similar defined for the step $\mathcal{B}_{n-1}$ as $\kappa, \lambda, \mu, \nu$ in Case 1; x_1, x_2, x_3, x_4 are the same as in Case 1 and therefore $(x_1 - \hat{\kappa})$, resp. $(x_2 - \hat{\lambda})$, resp. $(x_3 - \hat{\mu})$, resp. $(x_4 - \hat{\nu})$ is the number of occurrence of the transition t_1, resp. t_2, resp. t_3, resp. t_4 in the sequence $(\mathcal{B}_1 \ldots \mathcal{B}_{n-2})$.

For the time marking $\tilde{m} = \begin{pmatrix} \tilde{\alpha} & \tilde{p} \\ \tilde{\beta} & \tilde{q} \\ \tilde{\gamma} & \tilde{r} \end{pmatrix}$ holds

$$\begin{pmatrix} \tilde{\alpha} & \tilde{p} \\ \tilde{\beta} & \tilde{q} \\ \tilde{\gamma} & \tilde{r} \end{pmatrix} = \begin{pmatrix} \hat{\alpha} + \hat{p} & 0 \\ \hat{\beta} + \hat{q} & 0 \\ \hat{\gamma} + \hat{r} & 0 \end{pmatrix} \quad .$$

Because $m^*_{.1} \not\geq t_3^-$ and $m^*_1 \not\geq t_4^-$ do not hold and because we consider nets without self-concurrency of transitions[3], the last step $\mathcal{B}_n$ includes at least the transitions t_3 and t_4, i.e. $\mathcal{B}_n \supseteq \{t_3, t_4\}$, and it holds (corr. remark 2 and $d(t) > 0$ for each $t \in T$) $m^*_{.1} + t_3^- + t_4^- \leq \tilde{m}_{.1}$, i.e.

$$\tilde{m}_{.1} \geq \begin{pmatrix} 0 \\ 5 \\ 0 \end{pmatrix} \tag{14}$$

have to be fulfilled.

From (13) and (14) it follows:

$$5 \leq \hat{\beta} + \hat{q} = (x_1 - \hat{\kappa}) - 2(x_3 - \hat{\mu}) - (x_4 - \hat{\nu}) - 2\hat{\mu} - \hat{\nu} = x_1 - 2x_3 - x_4 - \hat{\kappa} \tag{15}$$

It is easy to see that for the time marking m^* the state equation leads to

$$\begin{pmatrix} 0 & p^* \\ 2 & q^* \\ 0 & r^* \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -x_1 + x_2 + 3x_3 & 0 \\ x_1 - 2x_3 - x_4 & 0 \\ -2x_2 + 2x_4 & 0 \end{pmatrix} + \begin{pmatrix} -\kappa & \lambda + 3\mu \\ -2\mu + \nu & \kappa \\ -2\lambda & 2\nu \end{pmatrix} \quad .$$

In particular, we obtain for

$$m^*_{1,2} = 2 = 1 + x_1 - 2x_3 - x_4 - 2\mu - \nu$$

$$\rightsquigarrow 1 = x_1 - 2x_3 - x_4 - 2\mu - \nu \quad . \tag{16}$$

Furthermore, it is clear that $\mathcal{B} \supseteq \{t_3, t_4\}$ and hence $\mu = \nu = 1$. Thus, it follows from (16):

$$1 = x_1 - 2x_3 - x_4 - 3$$

$$\rightsquigarrow 4 = x_1 - 2x_3 - x_4 \tag{17}$$

[3] In case of self-concurency, Case 2 is obviously trival, since Inequation (7) - (10) must hold in any case.

Putting (17) in (15) leads to $5 \leq 4 - \hat{\kappa}$, i.e. $1 \leq -\hat{\kappa}$, and this is a contradiction to $\hat{\kappa} \in \{0, 1\}$.

Thus, Case 2 is not possible too and following the time marking m^* can not be reached in Z_2 by initial time marking $m^{(0)}$.

$\square$

5 Conclusions

In this paper, we have developed a state equation for DPN and have presented a proving approach that utilizes the state equation.

Although the state equation holds for infinite sequences, its evaluation is limited by the largest duration that appears within the net, and hence, it is always finite.

The presented proving technique is generally applicable. It leads to a system of equations and inequations, and thus, it is always solvable in polynomial time.

In future work, we intend to extend the approach presented here to π-nets [3], allowing description of priorities within Time Petrinets.

Acknowledgments

This work was supported in parts by Microsoft Research Cambridge and in parts by DaimlerChrysler Research and Technology Berlin.

References

[1] C. Ramchandani. Analysis of Asynchronous Concurrent Systems by Timed Petri Nets. *Project MAC-TR 120, MIT*, Febr. 1974.

[2] 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.

[3] J. Richling, L. Popova-Zeugmann, and M. Werner. Verification of non-functional properties of a composable architecture with petrinets. In *Proceedings of the CS&P'2001 Workshop*, 2001.

[4] 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.

[5] P. H. Starke. *INA - Integrated Net Analyzer*. Berlin, 1997. Manual.

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