Observers for nondeterministic λ-free labeled Petri nets

Daniele Corona, Alessandro Giua, Carla Seatzu
Dip. di Ingegneria Elettrica ed Elettronica
Università di Cagliari, Italy
Email: daniele.corona,giua,seatzu@diee.unica.it

Jorge Júlvez
Dep. de Informática e Ingenierá de Sistemas
Universidad de Zaragoza, Spain
Email: julvez@posta.unizar.es

Abstract— **In this paper we deal with the problem of estimating the marking of a labeled Petri net with nondeterministic transitions. In particular, we consider the case in which nondeterminism is due to the presence of transitions that share the same label and that can be simultaneously enabled. Under the assumption that: the structure of the net is known, the initial marking is known, the transition labels can be observed, the nondeterministic transitions are contact-free, we present a technique for characterizing the set of markings that are consistent with the actual observation. More precisely, we show that the set of markings consistent with an 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 consider the problem of estimating the marking of a Petri net based on the observation of transition labels.

The problem of estimating the state of a dynamic system is a fundamental issue in *system theory*. A similar problem has also been addressed in theoretical *computer science* within the framework of nondeterministic language generators. Nevertheless, the problem statement is quite different depending on the considered framework.

- In system theory, a state observer reconstructs the plant states that cannot be measured on the base of the observation of some physical variables. The initial state of the system is completely unknown, while a perfect knowledge of the system dynamics is usually assumed, i.e., the behaviour of the system is *deterministic*.
  Analogous problems in the case of discrete event systems (DES) have 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. The main drawback of the automata based approach is the requirement that the set of consistent markings must explicitly be enumerated. A valid solution to this problem has been proposed using Petri nets [5]. In particular, in [5] a procedure that simply produces an estimate of the state has been proposed, while the special structure of Petri nets allowed us to determine, using linear algebraic tools, if a given marking is consistent with the observed behaviour without the explicit enumeration of the (possibly infinite) consistent set.
- In the context of computer science, where the behaviour of a system is modeled by a *language*, the problem of observation is quite different. The event set E of a DES is viewed as an alphabet, and a sequence of events from this alphabet forms a *word* (or a *string*) of events, that describe a particular evolution of the system.
  The state observer of a DES aims to provide 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.
  1) *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.
  2) *Undistinguishable 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 labeled at a given state.

For DES modeled as finite automa, 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 mentioned 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 Petri nets as discrete event models and address the observer design from a computer science point of view.

We first observe that an analogous determinization procedure as that used in the case of automata, cannot be used in the Petri net (PN) framework. In fact, a nondeterministic PN cannot be converted into an equivalent deterministic PN, because of the following strict inclusions

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

where

- $\mathcal{L}_{\rm det}$ 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 undistinguishable 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 undistinguishable 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.

In this paper we propose a different 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. We extend the results proposed in [6] to 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 four assumptions: (A1) the net structure is known, (A2) the initial marking is known, (A3) the label function is λ-free and labels associated to transitions may be observed, (A4) the nondeterministic transitions are *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'.

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 some parameters that can be recursively computed. The main advantage of the proposed approach is that we need not exhaustively enumerate all consistent markings.

The validity of the proposed characterization has not been formally proved yet, but it has been verified through a wide investigation of the problem and many numerical examples. Note however that a formal proof has been given in [6] under the additional assumption that the same label cannot be associated to more than two transitions.

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" step of transitions using logical formulas, without having to enumerate this set. Other authors [8] have also discussed the problem of estimating the marking of a Petri net using a mix of transition firings and place observations. Finally, Zhang and Holloway [13] used a Controlled Petri Net model for forbidden state avoidance under partial *event* observation with the assumption that the initial marking be known.

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 [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 $M' = M + C(\cdot, t)$. We write $M\,[\sigma\rangle$ to denote that the sequence of transitions σ is enabled at M, and we write $M\,[\sigma\rangle\,M'$ to denote that the firing of σ yields M'. We 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 $\vec{\sigma} \in \mathbb{N}^n$ that satisfies the *state equation* $M = M_0 + C \cdot \vec{\sigma}$, i.e., $PR(N, M_0) = \{M \in \mathbb{N}^m \mid \exists \vec{\sigma} \in \mathbb{N}^n : M = M_0 + C \cdot \vec{\sigma}\}$. It holds that $R(N, M_0) \subseteq PR(N, M_0)$.

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 while no transition may be labeled with the empty string ε.

Using the notation of [11] and [4] we say that this labeling function is λ-*free*[1].

Definition 1. *A Petri net system* $\langle N, M_0 \rangle$ *with* λ*-free labeling function* $L : T \to E$ *is* deterministic *if for all markings* $M \in R(N, M_0)$ *and for any two transitions* $t, t' \in T$*:*

$$t \neq t', \ L(t) = L(t'), \ M[t\rangle \implies \neg M[t'\rangle,$$

i.e., if two transitions are labeled with the same symbol they cannot simultaneously be enabled at M. ■

From the above definition it is clear that determinism is a behavioral property because it not only depends on the structure of the net, but on the reachable set (i.e., on the initial marking) as well. However, it is also possible to introduce a structural definition of determinism.

Definition 2. *A Petri net* N *with* λ*-free labeling function* $L : T \to E$ *is* structurally deterministic *if for any two transitions* $t, t' \in T$*:*

$$t \neq t' \implies L(t) \neq L(t'),$$

i.e., two different transitions cannot be labeled with the same symbol. ■

Note that if a Petri net N is structurally deterministic, then the net system $\langle N, M_0 \rangle$ is deterministic for all initial marking M_0.

In this paper we consider Petri nets that are not structurally deterministic. 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, $T = T^d \cup T^n$.

Analogously, we say that an event e is nondeterministic if there exists more than one transition t such that $L(t) = e$, otherwise we say that the event e is deterministic. Therefore, with no ambiguity on the notation, we may write $E = E^d \cup E^n$.

Note that the labeling function restricted to T^d is an isomorphism and thus, with no loss of generality we can assume $E^d = T^d$.

We denote as T_e the set of transitions labeled e, i.e,

$$T_e = \{t \in T \mid L(t) = e\}.$$

The restriction of the incidence matrix C to T_e is denoted C_e and the restriction of the firing vector $\vec{\sigma}$ to T_e is denoted $\vec{\sigma_e}$.

Finally, to each set of nondeterministic transitions T_e we associate the set $\mathcal{T}_e$ containing all possible subsets of transitions, apart from itself and the empty set, i.e.,

$$\mathcal{T}_e = \{\tau \subseteq T_e \mid \tau \neq \emptyset, \ \tau \neq T_e\} = 2^{T_e} \setminus \{\emptyset, T_e\}.$$

Clearly, $|\mathcal{T}_e| = 2^{n_e} - 2$ where n_e denotes the number of nondeterministic transitions labeled e.

[1]In the Petri net literature the empty string is denoted λ, while in the formal language literature it is denoted ε. In this paper we denote the empty string ε but, for consistency with the Petri net literature, we still use the term λ-*free* for the labeling function.

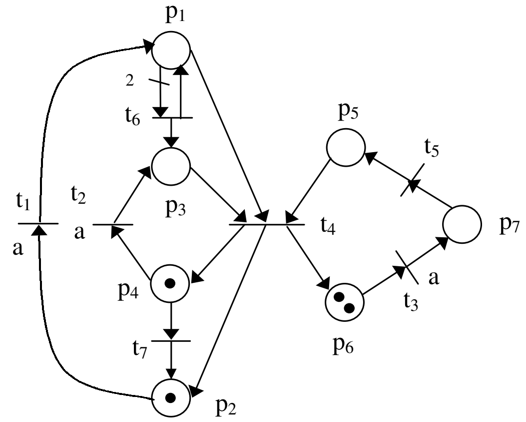

Fig. 1. A Petri net system that can only be partially observed

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, $w_0 = \varepsilon$.

III. 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) The label function is λ-free and 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 behavior.

Definition 3. *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* $L(\sigma) = w\}$. ■

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.

Note that the cardinality of the set of consistent markings may either increase or decrease as the length of the observed word increases.

Example 4. Let us consider the Petri net system in Figure 1 where $T^n = T_a = \{t_1, t_2, t_3\}$ and $T^d = \{t_4, t_5, t_6, t_7\}$.

Clearly, when no event has been observed,

$$\mathcal{C}(\varepsilon) = \{[0\ 1\ 0\ 1\ 0\ 2\ 0]^T\}.$$

Let us first assume that the event a is observed. Given the initial marking M_0, all nondeterministic transitions may have fired, thus

$$\begin{array}{rl}\mathcal{C}(a) = & \{[1\ 0\ 0\ 1\ 0\ 2\ 0]^T, \\ & [0\ 1\ 1\ 0\ 0\ 2\ 0]^T, \\ & [0\ 1\ 0\ 1\ 0\ 1\ 1]^T\}.\end{array}$$

Now, assume that the event a is observed again, i.e., $w = aa$. Given the initial marking, we know for sure that both transitions t_1 and t_2 may have fired at most once, while transition t_3 may have fired twice. Therefore,

$$\begin{array}{rl}\mathcal{C}(aa) = & \{[1\ 0\ 1\ 0\ 0\ 2\ 0]^T, \\ & [0\ 1\ 1\ 0\ 0\ 1\ 1]^T, \\ & [0\ 1\ 0\ 1\ 0\ 0\ 2]^T, \\ & [1\ 0\ 0\ 1\ 0\ 1\ 1]^T\}.\end{array}$$

Now, if the deterministic transition t_7 fires we can conclude that no previous observation of a was due to the firing of t_2 because the firing of t_2 would have disabled t_7. Therefore, the only sequences that may have fired are $\sigma_1 = t_1t_3t_7$, $\sigma_2 = t_3t_1t_7$, $\sigma_3 = t_3t_3t_7$. Consequently,

$$\mathcal{C}(aat_7) = \{[1\ 1\ 0\ 0\ 0\ 1\ 1]^T, [0\ 2\ 0\ 0\ 0\ 0\ 2]^T\}$$

Assume that the deterministic transition t_5 fires. The firing of t_5 is enabled at both markings in $\mathcal{C}(aat_7)$, thus

$$\mathcal{C}(aat_7t_5) = \{[1\ 1\ 0\ 0\ 1\ 1\ 0]^T,\ [0\ 2\ 0\ 0\ 1\ 0\ 1]^T\}.$$

Finally, if t_5 is observed again we can conclude that only the second marking in $\mathcal{C}(aat_7t_5)$ is compatible with the last observation, thus the actual marking of the net is completely reconstructed and

$$\mathcal{C}(aat_7t_5t_5) = \{[2\ 0\ 0\ 0\ 0\ 0\ 2]^T\}.$$

Note that this also implies that we have completely reconstructed the sequence of transitions that has actually fired, i.e., $\sigma = t_3t_3t_7t_5t_5$. ■

IV. THE CONTACT FREE CASE

As already discussed in the Introduction, the problem of defining the set of w-consistent markings using a fixed number of constraints has been already investigated by the same authors in [6]. In particular, in [6] we formally proved that a linear algebraic characterization of $\mathcal{C}(w)$ can be given, with a fixed number of constraints, when the following two conditions are verified.

(A4) Nondeterministic transitions are contact free, i.e., for any two nondeterministic transitions t_i and t_j, it holds that ${}^\bullet t_i^\bullet \cap {}^\bullet t_j^\bullet = \emptyset$.

(A5) For each label $e \in E$ there are at most two transitions such that $L(t) = e$, or equivalently, $|T_e| \leq 2$.

In this paper we discuss how it is possible to extend the results in [6] when the assumption (A5) is removed. Note that in this preliminary version of the paper we present this result as a conjecture, while a formal proof is still missing. As discussed in detail in the following, our conjecture is motivated by a wide investigation of the problem and by a careful examination of many numerical examples.

More precisely, we conjecture that, under the assumptions (A1) to (A4), 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.

Let us first introduce the following notation.

Definition 5. *Given a marking M_w and a transition $t \in T$, we define*

$$z_w(t) = \min_{p \in {}^\bullet t} \left\{ \left\lfloor \frac{M_w(p)}{Pre(p,t)} \right\rfloor \right\}$$

the enabling degree of transition t at M_w.

Given a set of transitions $\tau \subseteq T$, we also define

$$z_w(\tau) = \sum_{t \in \tau} z_w(t).$$

Finally, given a vector $\vec{\sigma} \in \mathbb{N}^n$, we denote as

$$\sigma(\tau) = \sum_{t \in \tau} \sigma(t).$$

■

Note that if all transitions in τ are conflict free, then $z_w(\tau)$ represents the number of times transitions in τ may simultaneously fire at M_w.

Conjecture 6. *Let us consider a labeled Petri net system $\langle N, M_0 \rangle$ and let $L : T \to E$ be its labeling function. Let assumptions (A1) to (A4) be verified. Then, for all words $w \in E^*$ the set of w-consistent markings $\mathcal{C}(w)$ is equal to*

$$\mathcal{C}(w) = \{M \in \mathbb{N}^m \mid M = M_w + \sum_{e \in E^n} C_e \vec{\sigma}_e; \quad \vec{\sigma}_e \in \mathcal{S}_e(w)\} \tag{1}$$

where

$$\begin{array}{rl}\mathcal{S}_e(w) = \{\vec{\sigma} \in \mathbb{N}^{n_e} \mid (\forall \tau \in \mathcal{T}_e) & \sigma(\tau) \leq u_w(\tau), \\ & \sigma(T_e) = u_w(T_e)\},\end{array} \tag{2}$$

and the upper bounds $u_w(\tau)$ and $u_w(T_e)$, as well as the marking M_w, are computed using the recursive Algorithm 7. ■

Therefore, the number of constraints used to describe the set $\mathcal{S}(w)$ is equal to $\sum_{e \in E^n} 2^{n_e} - |E^n|$, regardless of the length of the observed word w.

Now, before examining in detail the steps of the algorithm, let us discuss the physical meaning of all the parameters characterizing the above set (1).

Let us preliminary observe that the firing of a nondeterministic transition t may be *detected* (or *reconstructed*) when a deterministic transition t_d is observed and the firing of t is strictly necessary to enable t_d. Therefore, using Algorithm 7, we define M_w as the marking that we reach from the initial one by firing all the observed deterministic transitions, and all those nondeterministic transitions that have been detected. In the following we say that M_w is the *basis marking* given the actual observation w.

Algorithm 7 (Upper bounds and basis marking computation).

1. Let $w = w_0$ and $M_w = M_0$.
2. Let $u_w(\tau) = 0$ for all $e \in E^n$ and for all $\tau \in \mathcal{T}_e$.
3. Let $u_w(T_e) = 0$ for all $e \in E^n$.
4. Wait until an event e is observed.
5. Let $flag = 0$.
6. If $e \in E^d$, then

```
        let t = L^{-1}(e),
        if •t ∩ (•T^n•) = ∅, then                                   (Case A)
            M_{we} = M_w + C(·, t)
        endif
        if •t ∩ (T^n•) = P_t ≠ ∅, then                              (Case B)
            for all p ∈ P_t, then
                let {t̂} = T^n ∩ •p
                let α = max_{p∈P_t} { 0, ⌈ (Pre(p,t) − M_w(p)) / Post(p,t̂) ⌉ }
                for all τ ∈ T_{L(t̂)} such that t̂ ∈ τ, then
                    u_{we}(τ) = u_w(τ) − α
                endfor
                u_{we}(T_{L(t̂)}) = u_w(T_{L(t̂)}) − α
                for all τ ∈ T_{L(t̂)} such that t̂ ∉ τ, then
                    u_{we}(τ) = min{u_w(τ), u_{we}(T_{L(t̂)})}
                endfor
                M_w = M_w + αC(·, t̂)
                flag = 1
            endfor
            M_{we} = M_w + C(·, t)
        endif
        if •t ∩ (•T^n) ≠ ∅, then                                    (Case C)
            if flag = 0, then
                M_{we} = M_w + C(·, t)
            endif
            let T_r(t) = {t̂ ∈ T^n | •t ∩ •t̂ ≠ ∅}
            for all t̂ ∈ T_r(t), then
                u_{we}({t̂}) = min{u_w({t̂}), z_{we}(t̂)}
                for all τ ∈ T_{L(t̂)} such that t̂ ∈ τ with τ ≠ {t̂}, then
                    u_{we}(τ) = min{u_w(τ), u_{we}({t̂}) + u_w(τ \ {t̂})}
                endfor
                u_{we}(T_{L(t̂)}) = min{u_w(T_{L(t̂)}), u_{we}({t̂}) + u_w(T_{L(t̂)} \ {t̂})}
                M_{we} = M_w
            endfor
        endif
    else                                                            (Case D)
        for all τ ∈ T_e, then
            u_{we}(τ) = min{u_w(τ) + 1, z_w(τ)}
        endfor
        u_{we}(T_e) = u_w(T_e) + 1
        M_{we} = M_w
    endif
```

7. $w = we$
8. Goto 4.

■

Fig. 2. The algorithm for the upper bounds and the basis marking computation.

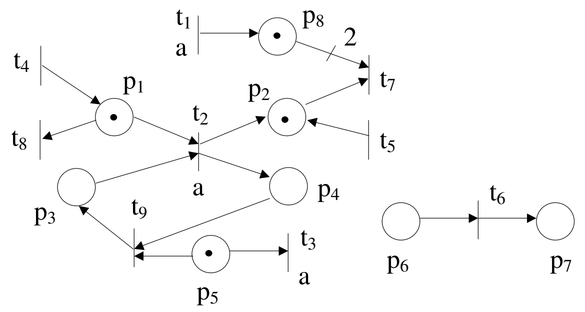

Fig. 3. The generic substructure of a more complex Petri net that satisfies the contact-free assumption.

Moreover, for each nondeterministic event e, the upper bound $u_w(T_e)$ denotes how many times the event e has been observed in w without being detected.

Finally, the upper bound $u_w(\tau)$ relative to a given subset $\tau \subset \mathcal{T}_e$, imposes a limit on the maximum number of times all transitions in τ may have fired, given the actual observation w, and taking into account that a certain number of nondeterministic transitions labeled e may have been detected.

Now, let us discuss in detail all cases in Algorithm 7. Consider the labeled Petri net in Figure 3 that represents the generic substructure of a more complex Petri net that satisfies the contact-free assumption (A4). Let us assume that in this subnet the only nondeterministic transitions are those labeled a. Let w be the actual observed word of events and let M_w be the marking shown in Figure 3. Finally assume $|w|_a \geq 1$.

- *A deterministic transition t such that ${}^\bullet t \cap ({}^\bullet T^{n\bullet}) = \emptyset$ fires.* (Case A)
  Assume that t_4 fires. In such a case we only update the basis marking taking into account that the deterministic transition t_4 has fired, but we deduce no information on the number of times the nondeterministic transitions have eventually fired. The same holds if we observe t_5 or t_6.
- *A deterministic transition t such that ${}^\bullet t \cap (T^{n\bullet}) = P_t \neq \emptyset$ fires.* (Case B)
  Assume that the firing of t_7 is observed. In such a case we know for sure that each place $p \in {}^\bullet t_7$ (namely, p_2 and p_8) contains a number of tokens that is greater or equal than $Pre(p, t_7)$. Now, given the basis marking M_w, if for some place $p \in {}^\bullet t_7$, $M_w(p) < Pre(p, t_7)$, we know for sure that the nondeterministic transition ${}^\bullet p$ has fired and we can also evaluate (see Algorithm 7) how many times it has fired. We consequently update the basis marking and the upper bounds relative to all subsets containing ${}^\bullet p$.
  As an example, in the case at hand, we can conclude that one of the previous observations of a was due to the firing of t_1. Therefore, the basis marking M_w is updated to $M_{we} = M_w + C(\cdot, t_1) + C(\cdot, t_7)$.
- *A deterministic transition t such that ${}^\bullet t \cap ({}^\bullet T^n) \neq \emptyset$ fires.* (Case C)
  Assume that t_8 fires. In such a case it may occur that the upper bounds associated to subsets of nondeterministic transitions may decrease. In fact, if t_8 fires, we know for sure that if p is an input place of t_8, then it should contain a number of tokens that is greater or equal to $Pre(p, t_8)$. Therefore, if there is some nondeterministic transition exiting p, we know for sure that the maximum number of times it may have fired must ensure that in p there are at least $Pre(p, t_8)$ tokens.
  As an example, if in the actual case the upper bound associated to $\tau = \{t_2\}$ was 1, we reduce it to zero. Then, we update all the other $u_w(\tau)$'s relative to subsets τ containing t_2, as well as $u_w(T_a)$.
- *A nondeterministic event is observed.* (Case D)
  Assume that the nondeterministic event a is observed. In such a case we update the upper bounds $u_{wa}(\tau)$ relative to those subsets $\tau \in \mathcal{T}_a$ whose enabling degree at the current basis marking M_w is greater than the bound $u_w(\tau)$. Furthermore, we always increment of one unity the value of the bound of T_a, i.e., $u_{wa}(T_a) = u_w(T_a)+1$, that takes into account how many times the event a has been observed without being detected.

Let us finally observe that there may be transitions such as t_9 in Figure 3, for which cases B and C simultaneously occur. In such a situation we impose that both cases B and C are taken into account. More precisely, we first consider that ${}^\bullet t_8 \cap (T^{n\bullet}) = \{p_4\} \neq \emptyset$ (case B) and then we consider that ${}^\bullet t_8 \cap ({}^\bullet T^n) = \{p_5\} \neq \emptyset$. Therefore, if t_9 fires we may first increment the upper bounds associated to subsets containing t_2 and then we eventually reduce the upper bounds associated to subsets containing t_3. Clearly, as a consequence, it may occur that the upper bounds associated to subsets τ containing both transitions may keep unaltered. Note that, the binary variable $flag$ has been introduced so as to be sure that the basis marking is not updated twice by the firing of the observed transition t.

Remark 8. If we assume that no more than two transitions may have the same label (i.e., under assumption (A5)), the linear algebraic characterization (1) reduces to the one proposed in [6]. In such a case, for all $e \in E^n$ the only considered subsets $\tau \in \mathcal{T}_e$ are singleton, but, as formally proved in [6], under assumption (A5) we can characterize the set of w-consistent markings by simply computing the upper bounds on the maximum number of times each nondeterministic transition has fired without being detected, as well as the basis marking M_w. ■

On the contrary, if we remove assumption (A5), the upper bounds associated to the only singleton sets are no longer enough. This can be immediately proved by looking at the following simple example.

Example 9. Let us consider the labeled Petri net system in Figure 4. When no event is observed we set $M_{w_0} = M_0$, $u_{w_0}(\tau) = 0$ for all $\tau \in \mathcal{T}_a$, and $u_{w_0}(T_a) = 0$.

In the following we denote as $\tau_{i_1 \, \ldots \, i_k}$ the subset of $\mathcal{T}_a$ of cardinality k, containing transitions $t_{i_1}, \cdots, t_{i_k}$.

Assume $w = a$. The only nondeterministic transitions that are enabled at M_{w_0} are t_1 and t_2, thus, in accordance to

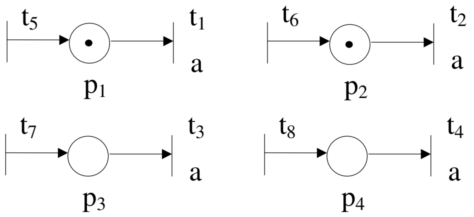

Fig. 4. An example showing that singletons in $\mathcal{T}_a$ are not enough to describe $\mathcal{C}(w)$.

Algorithm 7, we set to 1 the upper bounds relative to all subsets τ containing at least one transition among t_1 or t_2, namely $u_a(\tau_1)$, $u_a(\tau_2)$, $u_a(\tau_{12})$, $u_a(\tau_{13})$, $u_a(\tau_{14})$, $u_a(\tau_{23})$, $u_a(\tau_{24})$, $u_a(\tau_{123})$, $u_a(\tau_{124})$, $u_a(\tau_{234})$, as well as $u_a(T_a)$. On the contrary the upper bounds relative to all the other subsets are kept equal to zero. Finally, the basis marking keeps the same.

Now, let us assume that the sequence of events t_7t_8a is further observed. The observation of the deterministic transitions t_7 and t_8 only implies that the basis marking is updated to $M_w = M_{ade} = [1\ 1\ 1\ 1]^T$. When the last event a is observed, i.e., $w = adea$, the upper bounds are set to $u_w(\tau_1) = u_w(\tau_2) = u_w(\tau_3) = u_w(\tau_4) = 1$, $u_w(\tau_{12}) = u_w(\tau_{13}) = u_w(\tau_{14}) = u_w(\tau_{23}) = u_w(\tau_{24}) = 2$, $u_w(\tau_{34}) = 1$, $u_w(\tau_{123}) = u_w(\tau_{124}) = u_w(\tau_{134}) = u_w(\tau_{234}) = 2$, $u_w(T_a) = 2$.

Note that if the upper bounds relative to the only singleton sets would have been considered, the spurious solution $M = M_0$ obtainable by firing the sequence of transitions $\sigma = t_7t_8t_3t_4$ for which $\sigma(3) = \sigma(4) = 1$, would have been considered consistent with the actual observation. On the contrary, using the proposed algebraic characterization this solution is rejected thanks to the constraint $\sigma(3) + \sigma(4) \leq u_w(\tau_{34}) = 1$ that keeps track of the fact that only the second observation of a may be due to the firing of either transition t_3 or t_4. ■

V. A FINAL EXAMPLE

Let us consider again the Petri net system in Figure 1 whose initial marking is $M_0 = [0\ 1\ 0\ 1\ 0\ 2\ 0]^T$. Initially, when no event is observed the basis marking is the initial marking and all the upper bounds are set to zero. As a new event is observed, the algorithm updates the basis marking and the upper bounds as listed in Table V. Data in the table are then used to construct the set of admissible markings as described in Conjecture 6.

Let us show for instance how to use the table to compute the set $\mathcal{C}(a)$. It holds that

$$\begin{aligned}\mathcal{S}_a(a) = \{\vec{\sigma} \in \mathbb{N}^{n_a} \ \mid \quad & \sigma_1 \leq u_a(\tau_1) = 1, \\ & \sigma_2 \leq u_a(\tau_2) = 1, \\ & \sigma_3 \leq u_a(\tau_3) = 1, \\ & \sigma_1 + \sigma_2 \leq u_a(\tau_{12}) = 1, \\ & \sigma_1 + \sigma_3 \leq u_a(\tau_{13}) = 1, \\ & \sigma_2 + \sigma_3 \leq u_a(\tau_{23}) = 1, \\ & \sigma_1 + \sigma_2 + \sigma_3 = u_a(T_a) = 1\}\end{aligned}$$

The solutions of this integer inequality system are:

$$\begin{aligned}\vec{\sigma}_1 &= [0\ 0\ 1]^T, \\ \vec{\sigma}_2 &= [0\ 1\ 0]^T, \\ \vec{\sigma}_3 &= [1\ 0\ 0]^T,\end{aligned}$$

which substituted in

$$M = M_a + C_a \vec{\sigma}_i, \quad i = 1, 2, 3$$

provide the set of admissible markings:

$$\begin{aligned}\mathcal{C}(a) = \quad & \{[1\ 0\ 0\ 1\ 0\ 2\ 0]^T, \\ & [0\ 1\ 1\ 0\ 0\ 2\ 0]^T, \\ & [0\ 1\ 0\ 1\ 0\ 1\ 1]^T\}.\end{aligned}$$

Note that the evaluation of the set of admissible markings is fast enough to be performed real time, which is an essential feature for real applications. Now we repeat the procedure for all the other events to obtain:

$$\begin{aligned}\mathcal{C}(aa) = \quad & \{[1\ 0\ 1\ 0\ 0\ 2\ 0]^T,\ [0\ 1\ 1\ 0\ 0\ 1\ 1]^T, \\ & [0\ 1\ 0\ 1\ 0\ 0\ 2]^T,\ [1\ 0\ 0\ 1\ 0\ 1\ 1]^T\} \\ \mathcal{C}(aat_7) = & \{[1\ 1\ 0\ 0\ 0\ 1\ 1]^T,\ [0\ 2\ 0\ 0\ 0\ 0\ 2]^T\} \\ \mathcal{C}(aat_7t_5) = & \{[1\ 1\ 0\ 0\ 1\ 1\ 0]^T,\ [0\ 2\ 0\ 0\ 1\ 0\ 1]^T\} \\ \mathcal{C}(aat_7t_5t_5) = & \{[0\ 2\ 0\ 0\ 2\ 0\ 0]^T\} \\ \mathcal{C}(aat_7t_5t_5a) = & \{[1\ 1\ 0\ 0\ 2\ 0\ 0]^T\} \\ \mathcal{C}(aat_7t_5t_5aa) = & \{[2\ 0\ 0\ 0\ 2\ 0\ 0]^T\}\end{aligned}$$

.

Finally, since the net is bounded, it is possible to compute the sets of admissible markings by following the procedure mentioned in the introduction. Figure 5 shows the DFA (33 states and 69 transitions) obtained from the non deterministic reachability graph (42 states and 99 transitions) of the net.

VI. CONCLUSIONS

In this paper we have presented a marking estimation procedure that can be applied to λ-free labeled Petri nets. Under the assumption that all nondeterministic transitions are contact-free, we conjecture that the set of markings consistent with an observed word can be described by a constraint set of linear inequalities: this set 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 provide a formal proof of the above statement, that at present has only been given in the restricted case that at most two transitions may share the same label.

Then, we believe it may be possible to modify the structure of the constraint set to also take into account the case that the initial marking is not known.

Finally, we plan to extend this approach to *arbitrary labeling functions*, i.e., functions $L : T \to E \cup \{\varepsilon\}$ that may assign to one or more transitions the empty string ε. Transitions labeled by ε are called *silent* (or *unobservable*) because their firing cannot be detected.

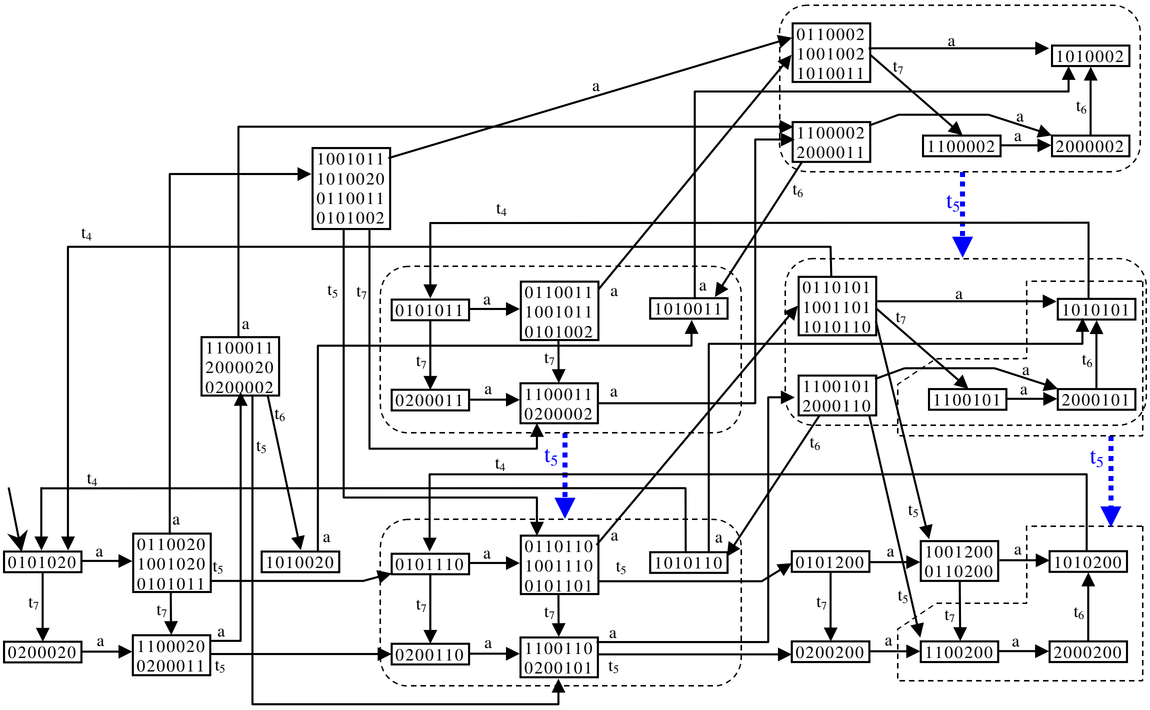

Fig. 5. DFA corresponding to the Petri net in Figure 1. The thick dotted blue arrows indicate the existence of an edge from each element of the dashed macrostate. This is to reduce the complexity of the graph.

w	M_w	$u_w(\tau_1)$	$u_w(\tau_2)$	$u_w(\tau_3)$	$u_w(\tau_{12})$	$u_w(\tau_{13})$	$u_w(\tau_{23})$	$u_w(T_a)$
ε	$[0\ 1\ 0\ 1\ 0\ 2\ 0]^T$	0	0	0	0	0	0	0
a	$[0\ 1\ 0\ 1\ 0\ 2\ 0]^T$	1	1	1	1	1	1	1
aa	$[0\ 1\ 0\ 1\ 0\ 2\ 0]^T$	1	1	2	2	2	2	2
aat_7	$[0\ 2\ 0\ 0\ 0\ 2\ 0]^T$	1	0	2	1	2	2	2
aat_7t_5	$[0\ 2\ 0\ 0\ 1\ 1\ 0]^T$	1	0	1	1	1	1	1
$aat_7t_5t_5$	$[0\ 2\ 0\ 0\ 2\ 0\ 0]^T$	0	0	0	0	0	0	0
$aat_7t_5t_5a$	$[0\ 2\ 0\ 0\ 2\ 0\ 0]^T$	1	0	0	1	1	0	1
$aat_7t_5t_5aa$	$[0\ 2\ 0\ 0\ 2\ 0\ 0]^T$	2	0	0	2	2	0	2
$aat_7t_5t_5aat_6$	$[1\ 0\ 1\ 0\ 2\ 0\ 0]^T$	0	0	0	0	0	0	0
$aat_7t_5t_5aat_6t_4$	$[0\ 1\ 0\ 1\ 1\ 1\ 0]^T$	0	0	0	0	0	0	0

TABLE I

THE RESULTS OF THE EXAMPLE IN SECTION V.

REFERENCES

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

[2] Caines, P.E., Greiner, R., Wang, S. (1988). *Dynamical logic observers for finite automata*, 27th Conf. on Decision and Control, Austin, Texas, pp. 226–233.

[3] Caines, P.E., Wang, S. (1989). *Classical and logic based regulator design and its complexity for partially observed automata*, 28th Int. Conf. on Decision and Control, Tampa, Florida, pp. 132–137.

[4] Gaubert, S., Giua, A (1999). *Petri net languages and infinite subsets of* $\mathbb{N}^m$, Journal of Computer and System Sciences, Vol. 59, No. 3, pp. 373-391.

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

[6] Giua, A., Júlvez, J., Seatzu, C. (2003). *Marking estimation of Petri nets based on partial observation*, 2003 American Control Conference, Denver, Colorado pp. 326-331.

[7] Kumar, R., Garg, V., Markus, S.I. (1993). *Predicates and predicate transformers for supervisory control of discrete event dynamical systems*, IEEE Trans. on Automatic Control, Vol. 38, No. 2, pp. 232-247.

[8] Meda, M.E., Ramírez, A., Malo, A. (1998). *Identification in discrete event systems*, IEEE Int. Conf. on Systems, Man and Cybernetics, San Diego, California, pp. 740-745.

[9] Murata,T. (1989). *Petri nets: properties, analysis and applications*, Proc. IEEE, Vol. 77, No. 4, pp. 541-580.

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

[11] Peterson, J.L. (1981). *Petri net theory and the modeling of systems*, Prentice-Hall, 1981.

[12] Ramadge, P.J. (1986). *Observability of discrete-event systems*, 25th Conf. on Decision and Control, Athens, Greece, pp. 1108-1112.

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