THE OBSERVER COVERABILITY GRAPH FOR THE ANALYSIS OF OBSERVABILITY PROPERTIES OF PLACE/TRANSITION NETS

Alessandro Giua, Carla Seatzu

Department of Electrical and Electronic Engineering, University of Cagliari, Italy
fax: +39 (070) 675-5900
e-mail: {giua,seatzu}@diee.unica.it.

Keywords: Discrete event systems; Petri nets; observers.

Abstract

In this paper we discuss the problem of estimating the marking of a Place/Transition net based on event observation, assuming that the net structure is known while the initial marking is not known. We consider different observability properties, some of which are new and some of which have already been defined by the authors in previous works, where a characterization based on the net language was also given to prove that they are decidable. Checking for language inclusion is difficult, thus in this paper we introduce a useful analysis tool, called observer coverability graph, *that represents both the set of reachable markings of a net system and the corresponding estimate error. We also show that the graph provides either semi–decision or decision conditions for the considered properties.*

1 Introduction

Observability is a fundamental property that has received a lot of attention in the framework of time–driven systems, given the importance of reconstructing plant states that cannot be measured. Although less popular in the case of discrete–event systems, the issue of state estimation has been discussed in the literature. For systems represented by finite automata, Ramadge [7] was the first to show how an observer could be designed for a partially observed system. Other authors further explored this issue and we can recall the work of Caines *et al.* [1, 2] and Özveren and Willsky [6] on the design of observers for automata, and the related results of Kumar *et al.* [5] in the framework of supervisory predicate control problems.

The main drawback of the automata based approach is the requirement that the set of consistent states — i.e., the set of states in which the systems may presently be given the observed behavior — must explicitly be enumerated. This was the main motivation that led some researchers to explore the observability properties of other models than automata, and in particular Petri nets have been considered.

As far as we know, the first approach to the design of observers for Petri net models was presented by one of us in [3]. In that work a general framework was introduced that was further explored in [4], and on which the results presented in this paper are also founded. This framework provides a useful paradigm that can be applied to different settings, from discrete event control, to failure diagnosis and error recovery. The main advantage of the approach introduced in [3] is that it allows one to compute an estimate of the marking (i.e., of the state), while the special structure of Petri nets permits to determine, using linear algebraic tools, if a given marking is consistent without the explicit enumeration of the (possibly infinite) consistent set.

A related approach was also used by Meda and Ramírez [8], who used Interpreted Petri nets to model the system and the observer. Ramirez *et al.* in [10] showed that observability defined as in [8] is equivalent to observability in [3], and provided algorithms to construct an observer for binary Interpreted Petri nets when the observability property is verified.

In this paper we consider the marking estimation problem presented in [3] where an algorithm was given to estimate the actual marking of the net based on the observation of a word of events (i.e., transition firings), under the assumption that the net structure is known while the initial marking is not known. The estimate is always a lower bound of the actual marking. The system that computes the estimate is called an observer.

The error function between the actual marking and the estimate was shown in [3] to be a monotonically non-increasing function of the observed word length. Observed words that lead to a null error are said to be "complete". Complete observers are the discrete-event counterpart of asymptotic observers for time-driven systems.

In [4] we defined several observability properties and showed that they are decidable. In particular we considered two main properties. *Marking observability* (MO) means that there exists at least one word that is complete, while *strong marking observability* (SMO) means that all words can be completed in a finite number of steps into a complete word. We also set up a hierarchy considering the possibility that the two properties are satisfied by a net N starting from an initial marking M_0, by a net N starting from any marking M reachable from an initial marking M_0 (uniform observability) or by a net N starting from any marking in $\mathbb{N}^m$ (structural observability) where m is the number of places of the net [4].

A characterization based on the net language for both marking and strong marking observability was given in [3], where it was proven that these properties are decidable. In [4] the decidability of (strong) uniform and (strong) structural marking observability has been proved by reducing them to other decision problems (e.g., home–space properties, marking reachability, existence of repetitive sequences), that can be checked

Published in the *Proc. 6th European Control Conference* (Porto, Portugal), pp. 1339–1344, September 2001.

using algorithms well known from the literature.

In this paper we first extend the notion of completeness and observability with respect to a single place. This is useful because sometimes one is only interested in reconstructing the marking of a subset of places. We also introduce a useful tool to prove some of the above properties without resorting to the study of the net language. This tool is the *observer coverability graph* (OCG), and can be seen as an extension of the classical coverability graph of Place/Transition nets for the analysis of observability properties. The OCG represents both the set of reachable markings of a net system and the error of the estimate computed in accordance with the estimation algorithm in [3]. More precisely, each node of the OCG contains a vector covering a marking of the net and a vector that keeps track of the estimation error on each place of the net.

The main results of this paper are two. Firstly, we give a procedure for the construction of this graph, and show that it is always finite. Secondly, we show that the OCG provides simple semi–decision (i.e., only sufficient) conditions for the completeness of a word and for the marking observability of a net system, and necessary and sufficient conditions for the strong marking observability of a net system.

This framework provides a useful paradigm that can be applied to different settings, from discrete event control, to failure diagnosis and error recovery. The assumption that only event occurrences, i.e., transition firings, may be observed — while the plant state, i.e., the marking, cannot — is common in discrete event control. The assumption that the state of the plant is not known (or is only partially known) is natural during error recovery. Consider for instance the case of a plant remotely controlled: if the communication fails the state may evolve and when the communication is re–established the state will be at best partially known. In a manufacturing environment, one may consider the case in which resources (i.e., tokens) enter unobserved, or in which we know how many resources have entered the system but not their exact location.

2 Background

In this section we first recall some basic terminology on Petri nets, then we recall some preliminary concepts already presented in [3].

2.1 Petri nets

In this subsection we recall the Petri net formalism used in this paper. For a more comprehensive introduction to Petri nets see [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. The *incidence matrix* of the net is defined as $C(p,t) = Post(p,t) - Pre(p,t)$.

A *marking* is a vector $M : P \to \mathbb{N}$ that assigns to each place of a P/T net a non-negative number of tokens, represented by black dots. 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 if $M \geq Pre(\cdot, t)$ (where $Pre(\cdot, t)$ denotes the column of Pre corresponding to transition t) and may fire yielding the marking $M' = M + C(\cdot, t)$. We write $M\ [w\rangle\ M'$ to denote that the enabled sequence of transitions w may fire at M yielding M'; we use the notation $M' = w(M)$ and $M = w^{-1}(M')$. Moreover, we denote $w(M_0) = M_w$. Finally, we denote as w_0 the sequence of null length. The set of all sequences firable in $\langle N, M_0 \rangle$ is denoted $L(N, M_0)$ (this is also called the prefix-closed free language of the net).

Let $w = t_{\alpha_1}, t_{\alpha_2}, \cdots, t_{\alpha_k}$ be a sequence in $L(N, M_0)$. The sequence $w_i = t_{\alpha_1}, \cdots, t_{\alpha_i}$ with $i \in \mathbb{N}$ and $i < k$ is a prefix of w of length i and we write $w_i \preccurlyeq w$.

A marking M is *reachable* in $\langle N, M_0 \rangle$ iff there exists a firing sequence w such that $M_0\ [w\rangle\ M$. The set of all markings reachable from M_0 defines the reachability set of $\langle N, M_0 \rangle$ and is denoted $R(N, M_0)$.

A *repetitive* sequence w is such that $M[w\rangle M'$ with $M' \geq M$. Then $\forall\, i \geq 1$, w^i is enabled at M.

Finally, we denote $\vec{0}_m$ ($\vec{1}_m$) a $m \times 1$ vector of zeros (ones).

2.2 Estimate and error

The aim of this subsection is that of recalling some preliminary concepts already presented in [3]. The proofs of all propositions are omitted and can be found in [3].

Firstly, we recall an algorithm for estimating the state of a net system $\langle N, M_0 \rangle$ whose marking cannot be directly observed under the following assumptions.

A1) The structure of the net $N = (P, T, Pre, Post)$ is known, while the initial marking M_0 is not.

A2) The event occurrences (i.e., the transition firings) can be observed.

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

Definition 1. *Given an observed word w, the set of w* consistent markings *is* $\mathcal{M}(w) = \{M \mid \exists M' \in \mathbb{N}^m, M'[w\rangle M\}$.

Given an evolution of the net $M_{w_0}[t_{\alpha_1}\rangle M_{w_1}[t_{\alpha_2}\rangle \cdots$, we use the following algorithm to compute the estimate μ_{w_i} of each actual marking M_{w_i} based on the observation of the word of events $w_i = t_{\alpha_1}, t_{\alpha_2}, \cdots, t_{\alpha_i}$.

Algorithm 2 ([3] M. Estimation with Event Observation).
1. Let the initial estimate be $\mu_{w_0} = \vec{0}_m$.
2. Let $i = 1$.
3. Wait until t_{α_i} fires.
4. Update the estimate $\mu_{w_{i-1}}$ to μ'_{w_i} with $\mu'_{w_i}(p) = \max\{\mu_{w_{i-1}}(p), Pre(p, t_{\alpha_i})\}$.
5. Let $\mu_{w_i} = \mu'_{w_i} + C(\cdot, t_{\alpha_i})$.
6. Let $i = i + 1$.
7. Goto 3. ■

Note that in step 4. of the algorithm we update the previously computed estimate $\mu_{w_{i-1}}$, since the firing of t_{α_i} implies that $M_{w_{i-1}} \geq Pre(\cdot, t_{\alpha_i})$. In the following we will always denote

the estimate computed by this algorithm after having observed the word w as μ_w.

Let us observe that the knowledge of the actual estimate and of the structure of the net, also enables us to compute an estimate of the initial marking as $\mu_{0,w} = w^{-1}(\mu_w)$.

The estimate computed by Algorithm 2 is a lower bound on the actual marking of the net.

Proposition 3 ([3]). *Let $w = t_{\alpha_1} t_{\alpha_2} \cdots \in L(N, M_0)$ be an observed string and w_i its prefix of length i. Then $\forall i$, holds $\mu_{w_i} \leq \mu'_{w_{i+1}} \leq M_{w_i}$.*

In [3] it has been given an easy characterization of the set of consistent markings in terms of estimate.

Theorem 4 ([3]). *Given an observed word $w \in L(N, M_0)$ and the estimated marking μ_w computed by Algorithm 2, the set of w* consistent markings *is $\mathcal{M}(w) = \{M \in \mathbb{N}^m \mid M \geq \mu_w\}$.*

In [4] we have also defined a meaningful measure of the place estimation error, as the token difference between a marking and its estimate in a given place.

Definition 5 ([4]). *Let us consider a place $p \in P$ and an observed word $w \in L(N, M_0)$. Let M_w and μ_w be the corresponding marking and its estimate. The* place estimation error *in p is $e_p(M_w, \mu_w) = M_w(p) - \mu_w(p)$ and its update after the firing of t is $e_p(M_w, \mu'_{wt}) = M_w(p) - \mu'_{wt}(p)$.*

Analogously, it is possible [3] to define a measure of the estimation error, as the token difference between a marking and its estimate.

Definition 6 ([3]). *Given a marking M_w and its estimate μ_w, the* estimation error *is $e(M_w, \mu_w) = \sum_{p \in P} e_p(M_w, \mu_w) = \vec{1}_m^T \cdot (M_w - \mu_w)$ and its update after the firing of t is $e(M_w, \mu'_{wt}) = \vec{1}_m^T \cdot (M_w - \mu'_{wt})$.*

Note that the place estimation error is a monotonically non-increasing function of the observed word length.

Proposition 7 ([4]). *Let $w = t_{\alpha_1} t_{\alpha_2} \cdots \in L(N, M_0)$ be an observed word and w_i its prefix of length i. Then $\forall i$ and $\forall p$: $e_p(M_{w_i}, \mu_{w_i}) \geq e_p(M_{w_i}, \mu'_{w_{i+1}}) = e_p(M_{w_{i+1}}, \mu_{w_{i+1}})$, and $e_p(M_{w_i}, \mu'_{w_{i+1}}) = \min\left\{e_p(M_{w_i}, \mu_{w_i}), M_{w_i} - Pre(p, t_{\alpha_{i+1}})\right\}$.*

Thus, it follows that also the estimation error is a monotonically non-increasing function of the observed word length.

Proposition 8 ([3]). *Let $w = t_{\alpha_1} t_{\alpha_2} \cdots \in L(N, M_0)$ be an observed word, w_i the prefix of w of length i, and μ_{w_i} and μ'_{w_i} the estimate and the updated estimate of M_{w_i}. Then $\forall i$:*

$$e(M_{w_i}, \mu_{w_i}) \geq e(M_{w_i}, \mu'_{w_{i+1}}) = e(M_{w_{i+1}}, \mu_{w_{i+1}}).$$

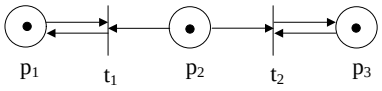

Figure 1: *A net system that is not MO, but whose places are MO.*

3 Properties of estimates

It is natural to ask under which conditions the estimated marking computed by algorithm 2 converges to the actual marking. This motivated us to define the following properties.

Definition 9. *Given a net system $\langle N, M_0 \rangle$, and a place $p \in P$, we say that $w \in L(N, M_0)$ is*

– p-complete *if $e_p(M_w, \mu_w) = 0$, i.e., if $\mu_w(p) = M_w(p)$;*

– marking complete *if $e(M_w, \mu_w) = 0$.*

Thus a marking complete word allows one to reconstruct the actual marking of the net.

Based on this, we can define these properties of a place and of a net system.

Definition 10. *Given a net system $\langle N, M_0 \rangle$, a place $p \in P$ is:*

— marking observable *(MO) if there exists a p-complete word $w \in L(N, M_0)$;*

— strongly marking observable *(SMO) in k_p steps (where k_p depends on the place p) if:*
(i) $\forall\, w \in L(N, M_0)$ such that $|w| \geq k_p$, w is p-complete;
(ii) $\forall\, w \in L(N, M_0)$ such that $|w| < k_p$, either w is p-complete or $\exists\, t \in T$ such that $M_0[wt\rangle$.

Definition 11 ([4]). *A net system $\langle N, M_0 \rangle$ is:*

— marking observable (MO) *if there exists a marking complete $w \in L(N, M_0)$;*

— strongly marking observable (SMO) *in k steps if:*
(i) $\forall w \in L(N, M_0)$ such that $|w| \geq k$, w is marking complete,
(ii) $\forall w \in L(N, M_0)$ such that $|w| < k$, either w is marking complete or $\exists\, t \in T$ such that $M_0[wt\rangle$.

The following implications hold:

— $\forall p,\ p$ is MO $\iff \langle N, M_0 \rangle$ is MO

— $\forall p,\ p$ is SMO $\iff \langle N, M_0 \rangle$ is SMO.

Note that the first one only holds in one sense. In fact, even if all places are observable, this does not imply that there exists one sequence that reconstructs the marking of all places.

Example 12. Let us consider the net system $\langle N, M_0 \rangle$ in figure 1. All places are MO but the net system is not MO. In fact, if t_1 fires, we reconstruct the marking of places p_1 and p_2, but the net reaches a dead marking, thus making it impossible to reconstruct the marking of place p_3. Analogously, the firing of t_2 enables us to reconstruct the actual marking of places p_2 and p_3, but it produces a deadlock, thus not enabling the reconstruction of the marking in p_1. ■

4 Observer coverability graph

In this section we show how to construct an *observer coverability tree* and the corresponding *observer coverability graph (OCG)* to represent both the set of reachable markings of a net system and the error of the estimate computed in accordance with algorithm 2. More precisely, each node of the OCG contains a vector M covering a marking of the net and an upper bound error vector $u \in \mathbb{N}^m$.

Algorithm 13 (Observer coverability tree).

1. Let $u_0 = M_0$. Label the initial node (M_0/u_0) as the root and tag it "new".

2. If "new" nodes exist, select a new node (M/u) and:

2.1. If (M/u) is identical to a node labeled "old" then tag (M/u) "old" and go to step 2.

2.2. If no transitions are enabled at M, tag (M/u) "dead" and go to step 2.

2.3. For each transition t enabled at M do the following:

2.3.1. $\forall\, p \in P$, if $M(p) = \omega$ then let $\tilde{M}(p) = M(p)$ and $\tilde{u}(p) = u(p)$,
else let $\tilde{M}(p) = M(p) + C(p,t)$ and $\tilde{u}(p) = \min\{u(p),\ M(p) - Pre(p,t)\}$;

2.3.2. on the path from the root to (M/u) if there exists a marking $\overline{M} \leq \tilde{M}$ and $\tilde{M} \neq \overline{M}$, i.e., $\overline{M}$ is covered by $\tilde{M}$, then let $\tilde{M}(p) = \omega$ for each p such that $\tilde{M}(p) > \overline{M}(p)$;

2.3.3. introduce $(\tilde{M}/\tilde{u})$ as a node, draw an arc with label t from (M/u) to $(\tilde{M}/\tilde{u})$, and tag $(\tilde{M}/\tilde{u})$ "new".

2.4 Tag (M/u) "old" and go to step 2. ■

Note that its construction follows the well known rules of a coverability tree for a P/T net [9]. Also, we note that the error bound vector u is set to the actual error for the root node and then it is updated as we add new nodes. Note, however, that whenever we reach a marking whose component $M(p)$ is ω, the error bound $u(p)$ is not updated any more (see step 2.3.1).

The **observer coverability graph** of a Petri net $\langle N, M_0\rangle$ is a labeled directed graph $\mathcal{G} = (V, E)$. Its node set V is the set of all distinct labeled nodes in the observer coverability tree, and each arc in E is labeled with a transition t to represent a firing such that $\delta((M/u), t) = (M'/u')$, where (M/u) and (M'/u') are in V. Note that in the OCG all tags used in the construction of the observer coverability tree are omitted. We will also represent the initial marking by a round corner box, while a thick box represents a marking whose estimation error bound vector is $u = \vec{0}_m$.

Example 14. Let us consider the net systems in figure 2 and their OCG. Since both the nets are unbounded, in both cases ω appears. The OCG of a bounded net is reported in figure 3. ■

Let us demonstrate that the OCG of a P/T net is finite.

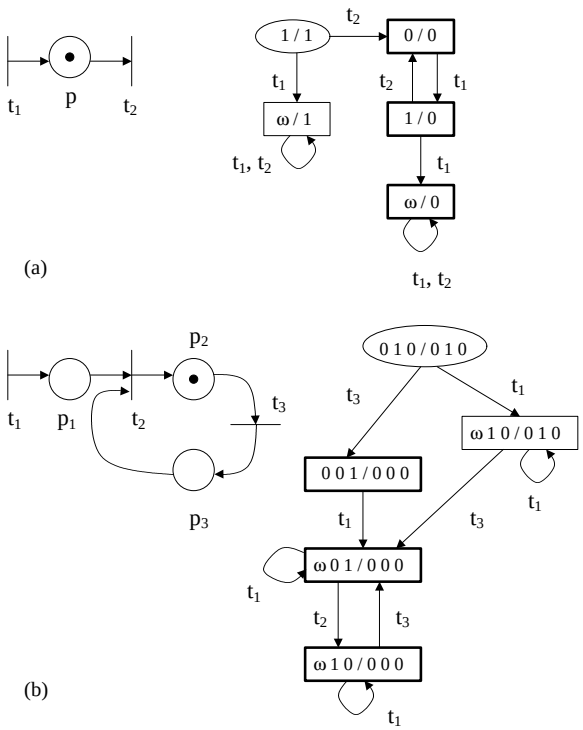

Figure 2: *Unbounded Petri nets and their observer coverability graphs.*

Property 15. *Let $\mathcal{G}$ be the OCG of $\langle N, M_0\rangle$. The number of nodes in $\mathcal{G}$ is bounded by $v = v' \cdot \prod_{p\in P}(M_0(p) + 1)$ where v' is the number of nodes in the usual coverability graph of $\langle N, M_0\rangle$.*

Proof: By virtue of algorithm 13 the initial error bound vector is equal to the initial estimate, i.e., $u_0 = M_0$. Moreover, by proposition 8 the place estimation error is a monotonically non-increasing function of the observed word length, thus the estimation error in the generic place p may assume at most $M_0(p)+1$ different values. It follows that the number of nodes in $\mathcal{G}$ is limited by the number of nodes v' in the coverability graph times $\prod_{p\in P}(M_0(p) + 1)$. □

5 Properties analysis

In this section we use the OCG as a tool to prove the properties presented in section 3. Let us first state the following proposition.

Proposition 16. *Let $\mathcal{G}$ be the OCG of $\langle N, M_0\rangle$. Given $w \in L(N, M_0)$, consider the node (M/u) reached on the graph executing w, i.e., let $(M/u) = \delta((M_0/u_0), w)$. It holds that:*

(i) the place estimation error is $e_p(M_w, \mu_w) \in [\ell(p), u(p)]$ where $u(p)$ is the component of u corresponding to place p and

$$\ell(p) = \begin{cases} u(p) & \text{if } M(p) \neq \omega \\ 0 & \text{if } M(p) = \omega \end{cases}$$

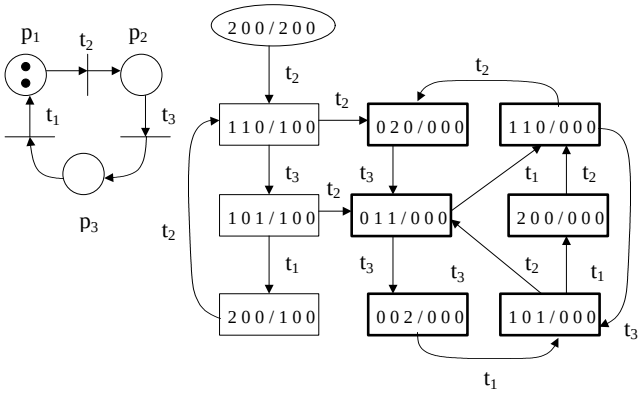

Figure 3: *A bounded Petri net and its observer coverability graph.*

(ii) the error is $e(M_w, \mu_w) \in \left[\sum_{p\in P} \ell(p), \sum_{p\in P} u(p)\right]$.

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

(i) When $w \equiv w_0$, i.e., w is a word of null length, $(M/u) = (M_0/u_0)$, and $e_p(M_{w_0}, \mu_{w_0}) = M_0(p) - 0 = M_0(p) \equiv u_0(p)$.

Assume that the property (i) holds for a word $w' \in L(N, M_0)$ and let $\delta((M_0/u_0), w') = (M'/u')$. Let t be an enabled transition at $M_{w'}$ and $w = w't$: in the OCG there will be a transition $\delta((M'/u'), t) = (M/u)$. We can consider two cases.

If $M(p) \neq \omega$, then $M_{w'}(p) = M'(p) \neq \omega$ and $e_p(M_w, \mu_w) = \min\{e_p(M_{w'}, \mu_{w'}),\ M_{w'}(p) - Pre(p,t)\} = \min\{u'(p),\ M'(p) - Pre(p,t)\} = u(p)$ where the first equality derives from proposition 7, the second one from the induction hypothesis, and the third one from step 2.3.1 of algorithm 13.

If $M(p) = \omega$, then $e_p(M_w, \mu_w) = \min\{e_p(M_{w'}, \mu_{w'}),\ M_{w'}(p) - Pre(p,t)\} \leq e_p(M_{w'}, \mu_{w'}) \leq u'(p) = u(p)$ where the last inequality derives from the induction hypothesis, and the last equality from step 2.3.1 of algorithm 13.

(ii) Immediately follows from the previous item. □

Example 17. Let us consider again the net system in figure 2.a and its OCG. The estimation error relative to the node labeled with $(\omega/1)$ may be either null or unitary. If we consider $w = t_1t_2t_2$ then $e_p(M_w, \mu_w) = 0$, thus on the OCG we read an upper bound of the estimation error. On the contrary, $e_p(M_w, \mu_w) = 1$ is the exact estimation error for all words w such that $\forall\, w' \preccurlyeq w$, $|w'|_{t_1} \geq |w|_{t_2}$.

Now, let us consider the net system in figure 2.b. Here, every node with label $M(p_1) = \omega$ is also characterized by $u(p_1) = 0$, i.e., the upper bound on the place estimation error in p_1 is null. Therefore, in this case in each node of the OCG we can read the actual place estimation error in p_1.

Finally, in the example in figure 3 no ω appears in $\mathcal{G}$ being the net bounded, thus in each node u is the exact estimation error vector. ■

5.1 Word completeness

A necessary and sufficient condition for completeness of a word was given in [3] in terms of languages.

Proposition 18 ([3]). *A word* $w \in L(N, M_0)$ *is* marking complete *iff* $\forall \overline{M}_0 < M_0 : w \notin L(N, \overline{M}_0)$.

Example 19. Let us consider the net system in figure 3. The word $w = t_2$ is not marking complete since $t_2 \in L(N, \overline{M}_0)$ with $\overline{M}_0 = [1\ 0\ 0] < M_0 = [2\ 0\ 0]$. On the contrary, the word $w = t_2t_2$ is marking complete. It can be proved with both theorem 18 and the OCG. ■

A simpler semi–decision procedure for completeness can be given using the OCG.

Proposition 20. *Let us consider a net system* $\langle N, M_0\rangle$ *and its OCG* $\mathcal{G}$*. Let* (M/u) *be the node in* $\mathcal{G}$ *reached executing* $w \in L(N, M_0)$*, i.e.,* $(M/u) = \delta((M_0/u_0), w)$ *and let us consider a place* $p \in P$*.*

(i) If $u(p) = 0$*, then* w *is* p*-complete.*

(ii) If $M(p) \neq \omega$ *and* $u(p) \neq 0$*, then* w *is not* p*-complete.*

Proof: It follows from proposition 16. □

Corollary 21. *Let us consider a net system* $\langle N, M_0\rangle$ *and its OCG* $\mathcal{G}$*. Let* (M/u) *be the node in* $\mathcal{G}$ *reached executing* $w \in L(N, M_0)$*, i.e.,* $(M/u) = \delta((M_0/u_0), w)$*.*

(i) If $\forall\, p \in P$*,* $u(p) = 0$*, then* w *is marking complete.*

(ii) If $\exists\, p \in P$ *such that* $M(p) \neq \omega$ *and* $u(p) \neq 0$*, then* w *is not marking complete.* ■

Example 22. Note that the OCG provides necessary and sufficient conditions for the completeness of a word only in the case of bounded P/T nets, when ω does not appear in the graph. On the contrary, it only provides two distinct sufficient or necessary conditions for the completeness of a word in the case of unbounded nets. As an example, let us consider the net system in figure 2.a. If we consider $w = t_1t_2t_2$, w is complete but this is not deducible from the OCG. ■

5.2 Observability

A necessary and sufficient condition for marking observability was given in [3].

Proposition 23 ([3]). *The net system* $\langle N, M_0\rangle$ *is* marking observable *iff* $L(N, M_0) \supsetneq \bigcup_{\overline{M}_0 < M_0} L(N, \overline{M}_0)$.

Checking for language inclusion is difficult thus we look for simpler decision procedures. In particular the OCG provides a simpler semi-decision (i.e., only sufficient) condition for the marking observability.

Proposition 24. *Let us consider a net system* $\langle N, M_0\rangle$ *and its OCG* $\mathcal{G}$*. A place* p *is* marking observable *if there exists a node in* $\mathcal{G}$ *such that* $u(p) = 0$*.*

Proof: It follows from the definition of marking observability and from proposition 20. □

Corollary 25. *Let us consider a net system* $\langle N, M_0\rangle$ *and its OCG* $\mathcal{G}$*. The system is* marking observable *if there exists a node in* $\mathcal{G}$ *such that* $u = \vec{0}_m$*.* ■

5.3 Strong observability

The OCG provides necessary and sufficient conditions for strong marking observability. Let us first demonstrate, as an intermediate result, that the repeated firing of a repetitive sequence does not decrease the place estimation error.

Lemma 26. *Let $\langle N, M_0\rangle$ be a net system and let us assume that there exists a firing sequence w' that enables a repetitive sequence w, i.e., $M_0[w'\rangle M_{w'}[w\rangle M_{w'w}$ with $M_{w'w} \geq M_{w'}$. Then for all $p \in P$ and $\forall\, i > 1$, $e_p(M_{w'w^i}, \mu_{w'w^i}) = e_p(M_{w'w}, \mu_{w'w})$.*

Proof: While observing a sequence w, the error may decrease only during step 4 of algorithm 2, i.e., when we compute the updating estimate.

Let t be the first transition in the sequence w. If t fires after $w'w^i$, in step 4 of algorithm 2 we have $\mu'_{w'w^it} \geq Pre(\cdot, t)$. Using proposition 7 it is easy to show that for all $i \geq 1$ holds $(M_{w'w^{i+1}} - \mu_{w'w^{i+1}}) \leq (M_{w'w^i} - \mu'_{w'w^it})$, thus $\mu_{w'w^{i+1}} \geq (M_{w'w^{i+1}} - M_{w'w^i}) + \mu'_{w'w^it} \geq \mu'_{w'w^it} \geq Pre(\cdot, t)$. Therefore, $\mu'_{w'w^{i+1}t} = \mu_{w'w^{i+1}}$, i.e., the estimate is not updated and the error for each place remains constant each time w is repeated after it has fired once. □

Proposition 27. *Let us consider a net system $\langle N, M_0\rangle$ and its OCG $\mathcal{G}$. A place $p \in P$ is* strongly marking observable *in k_p steps iff the error bound vector is such that $u(p) = 0$ for each node (M/u) in $\mathcal{G}$ such that: (a) the node (M/u) is in a cycle; (b) the node (M/u) is dead. Moreover, if (a) and (b) are satisfied, it is possible to compute k_p as the length[1] of the longest path that leads from the root to a node with $u(p) > 0$.*

Proof: (if) By proposition 15, the number of nodes in $\mathcal{G}$ is finite and equal to v. Thus any word w of length greater or equal to v must pass through a cycle in $\mathcal{G}$, hence w is p-complete by assumption (a). Any word of length less that v that leads to a dead marking is also p-complete, by assumption (b). This is sufficient to show that the place is SMO in k_p steps with $k_p \leq v$. The actual value of k_p may be computed as suggested in the statement.

(only if) We show this by contradiction, proving that if any of the two conditions are violated the place cannot be SMO. Clearly, if condition (b) is violated, the place is not strongly marking observable by definition. Now, let assume that (a) is violated. We consider two subcases.

(i) Assume there exists a node (M/u) along a cycle γ of $\mathcal{G}$ with $M(p) \neq \omega$ and $u(p) > 0$. Then there exists w' such that $M_{w'} = M$ and $e_p(M_{w'}, \mu_{w'}) = u(p) > 0$. The cycle γ corresponds to a word w such that $M_{w'}[w\rangle M_{w'}$, i.e., by Lemma 26 the infinite length sequence $w'w^i$ may be fired for all $i > 0$ without reducing the estimation error and the place is not SMO.

(ii) Assume there exists a node (M/u) with $M(p) = \omega$ and $u(p) > 0$ (we do not even need to assume it is along a cycle). Then consider the path along the observer coverability tree that reaches (M/u) from (M_0/u_0) and let $(\tilde{M}, \tilde{u})$ be the first node we encounter along this path with $M(p) = \omega$. Then, at step 2.3.2 of algorithm 13, we have identified a marking $\overline{M}$ such that $M_0[w'\rangle\overline{M}[w\rangle M_{w'w}$ and $M_{w'w} \geq M_{w'}$ ($\tilde{M}$ is obtained from $M_{w'w}$ by changing in ω the components greater that the corresponding components of $\overline{M}$). Also, $e_p(M_{w'w}, \mu_{w'w}) = \tilde{u}(p) \geq u(p) > 0$. Thus, by Lemma 26 the infinite length sequence $w'w^i$ may be fired for all $i > 0$ without reducing the estimation error and the place is not SMO. □

[1] The length of a path is given by the number of edges along the path.

Corollary 28. *Let us consider a net system $\langle N, M_0\rangle$ and its OCG $\mathcal{G}$. The system is* strongly marking observable *in k steps iff the error bound vector is $u = \vec{0}_m$ for each node (M/u) in $\mathcal{G}$ such that: (a) the node (M/u) is in a cycle; (b) the node (M/u) is dead. Moreover, if (a) and (b) are satisfied, it is possible to compute k as the length of the longest path that leads from the root to a node with $u \neq \vec{0}_m$.* ■

Example 29. All net systems in figures 2–3 are marking observable but not strongly marking observable. On the contrary, one example of strong marking observability (in one step) can be obtained if we consider the net in figure 3 with initial marking $M_0 = [1\ 0\ 0]^T$. ■

6 Conclusions

In this paper we dealt with the problem of estimating the marking of a Place/Transition net based on event observation. Words of events that allow one to reconstruct the marking of the net are called complete. We focused our attention on two main properties: *marking observability* and *strong marking observability* and introduced a useful analysis tool to prove the above properties: the *observer coverability graph*. This graph contains both the set of reachable markings of a net system and the corresponding estimate error and we showed that it provides simple decision or semi–decision conditions.

References

[1] P.E. Caines, R. Greiner, S. Wang, "Dynamical Logic Observers for Finite Automata," *Proc. 27th CDC*, Austin, TX, pp. 226–33, Dec. 1988.

[2] P.E. Caines, S. Wang, "Classical and Logic Based Regulator Design and its Complexity for Partially Observed Automata," *Proc. 28th CDC*, Tampa, FL, pp. 132–7, Dec. 1989.

[3] A. Giua, "Petri Net State Estimators Based on Event Observation," *Proc. 36th CDC*, San Diego, CA, pp. 4086–91, Dec. 1997.

[4] A. Giua, C. Seatzu, "Observability Properties of Petri Nets," *Proc. 39th CDC*, Sydney, Australia, pp. 2676–81, Dec. 2000.

[5] R. Kumar, V. Garg, S.I. Markus, "Predicates and Predicate Transformers for Supervisory Control of Discrete Event Dynamical Systems," *IEEE Trans. on Automatic Control*, 38(2), pp. 232–47, 1993.

[6] C.M. Özveren, A.S. Willsky, "Observability of Discrete Event Dynamic Systems," *IEEE Trans. on Automatic Control*, 35(7), pp. 797–806, 1990.

[7] P.J. Ramadge, "Observability of Discrete-Event Systems," *Proc. 25th CDC*, Athens, Greece, pp. 1108–12, Dec. 1986.

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

[9] T. Murata, “Petri Nets: Properties, Analysis and Applications,” *Proceedings IEEE*, 77(4), pp. 541–80, 1989.

[10] A. Ramírez, I. Rivera, E. Lopez, “Observer Design for Discrete Event Systems Modeled by Interpreted Petri Nets,” *2000 IEEE Int. Conf. on Robotics and Automation*, San Francisco, CA, pp. 2871–6, Apr. 2000.