Marking Estimation of Petri Nets based on Partial Observation

Alessandro Giua (†), Jorge Júlvez (‡)[1], Carla Seatzu (†)
(†) Dip. di Ingegneria Elettrica ed Elettronica, Università di Cagliari, Italy
{giua,seatzu}@diee.unica.it
(‡) Dep. de Inf. e Ing. de Sistemas, Centro Politécnico Superior, Universidad de Zaragoza, Spain
julvez@posta.unizar.es

Abstract

We present a technique for estimating the marking of a Petri net based on the observation of transition labels. In particular, the main contribution of the paper consists in deriving a methodology that can handle the case of nondeterministic transitions, i.e., transitions that share the same label. Under some technical assumptions, the set of markings consistent with an observation can be represented by a linear system with a fixed structure that does not depend on the length of the observed word. The validity of the proposed methodology is illustrated in detail through a numerical example.

1 Introduction

This paper deals with the problem of estimating the marking of a Place/Transition (P/T) net based on the observation of transition firings. The problem of estimating the state of a dynamic system is a fundamental issue in system theory and the construction of state observers for time-driven systems is treated in most linear systems textbooks. Although less popular in the case of discrete–event systems, the issue of state estimation under partial state observation has been discussed in the literature. For systems represented as finite automata, Ramadge [12] was the first to show how an observer could be designed for a partially observed system. Caines *et al.* [2] showed how it is possible to use the information contained in the past sequence of observations (given as a sequence of observation states and control inputs) to compute the set of consistent states, while in [3] the observer output is used to steer the state of the plant to a desired terminal state. A similar approach was also used by Kumar *et al.* [7] when defining observer based dynamic controllers in the framework of supervisory predicate control problems. Özveren and Willsky [10] proposed an approach for building observers that allows one to reconstruct the state of finite automata after a word of bounded length has been observed, showing that an observer may have an exponential number of states.

Let us define the set of *states consistent with the observed behavior* as the states in which the system may actually be given the observation. There are two main drawbacks in the above mentioned automata based approaches to the design of a discrete event observer. Firstly, the set of consistent states must explicitly be enumerated. Secondly, to compute the set of consistent states at step k it is not usually sufficient to know the new observation and the set of consistent states at step $k-1$, but it is necessary to recompute this set as a function of all previous observations.

Looking for more efficient approaches that do not require the enumeration of this set, we explored the possibility of using Petri nets as discrete event models [5, 6]. We showed that under the following three assumptions: (A1') the net structure is known; (A2') the initial marking is not known or is only known to belong to an initial macromarking, i.e., a given linear convex set; (A3') all transition firings can be observed; it is possible to represent the set of consistent markings (i.e., the states of the Petri net) as the solution of a linear system that has a fixed structure which only depends on two parameters (the estimate and the bound) that can be recursively computed. Note that other authors [8] have also discussed the problem of estimating the marking of a Petri net using a mix of transition firing and place observations.

In this paper, we further extend the approach of [5, 6] relaxing what we felt was its major limitation, i.e., the assumption (A3') that all transition firings can be observed. In fact, we assume that to each transition t is associated a label $L(t)$ and two or more transitions may have the same label. When t fires, only its label $L(t)$ is observed and this may introduce nondeterminism in the observer, in the sense that the observed word is not sufficient to reconstruct the transition firing and thus the actual marking. Note, however, that in this paper we restrict assumption (A2') assuming that the initial marking is perfectly known. In effect, this may not be strictly necessary but we need it in this paper to simplify the results we present.

In a first part of the paper, we show a rather simple result: using the net state equation it is possible to represent the set of consistent markings as the solution of a linear system that can be recursively computed, but whose structure, unfortunately, is not fixed: it grows linearly with the length of the observed word. 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" step of transitions using logical formulas, without having to enumerate this set.

In a second part of the paper, we propose a different approach that, under some technical assumptions, allows us to characterize the set of consistent markings as the solution of a different linear system with a fixed structure that depends on some parameters (the upper bounds u's) that can be recursively computed. In particular, we make some restrictions on the structure of the labeling function and we assume that the same label cannot be assigned to more than two transitions. Moreover, we assume that nondeterministic transitions (i.e., transitions whose label is also associated to other transitions) should also be *contact free*, i.e., if t and t' are nondeterministic transitions the set of input and output places of t cannot intersect the set of input and output places of t'. The validity of the proposed characterization has been formally proved and is illustrated in detail through a numerical example.

[1] Supported by a grant from D.G.A. REF B106/2001

0-7803-7896-2/03/$17.00 ©2003 IEEE

2 Background on Petri nets

In this section we recall the formalism used in the paper. For more details on Petri nets we address to [9].

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. The *preset* and *postset* of a node $X \in P \cup T$ are denoted ${}^\bullet X$ and $X^\bullet$ while ${}^\bullet X^\bullet = {}^\bullet X \cup X^\bullet$.

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 $M' = M + C(\cdot, t)$.

A *labeling function* $L : T \to E$ assigns to each transition $t \in T$ a symbol from a given alphabet E. Note that the same label $e \in E$ may be associated to more than one transition. Using the notation of [11] and [4] we say that the labeling function is *λ-free.* In the following we say that a transition t is *nondeterministic* if its label is also associated to other transitions, otherwise a transition t is said to be *deterministic.* We also denote T^d the set of deterministic transitions and T^n the set of nondeterministic transitions. Clearly, $T = T^d \cup T^n$. For simplicity of notation, we assume that the transition enumeration is such that $T^n = \{t_j \mid j = 1, \cdots, n^n\}$ and $T^d = \{t_j \mid j = n^n + 1, \cdots, n\}$, where $n^n = |T^n|$. Analogously, we say that an event e is deterministic if there exists only one transition t such that $L(t) = e$, otherwise we say that the event e is nondeterministic. Therefore, with no ambiguity on the notation, we may write $E = E^d \cup E^n$.

We denote as T_e the set of transitions labeled e, i.e, $T_e = \{t \in T \mid L(t) = e\}$. Moreover, we denote as $\vec{s}_e \in \{0, 1\}^n$ the characteristic vector of T_e, i.e., $\vec{s}_e(i) = 1$ if $L(t_i) = e$, and $\vec{s}_e(i) = 0$ otherwise.

We write $M\ [\sigma\rangle\ M'$ to denote that the enabled sequence of transitions σ may fire at M yielding M'. We denote as w the word of events associated to the sequence σ, i.e., $w = L(\sigma)$. Moreover, we denote as σ_0 the sequence of null length and w_0 the empty word. Finally, 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. In particular, for $i = 0$, we have by definition the empty word, $w_0 = \varepsilon$.

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 $R(N, M_0)$.

3 Problem statement

In this paper we deal with the problem of estimating the marking of a net system $\langle N, M_0 \rangle$ whose marking cannot be directly observed. The following properties of the system will be assumed.

(A1) The structure of the net N is known.

(A2) The initial marking M_0 is known.

(A3) Labels associated to transition firings can be observed.

After the word w 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 1. Given an observed word w, the set of *w-consistent markings* is $\mathcal{C}(w) = \{M \in \mathbb{N}^m \mid \exists$ a sequence of transitions $\sigma : M_0[\sigma\rangle M$ and $L(\sigma) = w\}$. ■

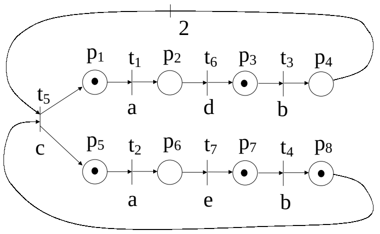

Figure 1: Petri net system that can only be partially observed

Our goal is that of providing a systematic and efficient procedure to estimate the set of markings that are consistent with an observed word.

Clearly, $\mathcal{C}(w_0) = M_0$ and $\mathcal{C}(w)$ is a singleton if for all e in w, T_e is a singleton. On the contrary, the degree of nondeterminism may increase as the cardinality of T_e increases.

Finally, let us observe through a simple example, that the cardinality of the set of consistent markings may either increase or decrease as the length of the observed word increases.

Example 2. Let us consider the Petri net system in figure 1 where $T^d = \{t_5, t_6, t_7\}$ and $T^n = \{t_1, t_2, t_3, t_4\}$. More precisely, $T_a = \{t_1, t_2\}$, $T_b = \{t_3, t_4\}$, $T_c = \{t_5\}$, $T_d = \{t_6\}$, and $T_e = \{t_7\}$.

Clearly when no event has been observed, $\mathcal{C}(\varepsilon) = \{[1\ 0\ 1\ 0\ 1\ 0\ 1\ 1]^T\}$. Let us first assume that the event b is observed. Given the initial marking M_0, either t_3 or t_4 may have been fired, thus $\mathcal{C}(b) = \{[1\ 0\ 0\ 1\ 1\ 0\ 1\ 1]^T, [1\ 0\ 1\ 0\ 1\ 0\ 0\ 2]^T\}$.

Now, let a be the next observed event. Label a is associated to transitions t_1 and t_2 and both transitions are enabled at both markings in $\mathcal{C}(b)$. Therefore, $\mathcal{C}(ba) = \{[0\ 1\ 0\ 1\ 1\ 0\ 1\ 1]^T, [1\ 0\ 0\ 1\ 0\ 1\ 1\ 1]^T, [0\ 1\ 1\ 0\ 1\ 0\ 0\ 2]^T, [1\ 0\ 1\ 0\ 0\ 1\ 0\ 2]^T\}$.

Now, if d is observed, we may be sure that neither $[1\ 0\ 0\ 1\ 0\ 1\ 1\ 1]^T$ nor $[1\ 0\ 1\ 0\ 0\ 1\ 0\ 2]^T$ in $\mathcal{C}(ba)$ may have been reached because none of these markings enables t_6. Thus, $\mathcal{C}(bad) = \{[0\ 0\ 1\ 1\ 1\ 0\ 1\ 1]^T, [0\ 0\ 2\ 0\ 1\ 0\ 0\ 2]^T\}$.

If b is observed again, both transitions t_3 and t_4 may have fired from the first marking in $\mathcal{C}(bad)$, while only transition t_3 may have fired from the second marking. Thus $\mathcal{C}(badb) = \{[0\ 0\ 0\ 2\ 1\ 0\ 1\ 1]^T, [0\ 0\ 1\ 1\ 1\ 0\ 0\ 2]^T\}$.

Finally, if we observe the deterministic event c we can conclude that only the first marking in $\mathcal{C}(badb)$ is compatible with the last observation, thus the actual marking of the net is completely reconstructed and $\mathcal{C}(badbc) = \{[1\ 0\ 0\ 0\ 2\ 0\ 1\ 0]^T\}$. ■

4 Computation of the set of consistent markings

We first present a recursive algorithm strictly based on the definition of the set of consistent markings $\mathcal{C}(w)$, then we provide an algebraic characterization of $\mathcal{C}(w)$.

Algorithm 3.

```
1. Let $\mathcal{C}(w_0) = M_0$.
2. Let $i = 0$.
3. Wait until a new event $e$ is observed.
4. Let $i = i + 1$.
5. Let $w_i = w_{i-1}e$.
6. Let $\mathcal{C}(w_i) = \emptyset$.
7. For all $M \in \mathcal{C}(w_{i-1})$ do
       For all $t$ such that $M[t\rangle$ and $L(t) = e$
           compute $M' = M + C(\cdot, t)$ and let $\mathcal{C}(w_i)$
               $= \mathcal{C}(w_i) \cup M'$.
8. Goto 3.                                                    ■
```

Clearly, the main disadvantage of the above iterative algorithm is that to compute the set of markings that are consistent with an observed word w of cardinality k, we preliminary need to compute the set of markings that are consistent with all prefixes $w_i \preccurlyeq w$, $i = 1, \cdots, k-1$. A solution to this problem consists in using a linear algebraic characterization of the set of consistent markings.

Proposition 4. Let $\langle N, M_0 \rangle$ be a net system and $w = e_1, \cdots, e_k$ be an observed word. The set of w-consistent markings is given by:

$$\begin{array}{lll} \mathcal{C}(w) = \{M^{(k)} \in \mathbb{N}^m \mid & & \\ \quad \vec{1}^T \cdot \vec{\sigma}^{(i)} = 1 & i = 1, \cdots k & (a) \\ \quad \vec{s}_{e_i} \cdot \vec{\sigma}^{(i)} = 1 & i = 1, \cdots k & (b) \\ \quad M^{(i-1)} \geq Pre \cdot \vec{\sigma}^{(i)} & i = 1, \cdots k & (c) \\ \quad M^{(i)} = M^{(i-1)} + C \cdot \vec{\sigma}^{(i)} & i = 1, \cdots k & (d) \\ \quad \vec{\sigma}^{(i)} \in \{0,1\}^n & i = 1, \cdots k\} & (e) \end{array}$$

where $M^{(0)} = M_0$ and $\vec{1}$ is the n-dimensional column vector of 1's.

Proof: It follows from the definition of the set of consistent markings. In fact, for any observed event e_i, we introduce an unknown vector $\vec{\sigma}^{(i)}$ of zeros and ones (constraint (e)) representing the firing vector associated to the observed event. Then, the first constraint (a) imposes that when the event e_i is observed, only one transition has fired and the second constraint (b) states that the label of that transition should be equal to the observed event. Moreover, if a transition has fired, then it should be enabled by at least one marking in the set $\mathcal{C}(w_{i-1})$ (inequality (c)) and its firing brings to a new marking that is given by constraint (d). □

Example 5. Let us consider again the net system depicted in fig. 1. Let us assume that the observed event is b. By virtue of Proposition 4 we may write: $\mathcal{C}(b) = \{M^{(1)} \in \mathbb{N}^8 \,|\, \vec{1}^T \cdot \vec{\sigma}^{(1)} = 1,\ \sigma_3^{(1)} + \sigma_4^{(1)} = 1,\ M^{(0)} \geq Pre \cdot \vec{\sigma}^{(1)},\ M^{(1)} = M^{(0)} + C \cdot \vec{\sigma}^{(1)},\ \vec{\sigma}^{(1)} \in \{0,1\}^7\}$ where $M^{(0)}$ is the initial marking. Now, let a be the next observed event. Using Proposition 4 we may conclude that $\mathcal{C}(ba) = \{M^{(2)} \in \mathbb{N}^8 \,|\, \vec{1}^T \cdot \vec{\sigma}^{(1)} = 1,\ \sigma_3^{(1)} + \sigma_4^{(1)} = 1,\ M^{(0)} \geq Pre \cdot \vec{\sigma}^{(1)},\ M^{(1)} = M^{(0)} + C \cdot \vec{\sigma}^{(1)},\ \vec{\sigma}^{(1)} = \{0,1\}^7,\ \vec{1}^T \cdot \vec{\sigma}^{(1)} = 1,\ \sigma_1^{(2)} + \sigma_2^{(2)} = 1,\ M^{(1)} \geq Pre \cdot \vec{\sigma}^{(2)},\ M^{(2)} = M^{(1)} + C \cdot \vec{\sigma}^{(2)},\ \vec{\sigma}^{(2)} \in \{0,1\}^7\}$ ■

This example clearly shows that, even if Proposition 4 enables us to directly describe the set of consistent markings without iterating on the sets of markings that are consistent with the prefixes of the observed word, it still presents a significant drawback. In fact, both the number of unknowns and the number of constraints increase as the length of the observed word increases.

The main goal of this paper is that of investigating whether it is possible to define the set of w-consistent markings using a fixed (even if large) number of constraints. A general solution to this problem has not been determined yet. But the wide variety of scenarios we dealt with, enables us to conclude that this possibility is mainly related to the degree of contact of nondenministic transitions and to the number of transitions with the same label.

Now, we derive some restrictive assumptions under which it is possible to prove that the set of consistent markings may be expressed with a fixed number of constraints.

5 The contact-free case

In this section we assume that the following two conditions are verified:

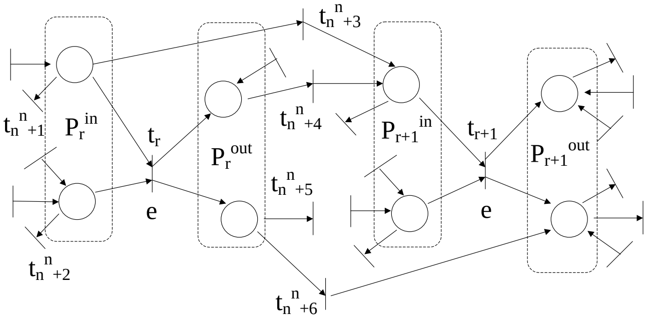

Figure 2: The generic couple of nondeterministic transitions t_r and t_{r+1}.

(A4) for each label $e \in E$ there are at most two transitions such that $L(t) = e$, or equivalently, $|T_e| \leq 2$;

(A5) nondeterministic transitions are contact free, i.e., for any two nondeterministic transitions t_i and t_j, it holds that $^\bullet t_i^\bullet \cap {}^\bullet t_j^\bullet = \emptyset$.

Note that, given assumption (A4), we always assume that the transition enumeration is such that $L(t_r) = L(t_{r+1})$ for $r = 1, 3, \cdots n^n - 1$.

In the following we formally prove that under the above assumptions, 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:

$$\begin{array}{llll} \mathcal{C}(w) = \{M \in \mathbb{N}^m \mid & M = M_0 + C\vec{\sigma}, & & \\ \quad \sigma_r \leq u_r & r = 1, 2, \cdots, n^n & (a) & \\ \quad \sigma_r + \sigma_{r+1} = n_r & r = 1, 3, \cdots, n^n - 1 & (b) & (1) \\ \quad \sigma_q = n_q & q = n^n + 1, \cdots, n & (c) & \\ \quad \vec{\sigma} \in \mathbb{N}^n\} & & (d) & \end{array}$$

is the set of w consistent markings where the upper bounds u_r's are appropriately computed and n_r (n_q) denotes the number of times a nondeterministic (deterministic) event $L(t_r)$ ($L(t_q)$) has been observed.

Note that any vector $\vec{\sigma}$ satisfying constraints (a) to (d) of eq. (1) represents an admissible firing vector associated to a sequence of transitions σ that may have fired and whose labeling is equal to the observed word w, i.e., $L(\sigma) = w$.

For any couple of nondeterministic transitions t_r and t_{r+1} we have 3 constraints: for each transition we need an upper bound on the number of times it may have fired, plus an additional constraint keeping into account the total number of times the corresponding nondeterministic event $L(t_r) = L(t_{r+1})$ has been observed (n_r). On the contrary, for each deterministic transition t_q we only need one constraint, because we exactly know how many times it has fired.

Looking at hypothesis (A4) and (A5) we may conclude that for each couple of nondeterministic transitions, the nets we are dealing with contain "nondeterministic" subnets whose structure is like that one shown in fig. 2, where weights associated to arcs are not required to be ordinary.

In the following page we have reported the algorithm that enables us to compute the upper bounds u_r's used in eq. (1).

The main idea behind this algorithm is that of evaluating the upper bounds u_r's on the base of the knowledge of two parameters associated to nondeterministic transitions. The first one is z_r^{in} that represents the enabling degree of transition t_r assuming that it has never fired. This parameter is used to update the upper bound u_r when one of the following two cases occur.

Algorithm 6 (Upper bounds computation).

```
1. Let $u_r = 0$ for all $r = 1, \cdots, n^n$.
2. Let $n_q = 0$ for all $q = n^n + 1, \cdots, n$.
3. Wait until an event $e$ is observed.
4. If $e \in E^d$, then
     let $t_q$ be such that $t_q \in T^d$ and $L(t_q) = e$
     $n_q = n_q + 1$
     if $t_q \in (^\bullet T^n)^\bullet$, then
         for every $r \in \{1, \ldots, n^n\}$ such that $t_r \in (^\bullet t_q)^\bullet$, do
             $z_r^{in} = \left\lfloor \min_{p \in ^\bullet t_r} \left\{ \frac{M_0(p) + \sum_{t_q \in ^\bullet p \cap T^d} n_q \cdot Post(p, t_q) - \sum_{t_q \in p^\bullet \cap T^d} n_q \cdot Pre(p, t_q)}{Pre(p, t_r)} \right\} \right\rfloor$
             $u_r = \min(u_r, z_r^{in})$
         endfor
     endif
     if $t_q \in (T^{n\bullet})^\bullet$, then
         for every $r \in \{1, \ldots, n^n\}$ such that $t_r \in^\bullet (^\bullet t_q)$, do
             $z_r^{out} = \left\lceil \max_{p \in t_r^\bullet} \left\{ \frac{\sum_{t \in p^\bullet \cap T^d} n_q \cdot Pre(p, t_q) - M_0(p) - \sum_{t \in ^\bullet p \cap T^d} n_q \cdot Post(p, t_q)}{Post(p, t_r)} \right\} \right\rceil$
             $u_{\bar{r}} = \min(u_{\bar{r}}, n_r - z_r^{out})$ where $\bar{r} = r + 1$ if $r$ is odd, else $\bar{r} = r - 1$
         endfor
     endif
5. If $e \in E^n$ then
     for every $r$ such that $L(t_r) = e$ do
         $z_r^{in} = \left\lfloor \min_{p \in ^\bullet t_r} \left\{ \frac{M_0(p) + \sum_{t_q \in ^\bullet p \cap T^d} n_q \cdot Post(p, t_q) - \sum_{t_q \in p^\bullet \cap T^d} n_q \cdot Pre(p, t_q)}{Pre(p, t_r)} \right\} \right\rfloor$
         $u_r = \min(u_r + 1, z_r^{in})$
     endfor
   endif
6. Goto 3.                                                              ■
```

— If a deterministic transition t_q fires and $t_q \in (^\bullet t_r)^\bullet$ (see t_{n^n+1}, t_{n^n+2} and t_{n^n+3} in fig. 2), the value of z_r^{in} may decrease because we know for sure that some token(s) in P_r^{in} were still available to enable t_q. Thus, by definition of z_r^{in}, we may conclude that t_r may have fired at most z_r^{in} times.

— A nondeterministic event e is observed and t_r is a transition whose label is e. In such a case, the value of z_r^{in} keeps the same and by definition of z_r^{in} we may conclude that t_r may have fired at most z_r^{in} times.

The second parameter used to compute the upper bounds is z_r^{out}. It is a measure of the number of tokens that have been removed from the output places to t_r by firing deterministic transitions exiting P_r^{out} (see t_{n^n+4}, t_{n^n+5} and t_{n^n+6} in fig. 2). In particular, the value of z_r^{out} is equal to the minimum number of times transition t_r has to be fired to fulfill the token demands of the transitions exiting P_r^{out}. Consequently, it enables us to evaluate which is the maximum number of times transition t_{r+1} may have fired, namely u_{r+1}. Analogously, the value of z_{r+1}^{out} enables us to update the upper bound u_r.

Example 7. Let us consider the ordinary Petri net system in figure 3. There are only two nondeterministic transitions whose label is a.

The upper bounds u_1 and u_2 may be updated as a consequence of three different types of observed events.

(1) If the first observed event is a, the upper bounds should be both updated to $u_1 = u_2 = 1$ being $z_1^{in} = z_2^{in} = 2$ and the initial bounds equal to zero. We are in the case of step 5 of Algorithm 6.

(2) If a is observed again, we are once again in the case of step 5 of Algorithm 6. The upper bounds are updated to $u_1 = u_2 = 2$ being $z_1^{in} = z_2^{in} = 2$ and the previous bounds equal to one.

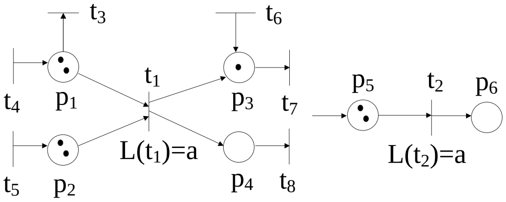

Figure 3: The Petri net system considered in example 7.

Now, let us assume that $L(t_3)$ is observed, thus $n_3 = 1$ and $z_1^{in} = 1$. This means that for sure t_1 has fired at most one time, otherwise t_3 would have not been enabled. Thus the upper bound of t_1 is updated to $u_1 = 1$. We are in the first *if* case of step 4 of Algorithm 6 being t_3 an output transition to one input place of t_1.

(3) Now, let us assume that $L(t_8)$ is observed, thus $w = aa\ L(t_3)\ L(t_8)$. This implies that t_1 should have fired at least once, and consequently t_2 should have fired at most once. In fact, in such a case $n_8 = 1$, $z_1^{out} = 1$ and consequently $u_2 = 1$. We are in the second *if* case of step 4 of Algorithm 6. ■

Lemma 8. Let us consider a Petri net system $\langle N, M_0 \rangle$ and let $L : T \to E$ be its labeling function. Assume that (A4) and (A5) are satisfied. Let $\mathcal{C}(w)$ be defined as in equation (1) where the upper bounds u_r's are computed using Algorithm 6. Assume that a label a is observed and there is a transition t_r labeled $L(t_r) = a$ with bound u_r such that it is disabled at any marking in $\mathcal{C}(w)$. Then the

new bound u_r' computed by Algorithm 6 fulfills $u_r = u_r'$.
Proof: First, notice that if transition t_r is disabled at any marking in $\mathcal{C}(w)$ then all solutions of equation (1) verify $\sigma_r = z_r^{in}$ where z_r^{in} is computed by Algorithm 6. In fact, σ_r cannot be greater than z_r^{in} and being less would mean that there is a marking in $\mathcal{C}(w)$ in which t_r is enabled. Furthermore $\sigma_r = u_r$ since if $\sigma_r < u_r$ then there would exist another solution for equation (1), let's say σ_r'', such that $\sigma_r'' > \sigma_r$, meaning that t_r was enabled at the consistent marking given by σ_r. Therefore we have $z_r^{in} = u_r$ and since step 5 of Algorithm 6 computes u_r' as $u_r' = min(u_r + 1, z_r^{in})$, we have $u_r' = z_r^{in} = u_r$. □

Proposition 9. Let us consider a Petri net system $\langle N, M_0\rangle$ and let $L : T \to E$ be its labeling function. Let us assume that assumptions (A4) and (A5) are satisfied and let w be an observed word of events. Then all markings in the set $\mathcal{C}(w)$ defined as in equation (1) are consistent with the observed word w, when the upper bounds u_r's are computed using Algorithm 6.
Proof: We prove this by induction on the length of the observed word.
When no event is observed, i.e., when $w = w_0$ is the empty word, using equation (1) we have that $\mathcal{C}(w_0) = \{M_0\}$, thus the statement of the proposition holds.
Moreover, when a word w_{k-1} of length $k-1$ is observed, we assume that all markings in $\mathcal{C}(w_{k-1})$ are consistent with w_{k-1}, where $\mathcal{C}(w_{k-1})$ is defined as in equation (1) and the bounds are computed using Algorithm 6.
Now, let e be a newly observed event, and let $w = w_k = w_{k-1}e$. We have to prove that all markings in $\mathcal{C}(w)$ are consistent with the observed word w.
For simplicity of presentation in the following we assume that there exists only one couple of nondeterministic transitions, thus $n^n = 2$ and $n^d = n - 2$. We call a their label, i.e., $L(t_1) = L(t_2) = a$. Note that such an assumption does not affect the validity of the proof thanks to the contact freeness hypothesis (A5).
We partition the set of transitions as follows (see fig. 2):

$$T = \overline{T} \cup T^{in} \cup T^{out} \cup T_a \tag{2}$$

where $T_a = \{t_1, t_2\}$; P_1^{in} (P_1^{out}) and P_2^{in} (P_2^{out}) are the set of input (output) places to transitions t_1 and t_2 respectively. T^{in} is the set of input and output transitions to P_1^{in} and P_2^{in}, apart from t_1 and t_2; T^{out} is the set of input and output transitions to P_1^{out} and P_2^{out}, apart from t_1 and t_2; finally, $\overline{T}$ is the set of deterministic transitions that are not contained in the previous sets.
Moreover, we define the following two sets[1]:

$$\mathcal{S} = \begin{cases} \sigma_1 \leq u_1 \\ \sigma_2 \leq u_2 \\ \sigma_1 + \sigma_2 = n_a \\ \sigma_1, \sigma_2 \in \mathbb{N} \end{cases} \quad \mathcal{S}' = \begin{cases} \sigma_1 \leq u_1' \\ \sigma_2 \leq u_2' \\ \sigma_1 + \sigma_2 = n_a' \\ \sigma_1, \sigma_2 \in \mathbb{N} \end{cases} \tag{3}$$

where $\mathcal{S}$ ($\mathcal{S}'$) consists of the subset of constraints of equation (1) only involving the nondetermininistic transitions t_1 and t_2, when the observed word is w_{k-1} (w). Clearly, these sets contain the only equations that are related to the nondeterministic part of the net, thus only an error on their definition may produce an error on the definition of the set of consistent markings. Therefore, the next step of the induction is proved if we demonstrate that each solution of $\mathcal{S}'$ originates from a solution of $\mathcal{S}$ when the bounds are updated using Algorithm 6, i.e.,
— if the observed event is deterministic, i.e., $e \neq a$, then $\mathcal{S}' \subseteq \mathcal{S}$;
— if the observed event is nondeterministic, i.e., $e = a$, then given a solution $\vec{\sigma} = (\sigma_1,\ \sigma_2) \in \mathcal{S}$, if t_1 (resp., t_2) is enabled from the marking corresponding to $\vec{\sigma}$, then $\vec{\sigma}' = (\sigma_1 + 1,\ \sigma_2) \in \mathcal{S}'$ (resp., $(\sigma_1,\ \sigma_2 + 1) \in \mathcal{S}'$).
Now, when an event e is observed, four different cases may occur.
(1) A transition $t \in \overline{T}$ has fired. In such a case $\mathcal{S}' \equiv \mathcal{S}$ and the statement of the proposition holds.
(2) A transition $t \in T^{in}$ has fired.
– a. – If $t \in {}^\bullet(P_1^{in}) \cup {}^\bullet(P_2^{in})$, no bound is updated thus $\mathcal{S}' \equiv \mathcal{S}$.
– b. – If $t \in (P_1^{in})^\bullet \cup (P_2^{in})^\bullet$ the upper bounds may either stay the same or may be even smaller thus $\mathcal{S}' \subseteq \mathcal{S}$.
(3) A transition $t \in T^{out}$ has fired.
– a. – If $t \in {}^\bullet(P_1^{out}) \cup {}^\bullet(P_2^{out})$, no bound is updated thus $\mathcal{S}' \equiv \mathcal{S}$.
– b. – If $t \in (P_1^{out})^\bullet \cup (P_2^{out})^\bullet$ the upper bounds may either stay the same or may be even smaller thus $\mathcal{S}' \subseteq \mathcal{S}$.
(4) A transition $t \in T_a$ has fired.
Let us denote T_a^e the set of transitions whose label is a and that are enabled by at least one marking in $\mathcal{C}(w_{k-1})$. Two different cases may occur: (1) T_a^e is a singleton, i.e., either $T_a^e = \{t_1\}$ or $T_a^e = \{t_2\}$. (2) $T_a^e = \{t_1, t_2\}$.
– 1. – With no loss of generality we may assume $T_a^e = \{t_1\}$. In such a case the generic solution $(\sigma_1',\ \sigma_2')$ of $\mathcal{S}'$ may always be written as $\sigma_1' = \tilde{\sigma}_1 + 1$, $\sigma_2' = \tilde{\sigma}_2$. In fact, if this was not possible, then $\sigma_1' = 0$ and $\sigma_2' = n_a' = n_a + 1 > n_a \geq u_2 = u_2'$, where the last equality follows from lemma 8. Therefore, we would obtain $\sigma_2' > u_2'$, that leads to a contradiction.
Now, we want to prove that $(\tilde{\sigma}_1,\ \tilde{\sigma}_2)$ is a solution of $\mathcal{S}$. By simply substituting $(\sigma_1',\ \sigma_2')$ in (3) where $\mathcal{S}'$ is defined, and taking into account that $n_a' = n_a + 1$, $u_2' = u_2$ and $u_1' = u_1 + 1$, we can trivially verify that $(\tilde{\sigma}_1,\ \tilde{\sigma}_2) \in \mathcal{S}$.
– 2. – Let us now consider the case in which $T_a^e = \{t_1, t_2\}$. We first observe that for at least one transition $t_i \in T_a^e$, $\sigma_i' > \sigma_i^{min}$, where σ_i^{min}, $i = 1, 2$, is the minimum value of σ_i for any $(\sigma_1,\ \sigma_2) \in \mathcal{S}$. In fact, if this was not true, then for all solutions $(\sigma_1,\ \sigma_2) \in \mathcal{S}$, and $(\sigma_1',\ \sigma_2') \in \mathcal{S}'$ it holds that $n_a' = \sigma_1' + \sigma_2' = \sigma_1^{min} + \sigma_2^{min} \leq \sigma_1 + \sigma_2 = n_a$ contradicting $n_a' = n_a + 1 > n_a$.
Now, with no loss of generality we assume that $\sigma_1' > \sigma_1^{min} \geq 0$. Then, we may write $\tilde{\sigma}_1 = \sigma_1' - 1$ and $\tilde{\sigma}_2 = \sigma_2'$. We show that $(\tilde{\sigma}_1,\ \tilde{\sigma}_2) \in \mathcal{S}$.
The only constraint that is not trivially verified is $\tilde{\sigma}_2 \leq u_2$. In fact, $\sigma_2' \leq u_2' \to \tilde{\sigma}_2 \leq u_2'$. However, we show that if $\sigma_2' = u_2' = u_2 + 1$ then $\sigma_1' = n_a' - u_2' = n_a + 1 - u_2 - 1 = n_a - u_2$. By assumption $\sigma_1' > \sigma_1^{min}$, thus $\sigma_1' > n_a - u_2$ that leads to a contradiction. □

Proposition 10. Let us consider a net system $\langle N, M_0\rangle$ and let $L : T \to E$ be its labeling function. Let us assume that assumptions (A4) and (A5) are satisfied and let w be an observed word of events. Then all markings that are consistent with the observed word w are contained in $\mathcal{C}(w)$, when $\mathcal{C}(w)$ is defined as in equation (1) and the upper bounds u_r's are computed using Algorithm 6.
Proof: We prove this by induction on the length of the observed word. Clearly, when no event is observed the only consistent marking is the initial one, thus the statement of the proposition holds. Moreover, we assume that it also holds when a word w_{k-1} is observed, i.e., we assume that there exists no marking that is consistent with w_{k-1} and that is not contained in $\mathcal{C}(w_{k-1})$.

[1] Slightly abusing the notation, we denote with $\mathcal{S}$ and $\mathcal{S}'$ both the set of constraints given by (3) and their respective solutions (σ_1, σ_2).

To complete the prove, we must demonstrate that when a new event e is observed, i.e., when the current word is $w = w_k = w_{k-1}e$, all markings that are consistent with w are contained in $\mathcal{C}(w)$. As in the case of the previous proposition, thanks to the contact freeness assumption (A5), we may assume that there exists only one couple of nondeterministic transitions, namely t_1 and t_2. Therefore, we may restrict our attention to the sets $\mathcal{S}$ and $\mathcal{S}'$ defined in equation (3). Now, the next step of the induction is proved if we demonstrate that, from each solution $(\sigma_1,\ \sigma_2) \in \mathcal{S}$ corresponding to a marking in $\mathcal{C}(w_{k-1})$ enabling a transition labeled e, we get a solution $(\sigma_1',\ \sigma_2') \in \mathcal{S}'$ that is a consistent marking associated to the observation of e.

We refer again to the partition of T introduced via equation (2) and we consider four different cases.

(1) A transition $t \in \overline{T}$ fires. Being $\mathcal{S}' \equiv \mathcal{S}$, the statement of the proposition is trivially verified.

(2) A transition $t \in T^{in}$ fires. In such a case, $\mathcal{S}' \subseteq \mathcal{S}$ and we must prove that when updating the bounds we are not neglecting markings that are consistent with w. However, by looking at Algorithm 6 we may observe that $\mathcal{S}' \subset \mathcal{S}$ if and only if $\exists r \in \{1, 2\}$ such that $t \in ({}^\bullet t_r)^\bullet$ and $z_r^{in} < u_r$ (first *if* case of step 4 of Algorithm 6). But this is correct because if we allow u_r' to be greater than z_r^{in}, the non–negativity constraints would be violated.

(3) A transition $t \in T^{out}$ fires. This case is similar to the previous one. In fact, $\mathcal{S}' \subseteq \mathcal{S}$. In particular, $\mathcal{S}' \subset \mathcal{S}$ if and only if $\exists r \in \{1, 2\}$ such that $t \in (t_r^\bullet)^\bullet$ and $n_r - z_r^{out} < u_{\bar{r}}$, where $\bar{r}$ is defined as in step 4 of Algorithm 6. But this is correct, because z_r^{out} denotes by definition the number of times transition t_r has fired for sure. If we allow $u_{\bar{r}}$ to be greater than $n_r - z_r^{out}$ (or equivalently u_r to be smaller than z_r^{out}), the non–negativity constraints are violated.

(4) A transition $t \in T^a$ fires. We must prove that, given a solution $\vec{\sigma} = (\sigma_1,\ \sigma_2) \in \mathcal{S}$, if t_1 (resp., t_2) is enabled from the marking corresponding to $\vec{\sigma}$, then $\vec{\sigma}' = (\sigma_1{+}1,\ \sigma_2) \in \mathcal{S}'$ (resp., $(\sigma_1,\ \sigma_2 + 1) \in \mathcal{S}'$).

With no loss of generality we may assume that t_1 is enabled from the marking corresponding to $\vec{\sigma}$. This implies that for that $\vec{\sigma}$ it holds that $\sigma_1 < z_r^{in}$ being by definition z_r^{in} the enabling degree of transition t_r assuming that t_r has never fired. Thus, $\sigma_1 < z_r^{in}, \quad \sigma_1 \leq u_r \quad \Longrightarrow$ $\sigma_1' = \sigma_1 + 1 \leq \min(u_r + 1, z_r^{in}) = u_1'$.

Moreover, $\sigma_1' - 1 + \sigma_2' = n_a \rightarrow \sigma_1' + \sigma_2' = n_a'$. Therefore, we may conclude that $(\sigma_1', \sigma_2') \in \mathcal{S}'$. □

Theorem 11. Let us consider a net system $\langle N, M_0 \rangle$ and let $L : T \rightarrow E$ be its labeling function. Let us assume that assumptions (A4) and (A5) are satisfied and let w be an observed word of events. Then the set $\mathcal{C}(w)$ defined by equation (1) contains all and only those markings that are consistent with the observed word w, when the upper bounds u_r's are computed using Algorithm 6.

Proof: It follows from propositions 9 and 10. □

Example 12. Let us consider again the Petri net system in fig. 1. Assumptions (A4) and (A5) are verified. Thus, by virtue of Theorem 11, the set of consistent markings can be described in terms of equation (1) where the upper bounds are computed using Algorithm 6.

All bounds are initially set to zero, thus $\mathcal{C}(\varepsilon) = \{M \in \mathbb{N}^8 \,|\, M = M_0 + C\vec{\sigma},\ \sigma_1, \sigma_2, \sigma_3, \sigma_4 \leq 0,\ \sigma_1 + \sigma_2 = 0,\ \sigma_3 + \sigma_4 = 1,\ \sigma_5 = \sigma_6 = \sigma_7 = 0,\ \vec{\sigma} \in \mathbb{N}^7\}$ and the only admissible firing vector is $\vec{\sigma} = \vec{0}$.

Assume that b is observed. Both u_3 and u_4 are updated to one, while the other bounds keeps equal to zero. Thus, $\mathcal{C}(b) = \{M \in \mathbb{N}^8 \,|\, M = M_0 + C\vec{\sigma},\ \sigma_1 \leq 0,\ \sigma_2 \leq 0,\ \sigma_3 \leq 1,\ \sigma_4 \leq 1,\ \sigma_1 + \sigma_2 = 0,\ \sigma_3 + \sigma_4 = 1,\ \sigma_5 = \sigma_6 = \sigma_7 = 0,\ \vec{\sigma} \in \mathbb{N}^7\}$.

It is easy to verify that in this case there are two admissible firing vectors and $\mathcal{C}(b) = \{[1\ 0\ 0\ 1\ 1\ 0\ 1\ 1]^T, [1\ 0\ 1\ 0\ 1\ 0\ 0\ 2]^T\}$.

Similarly, if a is observed, we get $u_1 = u_2 = 1$ and $\mathcal{C}(ba) = \{M \in \mathbb{N}^8 \,|\, M = M_0 + C\vec{\sigma},\ \sigma_1 \leq 1,\ \sigma_2 \leq 1,\ \sigma_3 \leq 1,\ \sigma_4 \leq 1,\ \sigma_1 + \sigma_2 = 1,\ \sigma_3 + \sigma_4 = 1,\ \sigma_5 = \sigma_6 = \sigma_7 = 0,\ \vec{\sigma} \in \mathbb{N}^7\}$.

This implies that there are four admissible firing vectors and $\mathcal{C}(ba) = \{[0\ 1\ 0\ 1\ 1\ 0\ 1\ 1]^T, [1\ 0\ 0\ 1\ 0\ 1\ 1\ 1]^T, [0\ 1\ 1\ 0\ 1\ 0\ 0\ 2]^T, [1\ 0\ 1\ 0\ 0\ 1\ 0\ 2]^T\}$.

Now, if d is observed, we have that $z_1^{out} = 1$. Consequently $u_2 = 0$ and $\mathcal{C}(bad) = \{M \in \mathbb{N}^8 \,|\, M = M_0 + C\vec{\sigma},\ \sigma_1 \leq 1,\ \sigma_2 \leq 0,\ \sigma_3 \leq 1,\ \sigma_4 \leq 1,\ \sigma_1 + \sigma_2 = 1,\ \sigma_3 + \sigma_4 = 1,\ \sigma_6 = 1,\ \sigma_5 = \sigma_7 = 0,\ \vec{\sigma} \in \mathbb{N}^7\}$.

Finally, if the whole observed word is $w = badbc$, then the marking is perfectly known being $\vec{\sigma} = [1\ 0\ 2\ 0\ 1\ 1\ 0]^T$ the only admissible firing vector. ■

6 Conclusions

We have presented a marking estimation procedure that can be applied to labeled Petri nets. Under some assumptions, we proved that the markings consistent with an observed sequence can be described by a constraint set of linear inequalites: this set has a fixed structure that does not change as the length of the observed sequence increases.

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] P.E. Caines, R. Greiner, S. Wang, "Dynamical Logic Observers for Finite Automata," *Proc. 27th Conf. on Decision and Control* (Austin, Texas), pp. 226–233, Dec. 1988.

[3] P.E. Caines, S. Wang, "Classical and Logic Based Regulator Design and its Complexity for Partially Observed Automata," *Proc. 28th Int. Conf. on Decision and Control* (Tampa, Florida), pp. 132–137, Dec. 1989.

[4] 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.

[5] A. Giua, "Petri Net State Estimators Based on Event Observation," *Proc. 36th Int. Conf. on Decision and Control* (San Diego, California), pp. 4086–4091, Dec. 1997.

[6] A. Giua, C. Seatzu, "Observability of place/transition nets," *IEEE Trans. on Automatic Control*, Vol. 47, No. 9, pp. 1424 - 1437, Sept. 2002.

[7] R. Kumar, V. Garg, S.I. Markus, "Predicates and Predicate Transformers for Supervisory Control of Discrete Event Dynamical Systems," *IEEE Trans. on Automatic Control*, Vol. 38, No. 2, pp. 232–247, 1993.

[8] 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.

[9] T. Murata, "Petri Nets: Properties, Analysis and Applications," *Proc. IEEE*, Vol. 77, No. 4, pp. 541–580, 1989.

[10] C.M. Özveren, A.S. Willsky, "Observability of discrete event dynamic systems," *IEEE Trans. on Automatic Control*, Vol. 35, No. 7, pp. 797–806, July 1990.

[11] J.L. Peterson, *Petri Net Theory and the Modeling of Systems*, Prentice-Hall, 1981.

[12] P.J. Ramadge, "Observability of Discrete-Event Systems," *Proc. 25th Conf. on Decision and Control* (Athens, Greece), pp. 1108–1112, Dec. 1986.