

# Verification of current-state opacity in discrete event systems using an observer net

## 1 Appendix

### 1.1 Petri nets

A Petri net is a four-tuple  $N = (P, T, Pre, Post)$ , where  $P$  is a set of  $m$  places, graphically represented by circles,  $T$  is a set of  $n$  transitions, graphically represented by bars,  $Pre : P \times T \rightarrow \mathbb{N}^1$  and  $Post : P \times T \rightarrow \mathbb{N}$  specify the arcs directed from places to transitions, and transitions to places, respectively.  $Pre$  and  $Post$  can be represented by  $m \times n$  matrices. The incidence matrix of the net  $N$  is accordingly defined by  $C = Post - Pre$ .

The input and output sets of a node  $x \in P \cup T$ , denoted by  $\bullet x$  and  $x^\bullet$ , respectively, are defined as  $\bullet x = \{y \in P \cup T \mid Pre(x, y) > 0\}$  and  $x^\bullet = \{y \in P \cup T \mid Post(x, y) > 0\}$ . A Petri net is said to be acyclic if there are no oriented cycles.

A marking is a mapping  $M : P \rightarrow \mathbb{N}$  that assigns to each place a non-negative integer number of tokens, graphically represented by black dots. The marking of place  $p$  at a  $M$  is denoted by  $M(p)$ . A marking  $M$  can be also denoted as  $M = \sum_{p \in P} M(p) \cdot p$ . A Petri net system

$\langle N, M_0 \rangle$  is a net  $N$  with *initial marking*  $M_0$ .

A transition  $t$  is said to be *enabled* at a marking  $M$  if  $M \geq Pre(\cdot, t)$  and its firing yields a marking  $M' = M + C(\cdot, t)$ . We write  $M[\sigma]$  to denote that a sequence of transitions  $\sigma = t_{j_1} \dots t_{j_k} \in T^*$ ,  $k \in \mathbb{N}$ , is enabled at  $M$ , and  $M[\sigma]M'$  to denote that firing the sequence  $\sigma$  yields  $M'$ . Given a sequence  $\sigma \in T^*$ , the function  $\pi : T^* \rightarrow \mathbb{N}^n$  associates with  $\sigma$  the Parikh vector  $y = \pi(\sigma) \in \mathbb{N}^n$ , i.e.,  $y(t) = k$  if transition  $t$  appears  $k$  times in  $\sigma$ .

A marking  $M$  is said to be *reachable* in  $\langle N, M_0 \rangle$  if there exists a sequence  $\sigma$  such that  $M[\sigma]M'$ . The set of all markings reachable from  $M_0$  defines the reachability set of  $\langle N, M_0 \rangle$ , denoted by  $R(N, M_0)$ , i.e.,  $R(N, M_0) = \{M \in \mathbb{N}^m \mid \exists \sigma \in T^* : M_0[\sigma]M\}$ . A Petri net is *bounded* if there exists a non-negative integer  $k \in \mathbb{N}$  such that for any place  $p \in P$  and any reachable marking  $M \in R(N, M_0)$ ,  $M(p) \leq k$  holds.

<sup>1</sup> In this work, we use  $\mathbb{N}$ ,  $\mathbb{Z}$  and  $\mathbb{R}$  to denote the sets of non-negative integers, integers, and real number, respectively.

### 1.2 Labeled Petri nets

A labeled Petri net is a four-tuple  $G = (N, M_0, E, \ell)$ , where  $\langle N, M_0 \rangle$  is a PN system,  $E$  is the alphabet (a set of labels) and  $\ell : T \rightarrow E \cup \{\varepsilon\}$  is a labeling function that assigns to each transition  $t \in T$  either a symbol from  $E$  or the empty word  $\varepsilon$ . The transition set  $T$  is partitioned into two disjoint sets  $T = T_o \dot{\cup} T_{uo}$ , where  $T_o = \{t \in T \mid \ell(t) \in E\}$  is the set of observable transitions and  $T_{uo} = T \setminus T_o = \{t \in T \mid \ell(t) = \varepsilon\}$  is the set of unobservable transitions. The labeling function can be extended to firing sequences  $\ell : T^* \rightarrow E^*$ , i.e.,  $\ell(\sigma t) = \ell(\sigma)\ell(t)$  with  $\sigma \in T^*$  and  $t \in T$ .

Given a labeled net system  $G = (N, M_0, E, \ell)$  and a marking  $M \in R(N, M_0)$ , we define the language generated from  $M$  as

$$\mathcal{L}(N, M) = \{w \in E^* \mid \exists \sigma \in T^* : M[\sigma] \text{ and } \ell(\sigma) = w\}$$

Let  $G = (N, M_0, E, \ell)$  be an LPN. A string belonging to  $\mathcal{L}(N, M_0)$  is called an observation of  $G$ , and denoted by  $w$ . We define the set of markings consistent with  $w$  as

$$\mathcal{C}(w) = \{M \in \mathbb{N}^m \mid \exists \sigma \in T^* : M_0[\sigma]M \text{ and } \ell(\sigma) = w\}$$

**Definition.** Given an LPN  $G = (N, M_0, E, \ell)$  and a marking  $M \in R(N, M_0)$ , the *unobservable reach* of  $M$  is defined as  $\mathcal{U}(M) = \{M' \in \mathbb{N}^m \mid \exists \sigma_u \in T_{uo}^* : M[\sigma_u]M'\}$ .

In simple words, the unobservable reach of a marking  $M$  is the set of markings reachable from  $M$  by firing only unobservable transitions.