State Estimation of λ-free Labeled Petri Nets with Contact-Free Nondeterministic Transitions*

Alessandro Giua, Daniele Corona, Carla Seatzu

Dip. Ingegneria Elettrica ed Elettronica, Università di Cagliari,
Piazza d'Armi, 09123 Cagliari, Italy.
Email: {giua,daniele.corona,seatzu}@diee.unica.it

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.

1 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 basis 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 [14] 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.* [9] when defining observer based dynamic controllers in the framework of supervisory predicate control problems. Özveren and Willsky [12] proposed an approach for building observers

*Published as: A. Giua, D. Corona, C. Seatzu, "State Estimation of lambda-free Labeled Petri Nets with Contact-Free Nondeterministic Transitions," *Discrete Event Dynamic Systems*, Vol. 15, No. 1, pp. 85–108, March 2005. The original publication is available at www.springerlink.com.

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. An extension to the case of times DES, where the timing information is used to improve the marking estimate has been presented in [6].

- 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 enabled 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. In particular, we assume that the nondeterminism of the net originates from the presence of transitions that share the same label and that may be simultaneously enabled from a reachable marking. The nondeterminism due to the presence of silent transitions is not considered here. We studied this problem in [7].

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 [4]

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

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 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 [8] 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.

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 [10] 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 [15] used a Controlled Petri Net model for forbidden state avoidance under partial *event* observation with the assumption that the initial marking be known.

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 [11].

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; $Pre : P \times T \Longrightarrow \mathbb{N}$ and $Post : P \times T \Longrightarrow \mathbb{N}$ 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 $M : P \Longrightarrow \mathbb{N}$ 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 $M\ [\varsigma\rangle$ to denote that the sequence of transitions $\varsigma = t_{j_1} \cdots t_{j_k}$ is enabled at M, and we write $M\ [\varsigma\rangle\ M'$ to denote that the firing of ς yields M'. We also denote $\sigma\ :\ T \Longrightarrow \mathbb{N}$ 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 $M_0\ [\varsigma\rangle\ M$. 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 $\sigma \in \mathbb{N}^n$ that satisfies the *state equation* $M = M_0 + C \cdot \sigma$, i.e., $PR(N, M_0) = \{M \in \mathbb{N}^m \mid \exists \sigma \in \mathbb{N}^n \ : \ M = M_0 + C \cdot \sigma\}$. It holds that $R(N, M_0) \subseteq PR(N, M_0)$.

Given a set of places $P' \subseteq P$, we denote $M \uparrow_{P'}$ the projection (i.e., restriction) of M to P'.

A *labeling function* $L : T \rightarrow E$ 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 [13] 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 $L : T \rightarrow E$ 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 $L : T \rightarrow E$ 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 (T^n) is denoted C_e (C^n) and the restriction of the firing vector σ to T_e is denoted σ_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.

We denote as w the word of events associated to the sequence ς, i.e., $w = L(\varsigma)$.

[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 a non erasing labeling function $L : T \rightarrow E$.

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) 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 $\varsigma : M_0[\varsigma\rangle M$ and $L(\varsigma) = w\}$.* ■

The set of consistent markings can be obviously described, on the basis of its definition, with an exhaustive enumeration of all markings.

Algorithm 4. *[8]*
1. Let $w_0 = \varepsilon$ and $\mathcal{C}(w_0) = M_0$.
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 $w_i \preccurlyeq w$, $i = 1, \cdots, k-1$. Furthermore each set $\mathcal{C}(w_i)$ must be explicitly enumerated.

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

Example 5. 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

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

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.

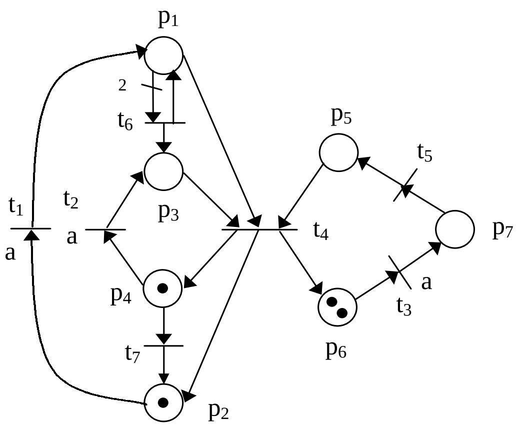

Figure 1: A Petri net system that can only be partially observed

Therefore,

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

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 $\varsigma_1 = t_1 t_3 t_7$, $\varsigma_2 = t_3 t_1 t_7$, $\varsigma_3 = t_3 t_3 t_7$. 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., $\varsigma = t_3 t_3 t_7 t_5 t_5$. ■

4 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 in [8] where 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 ${}^\bullet t_i^\bullet \cap {}^\bullet t_j^\bullet = \emptyset$ and ${}^\bullet t_i \cap t_i^\bullet = \emptyset$.

(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 [8] when the assumption (A5) is removed. More precisely, we show 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.

4.1 Computation of the set of consistent markings

Let us first introduce the following notation.

Definition 6. *Given a marking M and a transition $t \in T$, we define*

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

the enabling degree of transition t at M.

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

$$z(M,\tau) = \sum_{t \in \tau} z(M,t).$$

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

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

■

Remark 7. Note that if all transitions in τ are conflict free[2], then $z(M,\tau)$ represents the number of times transitions in τ may simultaneously fire at M. ■

Theorem 8. *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*

$$\mathcal{C}(w) = \mathcal{M}(w) \stackrel{\text{def}}{=} \{M \in \mathbb{N}^m \mid M = M_{b,w} + \sum_{e \in E^n} C_e \sigma_e; \quad \sigma_e \in \mathcal{S}_e(w)\} \tag{1}$$

where

$$\mathcal{S}_e(w) \stackrel{\text{def}}{=} \{\sigma \in \mathbb{N}^{n_e} \mid (\forall \tau \in \mathcal{T}_e) \quad \begin{array}{l} \sigma(\tau) \leq u_w(\tau), \\ \sigma(T_e) = u_w(T_e)\}, \end{array} \tag{2}$$

*is the set of w-*consistent nondeterministic firing vectors *and the upper bounds $u_w(\tau)$ and $u_w(T_e)$, as well as the marking $M_{b,w}$, are computed using the recursive Algorithm 9.*

Proof. See Appendix. □

Therefore, the number of constraints used to describe the set $\mathcal{S}_e(w)$ is equal to $2^{n_e} - 1$, 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 firstly observe that the firing of a nondeterministic transition t may be *reconstructed* when a deterministic transition t_d is observed and the firing of t is strictly necessary to enable t_d. Therefore, using Algorithm 9, we define the *basis marking* $M_{b,w}$ 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 reconstructed.

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 reconstructed.

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 reconstructed.

[2] Two transitions t_i and t_j are conflict free if they do not share input places, namely ${}^\bullet t_i \cap {}^\bullet t_j = \emptyset$.

Algorithm 9 (Upper bounds and basis marking computation)**.**

1. Let $w = \varepsilon$ and $M_{b,w} = M_0$.
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 ${}^\bullet t \cap ({}^\bullet T^{n\bullet}) = \emptyset$, then (Case A)
$M_{b,we} = M_{b,w} + C(\cdot, t)$
endif
if $P_t \overset{\text{def}}{=} {}^\bullet t \cap (T^{n\bullet}) \neq \emptyset$, then (Case B)
$\sigma_\alpha = \vec{0}$ (a vector of dimension $|T^n| \times 1$)
$flag = 1$
$T_{up} \overset{\text{def}}{=} T^n \cap^\bullet P_t$
for all $\hat{t} \in T_{up}$, then

$$\text{let } \sigma_\alpha(\hat{t}) = \max_{p \in P_t \,:\, Post(p,\hat{t}) \neq 0} \left\{ 0, \left\lceil \frac{Pre(p,t) - M_{b,w}(p)}{Post(p,\hat{t})} \right\rceil \right\}$$

endfor
for all $\tau \in \bigcup_{e \in E^n} 2^{T_e} \setminus \emptyset \;:\; \tau \cap T_{up} \neq \emptyset$, then

$$u_{we}(\tau) = u_w(\tau) - \sum_{t \in \tau} \sigma_\alpha(t)$$

endfor
$M_{b,we} = M_{b,w} + C(\cdot, t) + C^n \sigma_\alpha$
endif
if ${}^\bullet t \cap ({}^\bullet T^n) \neq \emptyset$, then (Case C)
if $flag = 0$, then
$M_{b,we} = M_{b,w} + C(\cdot, t)$
endif
let $\mathcal{T}_r(t) = \{\hat{t} \in T^n \mid {}^\bullet t \cap^\bullet \hat{t} \neq \emptyset\}$
for all $\hat{t} \in \mathcal{T}_r(t)$, then
$u_{we}(\{\hat{t}\}) = \min\{u_w(\{\hat{t}\}), z(M_{b,we}, \hat{t})\}$
for all $\tau \in \mathcal{T}_{L(\hat{t})}$ such that $\hat{t} \in \tau$ with $\tau \neq \{\hat{t}\}$, then
$u_{we}(\tau) = \min\{u_w(\tau), u_{we}(\{\hat{t}\}) + u_w(\tau \setminus \{\hat{t}\})\}$
endfor
endfor
endif

else (Case D)
for all $\tau \in \mathcal{T}_e$, then
$u_{we}(\tau) = \min\{u_w(\tau) + 1, z(M_{b,w}, \tau)\}$
endfor
$u_{we}(T_e) = u_w(T_e) + 1$
$M_{b,we} = M_{b,w}$
endif

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

■

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

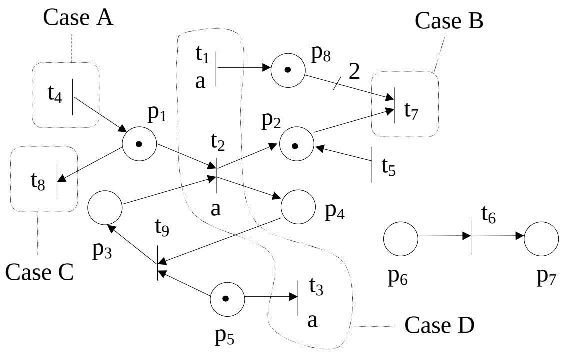

Figure 3: The generic substructure of a more complex Petri net that satisfies the contact-free assumption.

Now, let us discuss in detail all cases in Algorithm 9. 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 $M_{b,w}$ 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 $M_{b,w}$, if for some place $p \in^\bullet t_7$, $M_{b,w}(p) < Pre(p, t_7)$, we know for sure that the nondeterministic transition ${}^\bullet p$ has fired and we can also evaluate (see Algorithm 9) 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 $M_{b,w}$ is updated to $M_{b,we} = M_{b,w} + C(\cdot, t_1) + C(\cdot, t_7)$.

- *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 $M_{b,w}$ is greater than the bound $u_w(\tau)$. Furthermore, we always increment of one 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 reconstructed.

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.

4.2 Computational complexity

Let us now discuss the computational complexity of Algorithm 9.

Proposition 10. When an event e is observed and Algorithm 9 is used to update the basis marking and the upper bounds, the computational complexity, defined as the number of operations required, is of order

$$\mathcal{O}\left(|T^n| \cdot \sum_{e \in E^n} 2^{n_e - 1}\right).$$

Proof. It is immediate to verify that the worst case in terms of computational complexity holds when cases B and C occur simultaneously. As already discussed above, in such a case we first consider case B, and then we consider case C.

The worst-case number of operations required by case B depends on how many times each of the two consecutive *for* cycles is executed, i.e.,

$$\underbrace{|T^n|}_{\text{first } for \text{ cycle}} + \underbrace{\sum_{e \in E^n} 2^{n_e} - |E^n|}_{\text{second } for \text{ cycle}}.$$

The worst-case number of operations required by case C depends on how many times each of the two nested *for* cycles is executed, i.e.,

$$\underbrace{|T^n|}_{\text{first } for \text{ cycle}} \cdot \underbrace{\sum_{e \in E^n} 2^{n_e - 1}}_{\text{second } for \text{ cycle}}.$$

Because $|T^n| \geq 2$, the latter expression has greater order than the first, thus proving the statement. □

4.3 Discussion

In this section we discuss some relevant topics.

4.3.1 Requirement of bounds for each set in $\mathcal{T}_e$

If we assume that no more than two transitions, say $t_{e,1}$ and $t_{e,2}$, may have the same label (i.e., under assumption (A5)) the set $\mathcal{T}_e = \{\{t_{e,1}\}, \{t_{e,2}\}\}$ contains only singleton sets, for all $e \in E^n$. In such a case we formally proved in [8] that we can characterize the set of w-consistent markings by simply computing the upper bounds on the maximum number of times each nondeterministic transition may have fired.

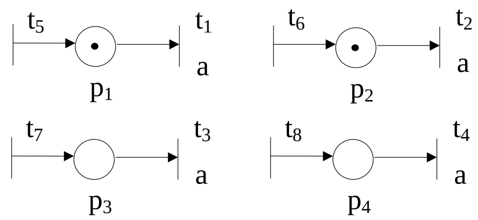

Figure 4: An example showing that singletons in $\mathcal{T}_a$ are not enough to describe $\mathcal{C}(w)$.

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

In the following we denote as $\tau_{i_1 \, \cdots \, i_k}$ 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_ε are t_1 and t_2, thus, in accordance to Algorithm 9, 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 $t_7 t_8 a$ is further observed. The observation of the deterministic transitions t_7 and t_8 only implies that the basis marking is updated to $M_{b,w} = M_{ade} = [1\ 1\ 1\ 1]^T$. 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 $\varsigma = t_7 t_8 t_3 t_4$ 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. ■

4.3.2 Requirement of the contact-free assumption

When the nondeterministic transitions are not conflict free, Remark 7 does not hold anymore. In this case one may think that it may be possible to modify Algorithm 9 for the computation of the bounds so that Equations (1) and (2) still hold.

Unfortunately this is not possible: next example shows that the set of w-consistent nondeterministic firing vectors may be non convex if the contact-freeness assumption is relaxed, hence it cannot be represented by the set (2).

Example 12. Let us consider the Petri net system in Figure 5 whose initial marking is equal to $M_0 = [2\ 0\ 0]^T$. Assume that the word $w = aaaa$ is observed. In this case the only admissible firing vectors are

$$\vec{\sigma}_1 = [2\ 0\ 2\ 0]^T, \quad \vec{\sigma}_2 = [0\ 2\ 0\ 2]^T.$$

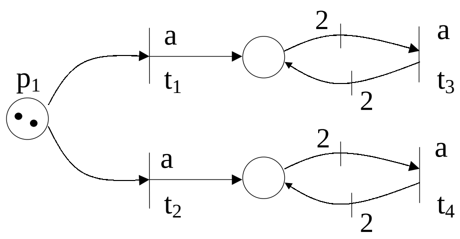

Figure 5: A net where the nondeterministic transitions are not contact-free (see Example 12).

On the contrary, the vector $\vec{\sigma} = [1\ 1\ 1\ 1]^T$ that is a linear combination of $\vec{\sigma}_1$ and $\vec{\sigma}_2$ is not an admissible firing vector, thus proving that the set of w-consistent nondeterministic firing vectors is not convex. ■

4.3.3 Uncertainty about the initial marking

The procedure we have presented in Algorithm 9 is based on the computation of the basis marking $M_{b,w}$ for all words $w \in E^*$. This is only possibile if the initial marking is known.

Note however that even if the initial marking is only known to belong to a given set, the proposed characterization of $\mathcal{C}(w)$ can still be used provided that one of the following two cases occur.

- The initial marking belongs to a set $\mathcal{M}_0$ that is described by constraints of the form (1) and (2).

  In this case we can still apply our approach. In fact, it is sufficient to take $M_{b,\varepsilon}$ equal to the basis marking that defines $\mathcal{M}_0$, and the upper bounds u_ε equal to the upper bounds defining $\mathcal{M}_0$ instead of initializing them to zero.

- The initial marking belongs to a finite set $\mathcal{M}_0 = \{M_0^1, \ldots, M_0^k\}$ with $k < +\infty$.

  In such a case the set of consistent markings can be given as the union of a finite number of sets of consistent markings $\mathcal{C}^i(w)$ of the form (1), each one computed initializing the basis marking to a different marking in $\mathcal{M}_0$.

  Note however that the number of these sets (that is initially equal to k) may decrease as the length of the observed word increases. In fact, for each observed word w and new observed event e, if there exists no marking in $\mathcal{C}^i(w)$ enabling a transition with label e, then we can restrict the set of admissible initial markings to $\mathcal{M}_0 \setminus \{M_0^i\}$.

4.4 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 4.4. Data in the table are then used to construct the set of admissible markings as described in Theorem 8.

w	$M_{b,w}$	$u_w(\tau_1)$	$u_w(\tau_2)$	$u_w(\tau_3)$	$u_w(\tau_{12})$	$u_w(\tau_{13})$	$u_w(\tau_{23})$	$u_w(T_a)$
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 1: The results of the example in Section 4.4.

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

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

The solutions of this integer inequality system are:

$$\begin{aligned}\sigma_1 &= [0\ 0\ 1]^T,\\ \sigma_2 &= [0\ 1\ 0]^T,\\ \sigma_3 &= [1\ 0\ 0]^T,\end{aligned}$$

which substituted in

$$M = M_a + C_a\sigma_i, \quad i = 1, 2, 3$$

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 6 shows the DFA (33 states and 69 transitions) obtained from the non deterministic reachability graph (42 states and 99 transitions) of the net.

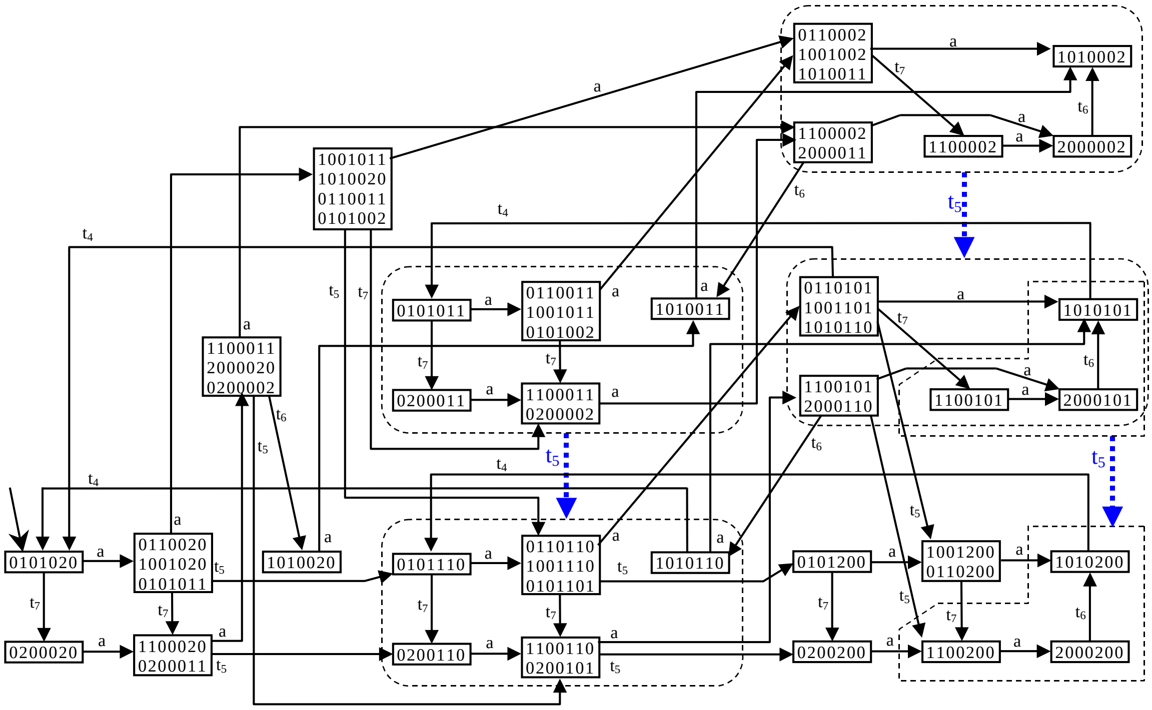

Figure 6: DFA corresponding to the Petri net in Figure 1. The thick dotted blue arrows indicate the existence of an edge from each element of the dashed macrostate. This is to reduce the complexity of the graph.

5 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 prove 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 remove the contact-free assumption, allowing the subnet composed of the nondeterministic transitions to have a more general structure. Note however that, as discussed in Section 4, when the contact-freeness assumption is removed, the form of the linear algebraic characterization cannot be the same, because the set of consistent nondeterministic firing vectors may be a non convex set.

Then, we believe it may be possible to modify the structure of the constraint set to also take into account the case in which only a partial information on the initial marking (not in the forms considered in Subsection 4.3.3) is known.

Appendix

Preliminary results

We first present two technical results.

Lemma 13. *The upper bounds computed using Algorithm 9 are such that for all $a \in E^n$ and for all $\tau \in \mathcal{T}_a$:*

$$u_w(\tau) \leq z(M_{b,w}, \tau).$$

Proof. We prove this by induction on the length of w. Assume that there exists only one nondeterministic event a, thus $T^n \equiv T_a$. Note that this does not affect the validity of the proof thanks to the contact-freeness assumption A4.

(*Basis step*) The result obviously holds for $w = \varepsilon$, since in this case $\forall \tau \in \mathcal{T}_a$ it holds $0 = u_\varepsilon(\tau) \leq z(M_{b,\varepsilon}, \tau)$.

(*Inductive step*) We show that if for a given w, $u_w(\tau) \leq z(M_{b,w}, \tau)$, then $\forall\ e \in E$: $u_{we}(\tau) \leq z(M_{b,we}, \tau)$

We consider the four cases of Algorithm 9.

Case A. In this case bounds u's and enabling degrees z's are not modified and the result follows by induction.

Case B. In this case for all τ it holds

$$u_{we}(\tau) = u_w(\tau) - \sum_{t\in\tau} \sigma_\alpha(t); \qquad \text{and} \qquad z(M_{b,we}, \tau) = z(M_{b,w}, \tau) - \sum_{t\in\tau} \sigma_\alpha(t),$$

and the result follows by induction.

Case C. When case C applies, we can update the values of the bounds u's and enabling degrees z's considering a transition $\hat{t} \in \mathcal{T}_r(t)$ at a time.

(a) It holds $u_{we}(\hat{t}) = \min\{u_w(\hat{t}), z(M_{b,we}, \hat{t})\} \leq z(M_{b,we}, \hat{t})$.

(b) Assume $\hat{t} \notin \tau$. Then $u_{we}(\tau) = u_w(\tau)$ and $z(M_{b,we}, \tau) = z(M_{b,w}, \tau)$ and the result follows by induction.

(c) Assume that $\hat{t} \in \tau$ and $\tau \in \{\hat{t}\}$. Then by definition it holds that

$$\begin{aligned} u_{we}(\tau) &= \min\left\{u_w(\tau), u_{we}(\hat{t}) + u_w(\tau \setminus \{\hat{t}\})\right\} \leq u_{we}(\hat{t}) + u_w(\tau \setminus \{\hat{t}\}) \\ &\leq z(M_{b,we}, \hat{t}) + z(M_{b,w}, \tau \setminus \{\hat{t}\}) = z(M_{b,we}, \hat{t}) + z(M_{b,we}, \tau \setminus \{\hat{t}\}) \\ &= z(M_{b,we}, \tau) \end{aligned}$$

where the second inequality follows from the inductive step.

Case D. By definition, $u_{we}(\tau) = \min\{u_w(\tau), z(M_{b,w}, \tau)\} \leq z(M_{b,w}, \tau) = z(M_{b,we}, \tau)$.

□

Corollary 14. *When a nondeterministic event $e \in E^n$ is observed, the upper bounds computed using Algorithm 9 (case D) are such that for all $e \in E^n$ and for all $\tau \subseteq \mathcal{T}_e$:*

$$u_w(\tau) \leq u_{we}(\tau) \leq u_w(\tau) + 1.$$

Proof. By definition, in case D of the algorithm the bounds are updated as follows:

$$u_{we}(\tau) = \min\{u_w(\tau) + 1, z(M_{b,w}, \tau)\}.$$

Thus the second inequality is obvious, while the first one can be proved observing that

$$u_{we}(\tau) = \min\{u_w(\tau) + 1, z(M_{b,w}, \tau)\} \geq \min\{u_w(\tau), z(M_{b,w}, \tau)\} = u_w(\tau)$$

where the last equality follows from the previous lemma. □

Main result: proof of Theorem 8

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

(*Basis step*) When no event is observed, i.e., $w = \varepsilon$, using equation (1) we have that $\mathcal{M}(\varepsilon) = \{M_0\}$, thus the statement of the proposition holds.

(*Inductive step*) Assume that $\mathcal{M}(w) = \mathcal{C}(w)$ for a given word w.

Let e be a newly observed event. We have to prove that $\mathcal{M}(we) = \mathcal{C}(we)$.

For simplicity of presentation in the following we assume that there exists only one nondeterministic event a, thus $T^n \equiv T_a$. Note that such an assumption does not affect the validity of the proof thanks to the *contact-freeness* hypothesis.

In the following $\mathcal{S}_a(w)$, $\mathcal{M}(w)$, $\mathcal{C}(w)$, $u_w(\tau)$, $M_{b,w}$ and $z(M_{b,w}, \tau)$ are simply denoted $\mathcal{S}$, $\mathcal{M}$, $\mathcal{C}$, $u(\tau)$, M_b and $z(\tau)$ respectively, while the corresponding elements associated to we are denoted $\mathcal{S}'$, $\mathcal{M}'$, $\mathcal{C}'$, $u'(\tau)$, M_b' and $z'(\tau)$.

Part 1: we show that $\mathcal{M}' \subseteq \mathcal{C}'$

When a deterministic event t is observed (cases A, B, and C of Algorithm 9), the statement is proved if we show that for all $M' \in \mathcal{M}'$ the predecessor marking $M \stackrel{\text{def}}{=} M' - C(\cdot, t)$ is such that $M \in \mathcal{C} = \mathcal{M}$, and M enables t.

Equivalently, we will prove that

$$\begin{array}{l}(\forall \sigma' \in \mathcal{S}')\ M' \stackrel{\text{def}}{=} M'_b + C_a\sigma' \Longrightarrow \\ (\exists \sigma \in \mathcal{S})\ M \stackrel{\text{def}}{=} M'_b + C_a\sigma' - C(\cdot, t) = M_b + C_a\sigma \text{ and } M \geq Pre(\cdot, t).\end{array}$$

We discuss the three cases separately.

Case A. In such a case $\mathcal{S} = \mathcal{S}'$, therefore if we take $\sigma = \sigma'$ we also have $\sigma \in \mathcal{S}$. Moreover, being $M'_b = M_b + C(\cdot, t)$, then $M \stackrel{\text{def}}{=} M'_b + C_a\sigma' - C(\cdot, t) = M_b + C_a\sigma$. Finally, to prove that $M \geq Pre(\cdot, t)$, it is sufficient to observe that the firing of t yield $M' \stackrel{\text{def}}{=} M'_b + C_a\sigma' \geq Post(\cdot, t) \Longrightarrow M_b + Post(\cdot, t) - Pre(\cdot, t) + C_a\sigma' \geq Post(\cdot, t) \Longrightarrow M = M_b + C_a\sigma \geq Pre(\cdot, t)$, thus proving the statement.

Case B. In this case there is no a priori inclusion relationship among $\mathcal{S}$ and $\mathcal{S}'$. If we take $\sigma = \sigma' + \sigma_\alpha$ (where σ_α is specified in Algorithm 9) then $\sigma \in \mathcal{S}$. In fact by construction, for all $\tau \subseteq T_a$,

$$\sigma'(\tau) \leq u'(\tau) = u(\tau) - \sum_{t \in \tau} \sigma_\alpha(t) \quad \Longrightarrow \quad \sigma(\tau) = \sigma'(\tau) + \sum_{t \in \tau} \sigma_\alpha(t) \leq u(\tau).$$

Therefore, being $M'_b = M_b + C(\cdot, t) + C_a\sigma_\alpha \Longrightarrow M \stackrel{\text{def}}{=} M'_b + C_a\sigma' - C(\cdot, t) = M_b + C_a\sigma$. To prove that $M \geq Pre(\cdot, t)$, we observe that the firing of t yield $M' \stackrel{\text{def}}{=} M'_b + C_a\sigma' \geq Post(\cdot, t) \Longrightarrow M_b + C_a\sigma_\alpha + Post(\cdot, t) - Pre(\cdot, t) + C_a\sigma' \geq Post(\cdot, t) \Longrightarrow M = M_b + C_a\sigma \geq Pre(\cdot, t)$, thus proving the statement.

Case C. In such a case $\mathcal{S}' \subseteq \mathcal{S}$, therefore given a $\sigma' \in \mathcal{S}'$, we can always choose $\sigma = \sigma'$ and $\sigma \in \mathcal{S}$. Moreover, being $M'_b = M_b + C(\cdot, t) \Longrightarrow M \stackrel{\text{def}}{=} M'_b + C_a\sigma' - C(\cdot, t) = M_b + C_a\sigma$. Finally, to prove that $M \geq Pre(\cdot, t)$, as in the previous items, we observe that the firing of t yield $M' \stackrel{\text{def}}{=} M'_b + C_a\sigma' \geq Post(\cdot, t) \Longrightarrow M_b + Post(\cdot, t) - Pre(\cdot, t) + C_a\sigma \geq Post(\cdot, t) \Longrightarrow M = M_b + C_a\sigma \geq Pre(\cdot, t)$, thus proving the statement.

When the nondeterministic event a is observed (case D of Algorithm 9), the statement is proved if we show that for all $M' \in \mathcal{M}'$, among the predecessor markings of M'

$$\mathcal{P}(M') \stackrel{\text{def}}{=} \{M \in \mathbb{N}^m \mid (\exists t \in T_a)\ M[t\rangle M'\},$$

there exists one marking $M \in \mathcal{P}(M')$ such that $M \in \mathcal{C} = \mathcal{M}$, and M enables t.

Case D. We prove this by induction on the cardinality of the set $|T_a|$, i.e., by induction on the number of nondeterministic transitions.

(*Base step*) When $|T_a| = 2$, the result holds because we have shown in [8] that $\mathcal{M}' = \mathcal{C}'$ [3].

[3]Note that in [8] we considered a slightly different linear algebraic characterization of the set of consistent markings. In fact, in [8] we do not define the basis marking, and the admissible firing vectors are assumed to be firable at the initial marking M_0. The components of the admissible firing vectors associated to deterministic transitions are exactly known, while an upper bound is given on the maximum number of times each nondeterministic transition may have fired. Finally, we also know how may times each nondeterministic event has been observed.

Using the notation of [8], if we assume that when the observed word is w, $M_0 \stackrel{\text{def}}{=} M_b$ and $n_q \stackrel{\text{def}}{=} 0$ for all $t_q \in T^d$, then the two linear characterizations are coincident. In fact, for all nondeterministic transition t, $z_r^{in}(t)$ is equal by definition to the enabling degree $z(t)$ at the actual basis marking M_b.

(*Inductive step*) Assume now that for $|T_a| = n-1$ it holds that $\mathcal{M}' \subseteq \mathcal{C}'$.

We prove the result holds also when $|T_a| = n$.

In fact, given a $\sigma' \in \mathcal{S}'$, or equivalently a marking $M' \stackrel{\text{def}}{=} M'_b + C_a\sigma' \in \mathcal{M}'$, let us define the set

$$T^+ = \{t \in T_a \mid \sigma'(t) = u'(t) = u(t) + 1\}$$

of the nondeterministic transitions that according to the chosen σ' have fired a number of times greater than their firing bound u at the previous step.

It is immediate to show by contradiction that $T_a \neq T^+$. In fact, assume $T_a = T^+$: then[4]

$$u'(T_a) \geq \sigma'(T_a) = \sum_{t \in T_a} \sigma'(t) = \sum_{t \in T_a} u'(t) = |T_a| + \sum_{t \in T_a} u(t) \geq |T_a| + u(T_a) = n + u(T_a),$$

thus contradicting the fact that $u'(T_a) = u(T_a) + 1$.

Assume $\tilde{t}$ is a nondeterministic transition that does not belong to T^+ and let $\tilde{n} = \sigma'(\tilde{t}) \leq u(\tilde{t})$. We will show that among all possible predecessors of M' there exists a consistent marking $M \in \mathcal{C}$ that can be reached from the basis marking M_b firing transition $\tilde{t}$ exactly $\tilde{n}$ times. Since M and M' correspond to firing vectors $\sigma \in \mathcal{S}$ and $\sigma' \in \mathcal{S}'$ with $\sigma(\tilde{t}) = \sigma'(\tilde{t})$, then $\exists\, \hat{t} \in T_a \setminus \{\tilde{t}\}$ such that $M\ [\ \hat{t}\ \rangle\ M'$.

To show this we define two new constraint sets $\tilde{\mathcal{S}}$ and $\tilde{\mathcal{S}}'$ obtained, resp., from $\mathcal{S}$ and $\mathcal{S}'$ substituting $\sigma(\tilde{t}) = \sigma'(\tilde{t}) = \tilde{n}$.

- Note that while $\mathcal{S}$ contains $2^n - 2$ inequality constraints, $\tilde{\mathcal{S}}$ contains $2^{n-1} - 2$ inequality constraints: in fact the inequality $\tilde{n} \leq u(\tilde{t})$ is trivially verified and can be removed, while for any other non empty $\tau \subseteq T_a \setminus \{\tilde{t}\}$ we have that the two inequalities

  $$\begin{array}{lcl} \sigma(\tau) & \leq & u(\tau) \\ \sigma(\tau) + \tilde{n} & \leq & u(\tau \cup \{\tilde{t}\}) \end{array}$$

  can be compacted into a single inequality

  $$\sigma(\tau) \quad \leq \quad \tilde{u}(\tau) \quad \stackrel{\text{def}}{=} \quad \min\left\{u(\tau), u(\tau \cup \{\tilde{t}\}) - \tilde{n}\right\}.$$

  The same reasoning applies to the set $\tilde{\mathcal{S}}'$ whose $2^{n-1} - 2$ inequalities take the from

  $$\sigma'(\tau) \quad \leq \quad \tilde{u}'(\tau) \quad \stackrel{\text{def}}{=} \quad \min\left\{u'(\tau), u'(\tau \cup \{\tilde{t}\}) - \tilde{n}\right\}.$$

  Finally, the equality constraint of $\tilde{\mathcal{S}}$ and $\tilde{\mathcal{S}}'$ are, respectively

  $$\sigma(T_a \setminus \{\tilde{t}\}) = \tilde{u}(T_a \setminus \{\tilde{t}\}) = u(T_a) - \tilde{n}; \qquad \sigma(T_a \setminus \{\tilde{t}\}) = \tilde{u}'(T_a \setminus \{\tilde{t}\}) = u'(T_a) - \tilde{n}.$$

- Let us define $\tilde{M}_b = M_b + \tilde{n}C(\cdot, \tilde{t})$ and $\tilde{M}'_b = M'_b + \tilde{n}C(\cdot, \tilde{t})$. We can also denote $\tilde{z}(\tau) = \sum_{t \in \tau} z(\tilde{M}_b, t)$: obviously, by assumption A4, if $\tilde{t} \notin \tau$ it also holds that $\tilde{z}(\tau) = \sum_{t \in \tau} z(M_b, t) = z(\tau)$.

- We now want to show that the new bounds of the set $\tilde{\mathcal{S}}'$ are related to the bounds of the set $\tilde{\mathcal{S}}$ as prescribed by Algorithm 9, i.e., we need to show that

  $$\tilde{u}'(\tau) = \min\left\{\tilde{u}(\tau) + 1, \tilde{z}(\tau)\right\} \tag{3}$$

  where the LHS is

  $$\begin{aligned} \tilde{u}'(\tau) &= \min\left\{u'(\tau), u'(\tau \cup \{\tilde{t}\}) - \tilde{n}\right\} \\ &= \min\left\{\min\left\{u(\tau) + 1, z(\tau)\right\}, u'(\tau \cup \{\tilde{t}\}) - \tilde{n}\right\} \\ &= \min\left\{u(\tau) + 1, z(\tau), u'(\tau \cup \{\tilde{t}\}) - \tilde{n}\right\}, \end{aligned}$$

[4]Here we are using the fact that $\sum_{t \in T_a} u(t) \geq u(T_a)$, otherwise $\mathcal{C} = \mathcal{M} = \emptyset$.

and the RHS is

$$\begin{aligned}\min\{\tilde{u}(\tau)+1,\tilde{z}(\tau)\} &= \min\left\{\min\left\{u(\tau),u(\tau\cup\{\tilde{t}\})-\tilde{n}\right\}+1,\tilde{z}(\tau)\right\}\\ &= \min\left\{u(\tau)+1,z(\tau),u(\tau\cup\{\tilde{t}\})-\tilde{n}+1\right\}.\end{aligned}$$

Recalling Corollary 14, one can immediately see that Equation (3) may only be violated if the LHS and RHS minima occur, respectively, at $u'(\tau\cup\{\tilde{t}\})-\tilde{n}$ and at $u(\tau\cup\{\tilde{t}\})-\tilde{n}+1$, and it holds

$$u'(\tau\cup\{\tilde{t}\}) \;=\; u(\tau\cup\{\tilde{t}\}) \;<\; u(\tau\cup\{\tilde{t}\})+1.$$

However, this would imply that

$$\begin{aligned}&\min\left\{u(\tau\cup\{\tilde{t}\})+1,z(\tau\cup\{\tilde{t}\})\right\}=u'(\tau\cup\{\tilde{t}\})=u(\tau\cup\{\tilde{t}\}) &\Longrightarrow\\ &\quad z(\tau\cup\{\tilde{t}\})=z(\tau)+z(\tilde{t})=u(\tau\cup\{\tilde{t}\}) &\Longrightarrow\\ &\quad z(\tau)=u(\tau\cup\{\tilde{t}\})-z(\tilde{t}).\end{aligned}$$

But this leads to a contradiction, because we assumed that the RHS minimum occurs at $u(\tau\cup\{\tilde{t}\})-\tilde{n}+1$, hence

$$z(\tau)\geq u(\tau\cup\{\tilde{t}\})-\tilde{n}+1\geq u(\tau\cup\{\tilde{t}\})-z(\tilde{t})+1,$$

being $\tilde{n}\leq u(\tilde{t})\leq z(\tilde{t})$ by Lemma 13.

- If we consider the set

$$\tilde{\mathcal{M}}=\{M^m\in\mathbb{N}\mid M=\tilde{M}_b+\tilde{C}_a\tilde{\sigma},\tilde{\sigma}\in\tilde{\mathcal{S}}\}\subseteq\mathcal{M}=\mathcal{C}$$

where $\tilde{C}_a$ is the restriction of the incidence matrix to $T_a\setminus\{\tilde{t}\}$, by the assumption at the inductive step (set $\tilde{\mathcal{S}}'$ contains $n-1$ variables) it follows that for any choice of $\tilde{\sigma}'\in\tilde{\mathcal{S}}'$ the marking $\tilde{M}'=\tilde{M}'_b+\tilde{C}_a\tilde{\sigma}'$ is such that there exists a $\tilde{M}\in\tilde{\mathcal{M}}$ enabling a transition $\hat{t}\in T_a\setminus\{\tilde{t}\}$ and such that $\tilde{M}[\hat{t}\rangle\tilde{M}'$. If, in particular, we choose $\tilde{\sigma}'$ such that $\tilde{\sigma}'(t)=\sigma'(t)\;\forall\, t\in T_a\setminus\{\tilde{t}\}$ we have that $M'=\tilde{M}'$, and this concludes the proof.

Part 2: we show that $\mathcal{M}'\supseteq\mathcal{C}'$

When a deterministic event t is observed, the statement is proved if we demonstrate that

$$\begin{aligned}&(\forall\sigma\in\mathcal{S})\quad \text{if } M\overset{\text{def}}{=}M_b+C_a\sigma\geq Pre(\cdot,t)\quad\Longrightarrow\\ &(\exists\sigma'\in\mathcal{S}')\quad M'\overset{\text{def}}{=}M+C(\cdot,t)=M'_b+C_a\sigma'.\end{aligned}$$

We discuss separately the four cases of Algorithm 9.

Case A. Let $\sigma\in\mathcal{S}$ be such that $M\overset{\text{def}}{=}M_b+C_a\sigma\geq Pre(\cdot,t)$. Because $\mathcal{S}=\mathcal{S}'$, if we take $\sigma'=\sigma$ then $\sigma'\in\mathcal{S}'$. Finally, $M[t\rangle M'$ where

$$M'=M_b+C(\cdot,t)+C_a\sigma=M'_b+C_a\sigma=M'_b+C_a\sigma'.$$

Case B. Let $\sigma\in\mathcal{S}$ be such that $M\overset{\text{def}}{=}M_b+C_a\sigma\geq Pre(\cdot,t)$. Because $M[t\rangle$ then $\sigma\geq\sigma_\alpha$ (by Algorithm 9). We can thus take $\sigma'=\sigma-\sigma_\alpha$ and observe that $\sigma'\in\mathcal{S}'$ because for all $\tau\in\mathcal{T}_a$,

$$\sigma'(\tau)=\sigma(\tau)-\sigma_\alpha(\tau)\leq u(\tau)-\sum_{t\in\tau}\sigma_\alpha(t)=u'(\tau),$$

while

$$\sigma'(T_a)=\sigma(T_a)-\sigma_\alpha(T_a)=u(T_a)-\sum_{t\in T_a}\sigma_\alpha(t)=u'(T_a).$$

Finally, $M[t\rangle M'$ where

$$M'=M_b+C(\cdot,t)+C_a\sigma=M'_b-C_a\sigma_\alpha+C_a\sigma=M'_b+C_a\sigma'.$$

Case C. Given a $\sigma \in \mathcal{S}$ such that $M \stackrel{\text{def}}{=} M_b + C_a\sigma \geq Pre(\cdot, t)$. Because $M[t\rangle$ then for all $\hat{t} \in \mathcal{T}_r(t)$ it holds $\sigma(\hat{t}) \leq z'(\hat{t})$.

Let us take $\sigma' = \sigma$ and observe that for all $\tau \in \mathcal{T}_a$ it holds $\sigma'(\tau) \leq u'(\tau)$. To show this, we can update the values of $u(\tau)$ considering a transition $\hat{t} \in T_a$ at a time.

(a) Assume $\tau = \{\hat{t}\}$. It holds $\sigma(\hat{t}) \leq u(\hat{t})$ and $\sigma(\hat{t}) \leq z'(\hat{t})$ then $\sigma'(\tau) = \sigma(\tau) \leq \min\{u(\hat{t}), z'(\hat{t})\} = u'(\hat{t})$.

(b) Assume $\tau \in \mathcal{T}_a$ and $\hat{t} \notin \tau$. Then $\sigma'(\tau) = \sigma(\tau) \leq u(\tau) = u'(\tau)$.

(c) Assume $\tau \in \mathcal{T}_a \setminus \{\hat{t}\}$ and $\hat{t} \in \tau$. Then by definition it holds that $\sigma(\tau) \leq u(\tau)$ and $\sigma(\tau) = \sigma(\hat{t}) + \sigma(\tau \setminus \{\hat{t}\}) \leq u'(\hat{t}) + u(\tau \setminus \{\hat{t}\})$ hence

$$\sigma'(\tau) = \sigma(\tau) \leq \min\left\{u(\tau), u'(\hat{t}) + u(\tau \setminus \{\hat{t}\})\right\} = u'(\tau).$$

Furthermore, for this choice of σ' the equality constraint is verified as well, because $\sigma'(T_a) = \sigma(T_a) = u(T_a) = u'(T_a)$. This shows that $\sigma' \in \mathcal{S}'$.

Finally it holds $M[t\rangle M'$ where

$$M' = M_b + C(\cdot, t) + C_a\sigma = M'_b + C_a\sigma = M'_b + C_a\sigma'.$$

Case D. Given a $\sigma \in \mathcal{S}$ let $M \stackrel{\text{def}}{=} M_b + C_a\sigma$. If $M[\hat{t}\rangle$ with $\hat{t} \in T_a$, then $\sigma(\hat{t}) < z(\hat{t})$. This also implies that for all non empty $\tau \subseteq T_a$ such that $\hat{t} \in \tau$ it holds: $u'(\tau) = u(\tau) + 1$.

Let us take σ' such that $\sigma'(\hat{t}) = \sigma(\hat{t}) + 1$ and $\sigma'(t) = \sigma(t)$ if $t \neq \hat{t}$. We show that $\sigma' \in \mathcal{S}'$. In fact:

(a) Assume $\tau \in \mathcal{T}_a$ and $\hat{t} \notin \tau$. Then $\sigma'(\tau) = \sigma(\tau) \leq u(\tau) \leq u'(\tau)$ (where the last inequality follows from Corollary 14.

(b) Assume $\tau \in \mathcal{T}_a$ and $\hat{t} \in \tau$. Then $\sigma'(\tau) = \sigma(\tau) + 1 \leq u(\tau) + 1 = u'(\tau)$.

(c) Assume $\tau = T_a$. Then $\sigma'(T_a) = \sigma(T_a) + 1 = u(T_a) + 1 = u'(T_a)$.

Finally it holds $M[t\rangle M'$ where

$$M' = M_b + C(\cdot, \hat{t}) + C_a\sigma = M'_b + C(\cdot, \hat{t}) + C_a\sigma = M'_b + C_a\sigma'.$$

□

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., Seatzu, C., Basile, F. (2004). "Observer based state-feedback control of timed Petri nets with deadlock recovery," *IEEE Trans. on Automatic Control*, Vol. 49, No. 1. pp. 17-29.

[7] Giua, A., Corona, D., Seatzu, C. (2004). "Marking estimation of Petri nets with silent transitions," submitted to the *2004 IEEE Int. Conf. on Decision and Control*.

[8] Giua, A., Júlvez, J., Seatzu, C. (2003). "Marking estimation of Petri nets with λ-free labeling," *Proc. Workshop on Discrete Event Systems Control*, Eindhoven, The Netherlansd, pp. 75-95. Revised version: "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, 2004 (to appear).

[9] 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.

[10] 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.

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

[12] 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.

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

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

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