Marking estimation of Petri nets with silent transitions

Alessandro Giua, Carla Seatzu
Dip. Ingegneria Elettrica ed Elettronica, Università di Cagliari,
Piazza D'Armi, 09123 Cagliari, Italy
e-mail: {giua,seatzu}@diee.unica.it

Daniele Corona
Delft Center for System and Control, Delft University of Technology
Mekelweg 2, 2628 CD Delft, The Netherland
e-mail: d.corona@dcsc.tudelft.nl

Abstract

In this paper we deal with the problem of estimating the marking of a labeled Petri net system based on the observation of transitions labels. In particular, we assume that a certain number of transitions are labeled with the empty string ε, while unique labels taken from a given alphabet are assigned to each of the other transitions. Transitions labeled with the empty string are called *silent* because their firing cannot be observed. Under some technical assumptions on the structure of the unobservable subnet we formally prove that the set of markings consistent with the observed word can be represented by a linear system with a fixed structure that does not depend on the length of the observed word.

I. Introduction

In this paper we address the problem of estimating the marking of a Petri net (PN) whose set of transitions is partitioned in two sets: observable transitions whose firing can be detected by an external observer, and unobservable transitions, i.e., transitions labeled with the empty string ε whose firing cannot be detected [2].

Published as: A. Giua, C. Seatzu, D. Corona, "Marking estimation of Petri nets with silent transitions," *IEEE Trans. on Automatic Control*, Vol. 52, No. 9, pp. 1695-1699, September 2007.

This is a fundamental issue in theoretical *computer science* within the framework of nondeterministic language generators. In fact, in this context, the behaviour of a discrete event system (DES) is modeled by a *language*: the event set E is viewed as an alphabet, and a sequence of events from this alphabet forms a *word* (or a *string*) of events, that describes a particular evolution of the system. The state observer of a DES aims at providing an estimate of the system state based on the observation of the word of events. The initial state is usually assumed to be known but, on the contrary, it may be the case that the system dynamics is not perfectly known in the sense that it may be *nondeterministic*.

More precisely, the nondeterminism may be due to two different facts.

— *Silent events.* There may be events that cause a change in the state of the DES but that are not observable by an outside observer. Events of this kind are labeled with the empty string ε.

— *Indistinguishable events.* There may be events whose occurrence from a given state yields two or more new states. Such is the case if two or more transitions labeled with the same symbol in E are enabled at a given state.

For DES modeled as finite automata, the most common way of solving the problem of partial observation is that of converting, using a standard *determinization* procedure, the nondeterministic finite automaton (NFA) into an equivalent deterministic finite automon (DFA) where: (i) each state of the DFA corresponds to a set of states of the NFA; (ii) the state reached on the DFA after the word w is observed, gives the set $\mathcal{C}(w)$ of *states consistent with the observed word* w.

However, there are some drawbacks in the above procedure. Firstly, each set $\mathcal{C}(w)$ must be exhaustively enumerated. Then, to compute $\mathcal{C}(w)$ we first need to compute $\mathcal{C}(w')$ for all prefixes $w' \preceq w$. Finally, if the NFA has n states, the DFA can have up to 2^n states.

In this paper we explore the possibility of using PN as discrete event models and address the observer design under the assumption that some transitions are labeled with the empty string ε, i.e., they are *silent*, while a different label is assigned to all the other transitions. Thus, if T is the set of transitions and T_ε is the set of silent transitions, all transitions in $T \setminus T_\varepsilon$ are *deterministic*.

We first observe that an analogous determinization procedure as that used in the case of automata, cannot be used in the PN framework. In fact, a nondeterministic PN cannot be converted into an equivalent deterministic PN, because of the strict inclusions [3]:

$$\mathcal{L}_{\text{det}} \subsetneq \mathcal{L} \subsetneq \mathcal{L}_\lambda$$

where

- $\mathcal{L}_{\text{det}}$ is the set of deterministic PN languages;
- $\mathcal{L}$ is the set of λ-free PN languages, namely, languages accepted by nets where no transition is labeled with the empty string: the nondeterminism here is associated to indistinguishable events because two transitions may share the same label;
- $\mathcal{L}_\lambda$ is the set of arbitrary PN languages where a transition may also be labeled with the empty string: the nondeterminism here is associated both to silent events and to indistinguishable events.

If one considers the restricted class of bounded PN (i.e., nets with a finite state space), it is possible to use the above results on automata theory to compute a state observer based on partial event observation. More precisely, we can first construct the reachability graph of the Petri net system, that under the assumption of arbitrary labeling is a NFA G. Then we construct the DFA G' equivalent to the NFA G. Note however that the resulting observer G' is an automaton, not a Petri net, thus all advantages that may derive from initially modeling the DES with a Petri net vanish.

The main contribution of this paper is that of providing an original approach to build a state observer that does not require the construction of the reachability graph, and thus works for both bounded and unbounded PN. More precisely, we derive an efficient technique for characterizing the set of markings that are consistent with the actual observation w, namely $\mathcal{C}(w)$.

In particular, we make the following five assumptions:

(A1) the net structure is known;

(A2) the initial marking is known;

(A3) the labels associated to the firing of transitions in $T \setminus T_\varepsilon$ can be observed, and a different label is associated to each transition;

(A4) the $T_\varepsilon-$induced subnet of N is *acyclic*;

(A5) the $T_\varepsilon-$induced subnet is *backward conflict free*, i.e., any two distinct silent transitions have no common output place.

Note that such assumptions, and in particular (A5), reduce the generality of the proposed results. However, we believe that significant problems within the framework of discrete event systems may be modeled under these assumptions. Moreover, this paper is also a first step towards more general formulations.

Under these assumptions, we show that the set of consistent markings can be written as the solution of a linear system with a fixed structure that depends on the value of a vector $M_b \in \mathbb{N}^m$, called the *basis marking*, that can be recursively computed. In particular, the set of consistent markings can be formulated as the sum of the basis marking and arbitrary effects of silent transitions, provided this sum is non-negative. The main advantage of the proposed approach is that we need not exhaustively enumerate all consistent markings.

We addressed a similar problem in [5], [6]. Note however that in [5], [6] we dealt with λ-free labeled PN, i.e., with PN where no transition is labeled with the empty string, and the nondeterminism was due to indistinguishable events. Under the assumption that the nondeterministic transitions are *contact-free*[1], we gave a linear algebraic characterization of the set of consistent markings that depends on some parameters that can be recursively computed.

Let us finally observe that a similar approach that uses a logical formalism rather than linear programming was also presented by Benasser [1]. This author has studied the possibility of defining the set of markings reached firing a "partially specified" set of transitions using logical formulas, without having to enumerate this set. Other authors [10] have also discussed the problem of estimating the marking of a Petri net using a mix of transition firings and place observations. Zhang and Holloway [12] used a Controlled Petri Net model for forbidden state avoidance under partial *event* observation with the assumption that the initial marking be known. Finally, a notion similar to that of basis marking we introduce in this paper, has already been used by Heymann and Lin in [7]. Here the authors deal with the problem of designing an on-line controller for partially observed DES, that is based on the definition of the *unobserved reach* set of a subset $x_\pi \subseteq X$ that is similar to the definition of the set of consistent markings we use in this paper. In fact, the unobserved reach set of x_π is defined as the set of all states that can be reached from any state $x' \in x_\pi$ by firing sequences of unobserved events.

II. Background on Petri nets

In this section we recall the formalism used in the paper. For more details on Petri nets we address to [11].

[1]Nondeterministic transitions are contact-free if for any two nondeterministic transitions t and t' the set of input and output places of t cannot intersect the set of input and output places of t'.

A *Place/Transition net* (P/T net) is a structure $N = (P, T, Pre, Post)$, where P is a set of m places; T is a set of n transitions; $Pre : P \times T \to \mathbb{N}$ and $Post : P \times T \to \mathbb{N}$ are the pre– and $post$– incidence functions that specify the arcs; $C = Post - Pre$ is the incidence matrix.

A *marking* is a vector $M : P \to \mathbb{N}$ that assigns to each place of a P/T net a non–negative integer number of tokens, represented by black dots. We denote $M(p)$ the marking of place p. A P/T *system* or *net system* $\langle N, M_0 \rangle$ is a net N with an initial marking M_0.

A transition t is enabled at M iff $M \geq Pre(\cdot\,, t)$ and may fire yielding the marking $M' = M + C(\cdot\,, t)$. We write $M\,[\sigma\rangle$ to denote that the sequence of transitions $\sigma = t_{j_1} \cdots t_{j_k}$ is enabled at M, and we write $M\,[\sigma\rangle\, M'$ to denote that the firing of σ yields M'. We also denote $\vec{\sigma} : T \to \mathbb{N}$ the *firing vector* associated to a sequence σ, i.e., $\sigma(t) = k$ if the transition t is contained k times in σ.

A marking M is *reachable* in $\langle N, M_0 \rangle$ iff there exists a firing sequence σ such that $M_0\,[\sigma\rangle\, M$. The set of all markings reachable from M_0 defines the *reachability set* of $\langle N, M_0 \rangle$ and is denoted $R(N, M_0)$. Finally, we denote $PR(N, M_0)$ the *potentially reachable set*, i.e., the set of all markings $M \in \mathbb{N}^m$ for which there exists a vector $\vec{y} \in \mathbb{N}^n$ that satisfies the *state equation* $M = M_0 + C \cdot \vec{y}$, i.e., $PR(N, M_0) = \{M \in \mathbb{N}^m \mid \exists\, \vec{y} \in \mathbb{N}^n : M = M_0 + C \cdot \vec{y}\}$. It holds that $R(N, M_0) \subseteq PR(N, M_0)$.

A Petri net having no directed circuits is called *acyclic*. For this subclass, the following result holds.

Theorem 1. *Let N be an acyclic Petri net.*

(i) If the vector $\vec{y} \in \mathbb{N}^n$ satisfies the equation $M_0 + C \cdot \vec{y} \geq \vec{0}$ there exists a firing sequence σ firable from marking M_0 and such that $\vec{\sigma} = \vec{y}$.

(ii) A marking M is reachable from M_0 if and only if there exists a non negative integer solution $\vec{\sigma}$ satisfying the state equation $M = M_0 + C \cdot \vec{\sigma}$, i.e., $R(N, M_0) = PR(N, M_0)$.

Proof: Note that, obviously, (i) implies (ii). These results follow from Theorem 16 of [11]. In effect, the statement of the theorem in [11] is equivalent to (ii) but the result is proved with an argument that also shows that (i) holds. □

A *labeling function* $L : T \to E \cup \{\varepsilon\}$ assigns to each transition $t \in T$ either a symbol from a given alphabet E or the empty string ε. We extend L to $L : T^* \to E^*$ in the natural way.

We denote as T_ε the set of transitions whose label is ε, i.e., $T_\varepsilon = \{t \in T \mid L(t) = \varepsilon\}$.

In this paper we assume that the same label $e \in E$ cannot be associated to more than one transition. Thus, the labeling function restricted to $T \setminus T_\varepsilon$ is an isomorphism, and with no loss of generality we assume $E = T \setminus T_\varepsilon$.

We denote as w the word of events associated to the sequence σ, i.e., $w = L(\sigma)$. Note that the length of a sequence σ (denoted $|\sigma|$) is always greater than or equal to the length of the corresponding word w (denoted $|w|$). In fact, if σ contains k' transitions labeled ε then $|\sigma| = k' + |w|$.

Moreover, we denote as σ_0 the sequence of null length and ε the empty word. We use the notation $w_i \preccurlyeq w$ to denote the generic prefix of w of length $i \leq k$, where k is the length of w.

Definition 2. *Given a net $N = (P, T, Pre, Post)$, and a subset $T' \subseteq T$ of its transitions, we define the $T'-$*induced subnet of N *as the new net $N' = (P, T', Pre', Post')$ where $Pre', Post'$ are the restriction of $Pre, Post$ to T'. The net N' is obtained from N removing all transitions in $T \setminus T'$. We also write $N' \prec_{T'} N$.* ■

III. Preliminary results

Let $\langle N, M_0 \rangle$ be a net system with incidence matrix $C \in \mathbb{Z}^{m \times n}$ and let $\tilde{M} \in \mathbb{N}^m$. We define

$$\Sigma(N, M_0, \tilde{M}) = \left\{ \vec{y} \in \mathbb{N}^n \mid M_0 + C\vec{y} \geq \tilde{M} \right\}$$

as the set of firing vectors that potentially correspond to sequences that lead from M_0 to a marking greater than or equal to $\tilde{M}$. To simplify the notation, when no ambiguity may result we write Σ to denote this set.

The set $(\Sigma, \leq)$ is a *poset* (partially ordered set) where $\leq$ is the usual relation on $\mathbb{N}^n$ defined as:

$$\vec{y} \leq \vec{y}\,' \qquad \Longleftrightarrow \qquad (\forall j = 1, \ldots, n) \quad y_j \leq y'_j.$$

Given two elements $\vec{y}\,', \vec{y}\,'' \in \Sigma$ we denote by $\oplus$ the componentwise $\min$ operator, i.e.,

$$\vec{y} = \vec{y}\,' \oplus \vec{y}\,'' \quad \Longleftrightarrow \quad (\forall j = 1, \ldots, n) \quad y_j = \min\{y'_j, y''_j\}.$$

Definition 3. *A net $N = (P, T, Pre, Post)$ is said* Backward Conflict Free *(BCF) if any two distinct transitions have no common output place.* ■

Thus, if N is BFC, each place p_i has at most one input transition t_{j_i} as shown in Figure 1.

Theorem 4. *If* $N = (P, T, Pre, Post)$ *is a* backward conflict free *net and if* $\Sigma \neq \emptyset$*, then* $(\Sigma, \leq)$ *has infimal* [2] *element*

$$\vec{y}^{\,\inf} = \bigoplus_{\vec{y} \in \Sigma} \vec{y}.$$

Proof: It is sufficient to show that the set Σ is closed under the $\oplus$ operator. To show this, assume $\vec{y}\,', \vec{y}\,'' \in \Sigma$. Then for all $p_i \in P$ the two vectors satisfy

$$\begin{cases} M_0(p_i) + C(p_i, \cdot)\vec{y}\,' \geq \tilde{M}(p_i) \\ M_0(p_i) + C(p_i, \cdot)\vec{y}\,'' \geq \tilde{M}(p_i). \end{cases} \tag{1}$$

Since N is BCF, then the row $C(p_i, \cdot)$ of the incidence matrix associated to place p_i contains at most one positive element $C(p_i, t_{j_i}) = \alpha_{i,j_i} > 0$, while for all $j \neq j_i$ it holds $C(p_i, t_j) = -\alpha_{i,j} \leq 0$. If no elements of $C(p_i, \cdot)$ is positive, then we define $j_i = n + 1$ and $\alpha_{i,j_i} = 0$.

Thus for all $p_i \in P$ we can rewrite inequalities (1) as follows:

$$\begin{cases} \alpha_{i,j_i} y'_{j_i} \geq \tilde{M}(p_i) - M_0(p_i) + \displaystyle\sum_{j=1, j \neq j_i}^{n} \alpha_{i,j} y'_j \\ \alpha_{i,j_i} y''_{j_i} \geq \tilde{M}(p_i) - M_0(p_i) + \displaystyle\sum_{j=1, j \neq j_i}^{n} \alpha_{i,j} y''_j. \end{cases} \tag{2}$$

Let us now consider a vector $\vec{y} = \vec{y}\,' \oplus \vec{y}\,''$. For all $p_i \in P$ it holds:

$$\begin{aligned} \alpha_{i,j_i} y_{j_i} &= \min\{\alpha_{i,j_i} y'_{j_i}, \alpha_{i,j_i} y''_{j_i}\} \\ &\geq \tilde{M}(p_i) - M_0(p_i) + \\ &\quad + \min\left\{\textstyle\sum_{j=1, j \neq j_i}^{n} \alpha_{i,j} y'_j, \sum_{j=1, j \neq j_i}^{n} \alpha_{i,j} y''_j\right\} \\ &\geq \tilde{M}(p_i) - M_0(p_i) + \sum_{j=1, j \neq j_i}^{n} \alpha_{i,j} y_j, \end{aligned} \tag{3}$$

i.e., $\vec{y} \in \Sigma$. □

Remark 5. *We want to point out where the assumption that* N *be backward conflict free is essential in the previous proof. Assume that a place* p_i *has two input transitions* t_{j_i} *and* t_{k_i}*. Then as we write equation (2) in terms of positive elements we need to write expressions of the form:*

$$\alpha_{i,j_i} y'_{j_i} + \alpha_{i,k_i} y'_{k_i} \geq \tilde{M}(p_i) - M_0(p_i) + \sum_{j=1, j \notin \{j_i, k_i\}}^{n} \alpha_{i,j} y'_j$$

[2]The infimal element of a poset $(A, \preccurlyeq)$ is an element $a^{\inf} \in A$ such that for any another $a' \in A$ it holds $a^{\inf} \preccurlyeq a'$. If the infimal element exists it is unique.

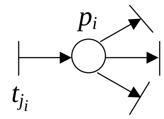

Fig. 1. *A place of a BCF net.*

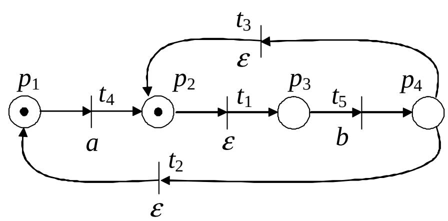

Fig. 2. *The Petri net system considered in Example 7.*

and now when we consider vector $\vec{y}$ it holds

$$\begin{gathered}\alpha_{i,j_i} y_{j_i} + \alpha_{i,k_i} y_{k_i} \leq \\ \min\{\alpha_{i,j_i} y'_{j_i} + \alpha_{i,k_i} y'_{k_i}, \alpha_{i,j_i} y''_{j_i} + \alpha_{i,k_i} y''_{k_i}\} \geq \\ \tilde{M}(p_i) - M_0(p_i) + \sum_{j=1, j \notin \{j_i, k_i\}}^{n} \alpha_{i,j} y_j\end{gathered}$$

i.e., we cannot conclude that $\vec{y} \in \Sigma$. ■

IV. AN ALGEBRAIC CHARACTERIZATION OF THE SET OF CONSISTENT MARKINGS

Let us consider a Petri net system $\langle N, M_0 \rangle$ with labeling function $L : T \to E \cup \{\varepsilon\}$.

Assume that conditions (A1) to (A5) in the Introduction hold.

After the word w of symbols in E has been observed, we define the set $\mathcal{C}(w)$ of w-consistent markings as the set of all markings in which the system may be, given the observed behaviour.

Definition 6. *Given an observed word w, the set of w-*consistent markings *is*

$$\begin{gathered}\mathcal{C}(w) = \{M \in \mathbb{N}^m \mid \exists \textit{ a sequence of transitions } \sigma : \\ M_0[\sigma\rangle M \textit{ and } L(\sigma) = w\}.\end{gathered} \tag{4}$$

■

Example 7. Let us consider the Petri net system in Figure 2 whose initial marking is equal to $M_0 = [1\ 1\ 0\ 0]^T$ and whose alphabet is $E = \{a, b\}$.

Assume that no event is initially observed, i.e., $\sigma = \sigma_0$ and $w = \varepsilon$. By definition, the set of markings that are consistent with the empty word is $\mathcal{C}(\varepsilon) = \{[1\ 1\ 0\ 0]^T,\ [1\ 0\ 1\ 0]^T\}$. In fact two different cases may have occurred: either no transition has fired or the silent transition t_1 has fired.

Now, assume that transition t_4 fires. Its firing can be observed being $L(t_4) = a \in E$. In such a case the set of markings that is consistent with the observed event a is $\mathcal{C}(a) = \{[0\ 2\ 0\ 0]^T$, $[0\ 1\ 1\ 0]^T,\ [0\ 0\ 2\ 0]^T\}$. In fact, five different sequences of transitions σ_i, $i = 1, \cdots, 5$, may have fired, namely, $\sigma_1 = t_4$, $\sigma_2 = t_4 t_1$, $\sigma_3 = t_1 t_4$, $\sigma_4 = t_4 t_1 t_1$, $\sigma_5 = t_1 t_4 t_1$, and for all of them $L(\sigma_i) = a$. Moreover, $M_0[\sigma_1\rangle\ [0\ 2\ 0\ 0]^T$, $M_0[\sigma_2\rangle\ [0\ 1\ 1\ 0]^T$, $M_0[\sigma_3\rangle\ [0\ 1\ 1\ 0]^T$, $M_0[\sigma_4\rangle\ [0\ 0\ 2\ 0]^T$ and $M_0[\sigma_5\rangle\ [0\ 0\ 2\ 0]^T$. ■

A. Main result

We formally prove that under assumptions (A1) to (A5), a fixed number of constraints, not depending on the length of the observed word w, may be used to describe the set of w consistent markings. In particular, we formally prove that:

$$\mathcal{M}(M_{b,w}) \triangleq \{M \in \mathbb{N}^m \mid M = M_{b,w} + C_\varepsilon\ \vec{y},\ \ \vec{y} \in \mathbb{N}^{n_\varepsilon}\} \tag{5}$$

is the set of w consistent markings, i.e., $\mathcal{M}(M_{b,w}) = \mathcal{C}(w)$, where $M_{b,w}$ is appropriately computed using the following recursive algorithm, C_ε is the restriction of the incidence matrix to silent transitions, and n_ε is the number of silent transitions.

Algorithm 8 ($M_{b,w}$ computation)**.**

1. Let $w = \varepsilon$ and $M_{b,w} = M_0$.

2. Wait until an event e is observed, and let t be the transition such that $L(t) = e$.

3. Set $\vec{y}^{\ inf} = \vec{0} \in \mathbb{N}^{n_\varepsilon}$, and $M = M_{b,w} - Pre(\cdot, t)$

While there exists a p_i such that $M(p_i) < 0$ do

(a) Look for the (unique) silent transition $t_{\varepsilon,i} \in^\bullet p_i$

(b) Let $\varrho = \left\lceil \dfrac{-M(p_i)}{Post(p_i, t_{\varepsilon,i})} \right\rceil$

(c) Update $\vec{y}^{\,inf} = \vec{y}^{\,inf} + \varrho\, \vec{e}_{\varepsilon,i}$
where $\vec{e}_{\varepsilon,i}$ is the normal basis
$i-th$ element of $\mathbb{N}^{n_\varepsilon}$.

(d) Update $M = M + \varrho\, C(\cdot, t_{\varepsilon,i})$.

endwhile

Let $M_{b,we} = M_{b,w} + C_\varepsilon\, \vec{y}^{\,inf} + C(\cdot, t)$ and $w = we$.

4. Goto 2. ■

Note that the main idea behind the proposed characterization originates from the consideration that, given the above assumptions (A4) and (A5), we can always describe the set of markings that are consistent with an observed word w as the set of markings that can be reached from a *basis marking* $M_{b,w}$, depending on w, by simply firing silent transitions. Using Algorithm 8 the basis marking $M_{b,w}$ is computed as the marking that is reached from the initial one by firing all the observed deterministic transitions and all those silent transitions whose firing is strictly necessary to enable the observed sequence. Thus, when no transition firing is observed, we take $M_{b,\varepsilon} = M_0$.

As formally proved in the following, the existence and unicity of the basis marking $M_{b,w}$ follows from Theorem 4. In fact, since the $T_\varepsilon-$induced subnet is acyclic, if we consider $\Sigma = \Sigma(N, M_{b,v}, Pre(\cdot, t))$, where $M_{b,v}$ is the basis marking before the last observed transition t, Σ represents the set of firing vectors that correspond to sequences of silent transitions that lead from $M_{b,v}$ to a marking greater than or equal to $Pre(\cdot, t)$, i.e., to a marking that enables t. By Theorem 4 we know for sure that the infimal element $\vec{y}^{\,\mathrm{inf}}$ of Σ exists and is unique. Therefore we update the basis marking taking into account that, before the firing of t, a certain number of silent transitions, corresponding to the firing vector $\vec{y}^{\,\mathrm{inf}}$, have fired to enable t.

We finally remark that the number of executions of *while* at step 3 of Algorithm 8 is less than or equal to the number of transition firings that are necessary to enable the observed transition t.

Example 9. Let us consider again the Petri net system in Figure 2.a. By definition the basis marking when no event is observed is $M_{b,\varepsilon} = M_0$.

Let us first assume that the event a is observed, i.e., transition t_4 has fired. The infimal vector $\vec{y}^{\,inf}$ is null, and according to Algorithm 8, the basis marking is updated to $M_{b,a} =$

$M_{b,\varepsilon} + C(\cdot, t_4) = [0\ 2\ 0\ 0]^T$.

Now, assume that the event b is observed, i.e., transition t_5 has fired. In this case $\vec{y}^{\,inf} = [1\ 0\ 0]^T$ because we know for sure that the silent transition t_1 has fired at least once to enable t_5, and the basis marking is updated to $M_{b,ab} = M_{b,a} + C_\varepsilon \cdot \vec{y}^{\,inf} + C(\cdot, t_5) = [0\ 1\ 0\ 1]^T$. ■

Now, let us prove an important property of acyclic Petri nets that will be useful in the following.

Lemma 10. *Let us consider an* acyclic *Petri net system* $\langle N, M_0 \rangle$. *Assume that two firing sequences* σ' *and* σ'' *are enabled at* M_0 *and assume that* σ'' *is still enabled after the firing of* σ'. *Then* $M_0[\sigma'\sigma''\rangle \bar{M}$ *and* $M_0[\sigma''\rangle M'' \implies (\exists \sigma'_{eq} :\ \vec{\sigma}'_{eq} = \vec{\sigma}')\ \ M''[\sigma'_{eq}\rangle \bar{M}$.

Proof: The first assumption $M_0[\sigma'\sigma''\rangle \bar{M}$ implies that $\bar{M} = M_0 + C \cdot \vec{\sigma}' + C \cdot \vec{\sigma}'' \geq \vec{0}$, with $\vec{\sigma}', \vec{\sigma}'' \geq \vec{0}$, while the second assumption $M_0[\sigma''\rangle M''$ implies that $M'' = M_0 + C \cdot \vec{\sigma}''$. Thus, $M'' + C \cdot \vec{\sigma}' = \bar{M} \geq 0$.

By Theorem 1, item (i), the above equation implies that there exists a firing sequence σ'_{eq} with $\vec{\sigma}' = \vec{\sigma}'_{eq}$ such that $M''[\sigma'_{eq}\rangle \bar{M}$, thus proving the statement. □

The above lemma ensures that if σ'' is enabled after the firing of σ', a sequence σ'_{eq} that is *equivalent* to σ' — in the sense that it is just a permutation of σ' — is enabled after the firing of σ''.

Theorem 11. *Let us consider a Petri net system* $\langle N, M_0 \rangle$ *and let* $L : T \to E \cup \{\varepsilon\}$ *be its labeling function. Assume that assumptions (A4) and (A5) are satisfied. Then, for all words* $w \in (T \setminus T_\varepsilon)^*$ *the equality* $\mathcal{C}(w) = \mathcal{M}(M_{b,w})$ *holds, where* $M_{b,w}$ *is computed using Algorithm 8.*

Proof: We prove this by induction on the length of the observed word.

(Basis Step.) If $w = \varepsilon$ then $M_{b,w} = M_0$ and

$$\begin{aligned} \mathcal{M}(M_{b,\varepsilon}) &= \mathcal{M}(M_0) \\ &= \{M \in \mathbb{N}^m \ \mid\ M = M_0 + C_\varepsilon\ \vec{y},\ \vec{y} \in \mathbb{N}^{n_\varepsilon}\} \\ &\supseteq \{M \in \mathbb{N}^m \ \mid\ M_0[\sigma_\varepsilon\rangle M,\ \sigma_\varepsilon \in {T_\varepsilon}^*\} \\ &= \mathcal{C}(\varepsilon). \end{aligned}$$

If N_ε is acyclic we can replace $\supseteq$ by $=$ according to Theorem 1, item (ii).

(Inductive Step.) Assume that $\mathcal{C}(v) = \mathcal{M}(M_{b,v})$ for a generic word $v \in E^*$.

We prove that $\mathcal{C}(ve) = \mathcal{M}(M_{b,ve})$ with $e \in E$.

We first observe that, if $t = L^{-1}(e)$ then

$$\begin{aligned}
\mathcal{C}(ve) &= \{M'' \in \mathbb{N}^m \mid M \in \mathcal{C}(v),\ M \geq Pre(\cdot,t), \\
&\qquad M[t\rangle M'[\sigma'_\varepsilon\rangle M'',\ \sigma'_\varepsilon \in {T_\varepsilon}^*\} \\
&= \{M'' \in \mathbb{N}^m \mid M \in \mathcal{M}(M_{b,v}),\ M \geq Pre(\cdot,t), \\
&\qquad M[t\rangle M'[\sigma'_\varepsilon\rangle M'',\ \sigma'_\varepsilon \in {T_\varepsilon}^*\} \\
&= \{M'' \in \mathbb{N}^m \mid M = M_{b,v} + C_\varepsilon\ \vec{y},\ \vec{y} \in \mathbb{N}^\varepsilon, \\
&\qquad M \geq Pre(\cdot,t),\ M[t\rangle M'[\sigma'_\varepsilon\rangle M'', \\
&\qquad \sigma'_\varepsilon \in {T_\varepsilon}^*\} \\
&\supseteq \{M'' \in \mathbb{N}^m \mid M_{b,v}[\sigma_\varepsilon\rangle M[t\rangle M'[\sigma'_\varepsilon\rangle M'', \\
&\qquad \sigma_\varepsilon, \sigma'_\varepsilon \in {T_\varepsilon}^*\}.
\end{aligned}$$

If N_ε is acyclic we can replace $\supseteq$ by $=$ according to Theorem 1, item (ii).

Now, let us notice that when a new transition t is observed, using Algorithm 8, we first update the basis marking $M_{b,v}$ to $M'_{b,v} = M_{b,v} + C_\varepsilon\ \vec{y}^{\ \mathrm{inf}}$ where $\vec{y}^{\ \mathrm{inf}}$ is the infimal vector of $\Sigma(N, M_{b,v}, Pre(\cdot,t))$. Moreover, since by assumption the $T_\varepsilon-$induced net is BCF, so by virtue of Theorem 4, $\vec{y}^{\ \mathrm{inf}}$ is unique for all $t \in T \setminus T_\varepsilon$ and for all $M_{b,v} \in \mathbb{N}^m$. Thus by definition $M'_{b,v}$ is the marking that can be obtained from $M_{b,v}$ by simply firing those transitions that are strictly necessary to enable t. Clearly, if $M_{b,v}$ already enables t, then $\vec{y}^{\ \mathrm{inf}} = \vec{0}$.

Furthermore, since N_ε is acyclic,

$$M = M'_{b,v} + C_\varepsilon\ \vec{y} \geq Pre(\cdot,t)$$

implies that

$$\exists\ \sigma_\varepsilon \in {T_\varepsilon}^*\ :\ \vec{\sigma}_\varepsilon = \vec{y}\ \text{ and }\ M'_{b,v}[\sigma_\varepsilon\rangle M[t\rangle M'.$$

Now, we first prove that $\mathcal{C}(ve) \subseteq \mathcal{M}(M_{b,ve})$. In fact, given any firing sequence ${\sigma_\varepsilon}^{\mathrm{inf}}$ that corresponds to the firing vector $\vec{y}^{\,\text{inf}}$, i.e., ${\vec{\sigma}_\varepsilon}^{\text{inf}} = \vec{y}^{\,\text{inf}}$, it holds that

$$\begin{aligned}
& M'' \in \mathcal{C}(ve) \\
& \quad \Leftrightarrow M_{b,v}[{\sigma_\varepsilon}^{\text{inf}}\rangle M'_{b,v}[\sigma_\varepsilon\rangle M[t\rangle M'[\sigma'_\varepsilon\rangle M'' \\
& \quad \Rightarrow \text{ by lemma 10, } (\exists \sigma_{\varepsilon,eq} \text{ with } \vec{\sigma}_{\varepsilon,eq} = \vec{\sigma}_\varepsilon) \\
& \quad\quad M_{b,v}[{\sigma_\varepsilon}^{\text{inf}}\rangle M'_{b,v}[t\rangle M_{b,ve}[\sigma_{\varepsilon,eq}\rangle M'[\sigma'_\varepsilon\rangle M'' \\
& \quad \Rightarrow M_{b,ve}[\sigma_{\varepsilon,eq}\rangle M'[\sigma'_\varepsilon\rangle M'' \\
& \quad \Leftrightarrow M_{b,ve}[\sigma''_\varepsilon\rangle M'', \;\; \sigma''_\varepsilon = \sigma_{\varepsilon,eq}\ \sigma'_\varepsilon \\
& \quad \Leftrightarrow M'' = M_{b,ve} + C_\varepsilon\ \vec{\sigma}''_\varepsilon \\
& \quad \Leftrightarrow M'' \in \mathcal{M}(M_{b,ve}).
\end{aligned}$$

We finally prove that $\mathcal{M}(M_{b,ve}) \subseteq \mathcal{C}(ve)$. In fact,

$$\begin{aligned}
M'' \in \mathcal{M}(M_{b,ve}) \;\; & \Leftrightarrow M'' = M_{b,ve} + C_\varepsilon \vec{y}\,' \\
& \Leftrightarrow \;\text{(by assumption (A4))} \\
& \quad\; \exists \sigma'_\varepsilon \in T^*_\varepsilon \;\;:\;\; M_{b,ve}[\sigma'_\varepsilon\rangle M'' \\
& \Leftrightarrow M_{b,v}[{\sigma_\varepsilon}^{\text{inf}}\rangle M'_{b,v}[t\rangle M_{b,ve}[\sigma'_\varepsilon\rangle M'', \\
& \quad\; M_{b,v} \in \mathcal{C}(v)
\end{aligned}$$

where ${\sigma_\varepsilon}^{\text{inf}}$ is any firing sequence such that ${\vec{\sigma}_\varepsilon}^{\text{inf}} = \vec{y}^{\,\text{inf}}$. Therefore by definition $M'' \in \mathcal{C}(ve)$, thus proving the statement. □

Example 12. Let us consider again the Petri net system in Figure 2.a. In the previous Example 9 we computed that $M_{b,a} = [0\ 2\ 0\ 0]^T$. This means that $\mathcal{M}(M_{b,a}) = \{M \in \mathbb{N}^m \mid M = M_{b,a} + C_\varepsilon\ \vec{y}, \;\; \vec{y} \in \mathbb{N}^3\}$ is the set of consistent markings. The above set can be also be rewritten as $\mathcal{M}(M_{b,a}) = \{M \in \mathbb{N}^m \mid M = [y_2 \;\; 2 - y_1 + y_2 \;\; y_1 \;\; - y_2 - y_3]^T, \; [y_1\ y_2\ y_3]^T \in \mathbb{N}^3\}$, thus $y_1 \in \{0, 1, 2\}$, $y_2 = y_3 = 0$, and $\mathcal{M}(M_{b,a}) = \{[0\ 2\ 0\ 0]^T, [0\ 1\ 1]^T, [0\ 0\ 2\ 0]^T\}$ that coincides with the set of consistent markings computed via the DFA in Figure 2.c. The same reasoning can be repeated for any other word of events. ■

Remark 13. *Given the characterization of the set of markings consistent with an observation w in equation (5) and a marking $\bar{M}$, it is easy to establish if $\bar{M}$ is reachable or not after the observation w. To this aim we need to check if the following constraint set of n_ε integer* *unknowns (the vector $\vec{y}$) is feasible:*

$$\begin{cases} \bar{M} = M_{b,w} + C\vec{y} \\ \vec{y} \in \mathbb{N}^{n_\varepsilon} \end{cases} \tag{6}$$

This can be easily done by simply solving a linear integer programming problem with unknowns M and $\vec{y}$, constraint set (6) and any linear performance index involving M. ■

V. Conclusions and future work

The main contribution of this paper is that of providing a marking estimation procedure for nondeterministic labeled Petri nets, where the nondeterminism is due to the presence of transitions labeled with the empty sting ε. Under some technical assumptions on the structure of the $T_\varepsilon-$induced net (i.e., it is acyclic and backward conflict free), we formally proved that the set of markings consistent with an observed word can be described by a constraint set of linear inequalities that has a fixed structure that does not change as the length of the observed sequence increases.

We plan to extend our results in several ways. Firstly, we plan to modify the structure of the constraint set to also take into account the case that the initial marking is not known. Then we want to extend this approach taking simultaneously into account the case in which the nondeterminism is due to silent transitions and the case of nondeterministic transitions that share the same label.

References

[1] A. Benasser, "Reachability in Petri nets: an approach based on constraint programming" (in French), *Ph.D. Thesis*, Université de Lille 1, 2000.

[2] D. Corona, A. Giua, C. Seatzu "Marking estimation of Petri nets with silent transitions," *43rd IEEE Conf. on Decision and Control*, pp. 966-971, Dec. 2004.

[3] S. Gaubert, A. Giua, "Petri net languages and infinite subsets of $\mathbb{N}^m$," *J. of Computer and System Sciences*, Vol. 59, No. 3, pp. 373-91, Dec. 1999.

[4] A. Giua, C. Seatzu, "Observer based state-feedback control of timed Petri nets with deadlock recovery," *IEEE Trans. on Automatic Control*, Vol. 49, No. 1, pp. 17-29, Jan. 2004.

[5] A. Giua, J. Júlvez, C. Seatzu, "Marking estimation of Petri nets with pairs of nondeterministic transitions," *Asian Journal of Control*, Special Issue on the "Control of Discrete Event Systems", Vol. 6, No. 2, pp. 270-280, 2004.

[6] A. Giua, D. Corona, C. Seatzu, "State Estimation of λ-free Labeled Petri Nets with Contact-Free Nondeterministic Transitions," *Journal of Discrete Event Dynamic Systems*, Vol. 15, No. 1, pp. 85-108, 2005.

[7] M. Heymann, F. Lin, "On-line control of partially-observed discrete-event systems," *J. of Discrete Event Dynamic Systems*, Vol. 4, No. 3, pp. 221–236, 1994.

[8] C.A.R Hoare, *Communicating Sequential Processes*, Prentice Hall 1985.

[9] J.E. Hopcroft, J.D. Ullman, *Introduction to Automata Theory, Languages, and Computation*, Addison-Wesley, 1979.

[10] M.E. Meda, A. Ramírez, A. Malo, "Identification in discrete event systems," *Proc. IEEE Int. Conf. on Systems, Man and Cybernetics*, San Diego, CA, pp. 740–5, Oct. 1998.

[11] T. Murata, "Petri nets: properties, analysis and applications," *Proc. IEEE*, Vol. 77, No. 4, pp. 541–580, 1989.

[12] L. Zhang, L.E. Holloway, "Forbidden state avoidance in controlled Petri nets under partial observation," *33rd Allerton Conference*, Monticello, Illinois, pp. 146–155, 1995.