Automatica 104 (2019) 238–241

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Technical communique

Deciding detectability for labeled Petri nets[☆]

Tomáš Masopust[a,b], Xiang Yin[c,d,*]

[a] Department of Computer Science, Palacky University, Olomouc, Czechia
[b] Institute of Mathematics, Czech Academy of Sciences, Brno, Czechia
[c] Department of Automation, Shanghai Jiao Tong University, Shanghai 200240, China
[d] Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai 200240, China

ARTICLE INFO

Article history:
Received 29 November 2018
Accepted 5 February 2019
Available online 20 March 2019

Keywords:
Discrete event systems
Petri nets
Detectability
Complexity
Decidability

ABSTRACT

Detectability of discrete event systems is a property to decide whether the current and subsequent states can be determined based on observations. We investigate the existence of algorithms for checking strong and weak detectability for systems modeled as labeled Petri nets. Strong detectability requires that we can *always* determine, after a finite number of observations, the current and subsequent markings of the system, while weak detectability requires that we can determine, after a finite number of observations, the current and subsequent markings for *some* trajectories of the system. We show that there is an algorithm to check strong detectability requiring exponential space, and that there is no algorithm to check weak detectability.

© 2019 Elsevier Ltd. All rights reserved.

1. Introduction

State estimation is one of the central problems in systems and control, playing a key role in problems where one needs to estimate the state of the system based on observations (Ozveren & Willsky, 1990; Ramadge, 1986; Shu, Lin, & Ying, 2007). We study such a property called *detectability* for labeled Petri nets (LPNs). The concept of detectability was proposed by Shu et al. (2007) for finite-state automata. It asks whether the current and subsequent states can be determined based on observations. Since then, it has drawn a considerable attention in the literature (Keroglou & Hadjicostis, 2017; Shu & Lin, 2011, 2013; Yin, 2017), including studies on the complexity of verification of different notions of detectability (Masopust, 2018; Yin & Lafortune, 2017; Zhang, 2017) and a generalization to, e.g., stochastic DES (Keroglou & Hadjicostis, 2017; Yin, 2017).

In this paper, we study the existence of algorithms for the verification of strong and weak detectability for LPNs, where the Petri net structure and the initial marking are known, and the system is partially observed via a labeling function.

For systems modeled by finite-state automata, there is an algorithm checking strong detectability in polynomial time (Shu & Lin, 2011) (actually, there is an efficient parallel algorithm (Masopust, 2018)). However, any algorithm checking weak detectability requires polynomial space (Yin & Lafortune, 2017; Zhang, 2017), and hence, according to the current knowledge, exponential times; this holds even for a very restricted type of automata (Masopust, 2018).

For systems modeled by LPNs, Zhang and Giua (2018) recently showed undecidability of weak detectability for LPNs with inhibitor arcs, which are computationally universal models, and stated the decidability questions of strong and weak detectability for LPNs as open problems.

In this paper, we solve these problems. Namely, we show that checking strong detectability for LPNs is decidable, by expressing it as a path formula in *Yen's logic*, the satisfiability of which is decidable (Yen, 1992), and that any algorithm requires exponential space, and is thus infeasible. Then we show that checking weak detectability for LPNs is undecidable, solving the second open problem and improving the result of Zhang and Giua (2018). We prove it by reduction from the *language inclusion problem* of two LPNs.

2. Preliminaries and definitions

We assume that the reader is familiar with the basics of Petri nets (Peterson, 1981). For a set A, $|A|$ denotes the cardinality of A. An *alphabet* Σ is a finite nonempty set of *events*. A *word* over Σ is a sequence of events of Σ. Let Σ^* denote the set of all finite words over Σ, the *empty word* denoted by ε, and let Σ^ω

☆ T. Masopust was partially supported by the Czech Science Foundation grant no. 19-06175J. X. Yin was supported by the National Natural Science Foundation of China (61803259, 61833012). The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Christoforos Hadjicostis under the direction of Editor André L. Tits.

* Corresponding author at: Department of Automation, Shanghai Jiao Tong University, Shanghai 200240, China.

E-mail addresses: masopust@math.cas.cz (T. Masopust), yinxiang@sjtu.edu.cn (X. Yin).

https://doi.org/10.1016/j.automatica.2019.02.058
0005-1098/© 2019 Elsevier Ltd. All rights reserved.

denote the set of all infinite words over Σ. For a word $u \in \Sigma^*$, $|u|$ denotes its length. Let $\mathbb{N} = \{0, 1, 2, \ldots\}$ denote the set of all non-negative integers.

A *Petri net* is a structure $N = (P, T, Pre, Post)$, where P is a finite set of *places*, T is a finite set of *transitions*, $P \cup T \neq \emptyset$ and $P \cap T = \emptyset$, and $Pre: P \times T \to \mathbb{N}$ and $Post: P \times T \to \mathbb{N}$ are the pre- and post-incidence functions specifying the arcs directed from places to transitions and vice versa. A *marking* is a map $M: P \to \mathbb{N}$ assigning to each place a number of tokens. A *Petri net system* (N, M_0) is the Petri net N with the initial marking M_0. A transition t is *enabled* in a marking M if $M(p) \geq Pre(p, t)$ for every place $p \in P$. An enabled transition t can *fire*, resulting in the marking $M'(p) = M(p) - Pre(p, t) + Post(p, t)$ for every $p \in P$. We write $M \xrightarrow{\sigma}_N$ to denote that the sequence of transitions σ is enabled in M of N, and $M \xrightarrow{\sigma}_N M'$ to denote that the firing of the sequence σ results in a marking M'. For simplicity, we omit the subscript N if the net is clear from the context. We write $L(N, M_0) = \{\sigma \in T^* \mid M_0 \xrightarrow{\sigma}\}$ to denote the set of all transition sequences enabled in the marking M_0. A marking M is *reachable* in the Petri net system (N, M_0) if there is a sequence of transitions $\sigma \in T^*$ such that $M_0 \xrightarrow{\sigma} M$. The set of all markings reachable from M_0 defines the reachability set of the Petri net system (N, M_0), denoted by $R(N, M_0)$.

A *labeled Petri net system* is a quadruple $G = (N, M_0, \Sigma, \ell)$, where (N, M_0) is a Petri net system, Σ is an alphabet (a set of labels), and $\ell: T \to \Sigma \cup \{\varepsilon\}$ is a labeling function assigning to each transition $t \in T$ a symbol from $\Sigma \cup \{\varepsilon\}$. The labeling function can be extended to $\ell: T^* \to \Sigma^*$ by $\ell(\sigma t) = \ell(\sigma)\ell(t)$ for $\sigma \in T^*$ and $t \in T$; we define $\ell(\lambda) = \varepsilon$ for the empty transition sequence λ. A transition $t \in T$ is observable if $\ell(t) \in \Sigma$; unobservable otherwise. The *language* of G is the set $L(G) = \{\ell(\sigma) \mid \sigma \in L(N, M_0)\}$. Similarly, $L^\omega(G)$ is the set of all infinite words generated by G. Finally, for a word $s \in L(G)$, $R(G, s) = \{M \mid \sigma \in L(N, M_0),\ \ell(\sigma) = s,\ M_0 \xrightarrow{\sigma} M\}$ denotes the set of all reachable markings consistent with the observation s.

As usual when detectability is discussed (Shu & Lin, 2011), we make the following two assumptions on the system G: (i) G is *deadlock free*, i.e., in every reachable marking of the system, there is a transition that can fire, and (ii) G cannot generate an infinite unobservable sequence.

3. Strong detectability

Strong detectability requires that we can determine, after a finite number of observations, the current and subsequent states for all trajectories of the system, formally defined as follows.

Definition 1. An LPN system $G = (N, M_0, \Sigma, \ell)$ is *strongly detectable* if there is an integer $n \geq 0$ such that for every infinite word $s \in L^\omega(G)$ and every finite prefix s' of s, if s' is longer than n, then $|R(G, s')| = 1$.

To check strong detectability, it suffices to verify whether there are two arbitrarily long sequences with the same observation leading to two different markings. To formalize this idea, we use the *twin-plant* construction for Petri nets used to test diagnosability (Cabasino, Giua, Lafortune, & Seatzu, 2012; Yin & Lafortune, 2017) and prognosability (Yin, 2018).

Let $G = (N, M_0, \Sigma, \ell)$ be an LPN, and let $G' = (N', M_0', \Sigma, \ell)$ be a place-disjoint copy of G, i.e., $N' = (P', T, Pre', Post')$ where $P' = \{p' \mid p \in P\}$ is a disjoint copy of P and the functions Pre' and $Post'$ are adjusted in the natural way. The copy G' has the same initial marking as G, i.e., $M_0'(p') = M_0(p)$ for every $p' \in P'$. We define a Petri net $(N_\|, M_{0,\|}) = ((P_\|, T_\|, Pre_\|, Post_\|), M_{0,\|})$ that is essentially the (label-based) synchronization of G and G', where the set of places is $P_\| = P \cup P'$, the initial marking $M_{0,\|} = [M_0^\top\ M_0'^\top]^\top$ is the concatenation of the initial markings of G and G', the transitions $T_\| = (T \cup \{\lambda\}) \times (T \cup \{\lambda\}) \setminus \{(\lambda, \lambda)\}$ are pairs of transitions of G and G' without the empty pair, and the functions $Pre_\|: P_\| \times T_\| \to \mathbb{N}$ and $Post_\|: P_\| \times T_\| \to \mathbb{N}$ are defined as follows: (i) for every $p \in P$ and every $t \in T$ with $\ell(t) = \varepsilon$, we define $Pre_\|(p, (t, \lambda)) = Pre(p, t)$ and $Post_\|(p, (t, \lambda)) = Post(p, t)$; (ii) for every $p' \in P'$ and every $t \in T$ with $\ell(t) = \varepsilon$, we define $Pre_\|(p', (\lambda, t)) = Pre'(p', t)$ and $Post_\|(p', (\lambda, t)) = Post'(p', t)$; (iii) for every $p \in P$ and every $t_1, t_2 \in T$ with $\ell(t_1) = \ell(t_2) \neq \varepsilon$, we define $Pre_\|(p, (t_1, t_2)) = Pre(p, t_1)$ and $Post_\|(p, (t_1, t_2)) = Post(p, t_1)$; (iv) for every $p' \in P'$ and every $t_1, t_2 \in T$ with $\ell(t_1) = \ell(t_2) \neq \varepsilon$, we define $Pre_\|(p', (t_1, t_2)) = Pre'(p', t_2)$ and $Post_\|(p', (t_1, t_2)) = Post'(p', t_2)$; (v) otherwise, no arc is defined, i.e., $Pre_\|(p, t) = Post_\|(p, t) = 0$.

Essentially, $(N_\|, M_{0,\|})$ tracks all pairs of sequences that have the same observation. Namely, for any $(\sigma, \sigma') \in L(N_\|, M_{0,\|})$, we have $\ell(\sigma) = \ell(\sigma')$, and for any $\sigma, \sigma' \in L(N, M_0)$ such that $\ell(\sigma) = \ell(\sigma')$, there is a sequence in $(N_\|, M_{0,\|})$ whose first and second components are σ and σ', respectively (possibly by inserting the empty transition sequence λ). For an example of the construction, we refer the reader to the literature (Cabasino et al., 2012; Yin, 2018).

Theorem 2. *An LPN $G = (N, M_0, \Sigma, \ell)$ is not strongly detectable if and only if, in $(N_\|, M_{0,\|})$, there exists a sequence*

$$M_{0,\|} \xrightarrow{\alpha}_{N_\|} M_1 \xrightarrow{\beta}_{N_\|} M_2 \xrightarrow{\gamma}_{N_\|} M_3$$

such that $(M_1 \leq M_2) \wedge |\beta| > 0 \wedge \bigvee_{p \in P} M_3(p) \neq M_3(p')$.

Proof. ($\Leftarrow$) Suppose that there is such a sequence. Let $M_{i,1}$ and $M_{i,2}$, for $i = 1, 2, 3$, denote the first and the second components of M_i, respectively, that is, $M_i = [M_{i,1}^\top\ M_{i,2}^\top]^\top$ where the lengths of $M_{i,1}$ and $M_{i,2}$ coincide and are equal to the number of places in G. Let $\alpha = (\alpha_1, \alpha_2)$, $\beta = (\beta_1, \beta_2)$, and $\gamma = (\gamma_1, \gamma_2)$. By the construction of $N_\|$, $\ell(\alpha_1) = \ell(\alpha_2)$, $\ell(\beta_1) = \ell(\beta_2)$, and $\ell(\gamma_1) = \ell(\gamma_2)$. Since $|\beta| > 0$, either β_1 or β_2 is not the empty transition; without loss of generality, let $\beta_1 \neq \lambda$.

Let $n \in \mathbb{N}$ be an arbitrary natural number. We consider an infinite sequence $\alpha_1\beta_1^{m+1}\gamma_1 w \in L^\omega(G)$, where w is an arbitrary infinite continuation of the sequence $\sigma_1 = \alpha_1\beta_1^{m+1}\gamma_1$ such that $\ell(w) \neq \varepsilon$; such a continuation exists by the assumptions that the system is deadlock free and there is no infinite unobservable sequence. The sequence σ_1 is well defined in G because $M_1 \leq M_2$, and hence the sequence $\sigma_2 = \alpha_2\beta_2^{m+1}\gamma_2 \in L(G)$ is also well defined in G. Let $M_0 \xrightarrow{\sigma_1}_N M_{\sigma_1}$ and $M_0 \xrightarrow{\sigma_2}_N M_{\sigma_2}$. Then

$$M_{\sigma_i} = M_{i,3} + m \cdot (M_{i,2} - M_{i,1}).$$

Let p be a place such that $M_3(p) \neq M_3(p')$. Then we can always find an integer $m \geq n$ such that $M_{\sigma_1}(p) \neq M_{\sigma_2}(p')$. Since $s = \ell(\alpha_1\beta_1^{m+1}\gamma_1) = \ell(\alpha_2\beta_2^{m+1}\gamma_2)$ is a prefix of $\ell(\alpha_1\beta_1^{m+1}\gamma_1 w)$, we have that $\{M_{\sigma_1}, M_{\sigma_2}\} \subseteq R(G, s)$, and hence $|R(G, s)| > 1$. Moreover, $M_1 \leq M_2$ implies the existence of β_1^ω in G, and hence $\ell(\beta_1) \neq \varepsilon$, because $\ell(\beta_1) = \varepsilon$ would give $\ell(\beta_1^\omega) = \varepsilon$, which contradicts the assumption that no such sequence exists. Therefore, $|s| \geq m + 1 > n$. Since n was chosen arbitrarily, the system is not strongly detectable.

($\Rightarrow$) Suppose that the system is not strongly detectable, that is, for every $n \in \mathbb{N}$ there exist $s \in L^\omega(G)$ and a finite prefix s' of s such that $|s'| \geq n$ and $|R(G, s')| > 1$. Then, for any $n \in \mathbb{N}$, there are sequences $\alpha, \beta \in L(N, M_0)$ such that (i) $\ell(\alpha) = \ell(\beta)$ and $|\ell(\alpha)| = |\ell(\beta)| \geq n$, and (ii) $M_0 \xrightarrow{\alpha}_N M_\alpha$ and $M_0 \xrightarrow{\beta}_N M_\beta$ with $M_\alpha \neq M_\beta$. By (i) and the construction of $N_\|$, there exists a sequence $\sigma \in L(N_\|, M_{0,\|})$ in $N_\|$ such that σ is in the form of $\sigma = (\alpha, \beta)$. Let $\sigma = t_1 t_2 \cdots t_k$ for some $t_i \in T_\|$ and $k \geq n$, and let $M_1, M_2, \ldots, M_k$ be the markings induced by the transitions, i.e., $M_{0,\|} \xrightarrow{t_1}_{N_\|} M_1 \xrightarrow{t_2}_{N_\|} M_2 \xrightarrow{t_3}_{N_\|} \cdots \xrightarrow{t_k}_{N_\|} M_k$, where $M_k = [M_\alpha^\top \; M_\beta^\top]^\top$.

Consider a computation tree consisting of the computations described above. Note that the same marking may appear at different places as different vertices of the tree. There is such a computation of length at least n for every $n \in \mathbb{N}$, and hence the tree is infinite. Therefore, by König's lemma (König, 1927) stating that every finitely branching infinite tree contains an infinite path, there is an infinite path $C_0, C_1, C_2, \ldots$ in the tree, where C_0 is the initial marking $M_{0,\|}$. Then, since vectors of natural numbers with the product order form a well-quasi-ordering, Dickson's lemma (Dickson, 1913) implies that there are $i < j$ such that $C_i \le C_j$. Since the tree consists only of computations of the above form, $C_0, C_1, \ldots, C_j$ is a prefix of such a computation, and hence there is a sequence $C_{j+1}, \ldots, C_m$ such that $C_0, C_1, \ldots, C_j, C_{j+1}, \ldots, C_m$ is a computation of the above form, that is, C_m is of the form $[M_\alpha^\top \; M_\beta^\top]^\top$ for some α and β satisfying (i) and (ii) above. Consider the sequence

$$M_{0,\|} \xrightarrow{t_1\cdots t_i}_{N_\|} C_i \xrightarrow{t_{i+1}\cdots t_j}_{N_\|} C_j \xrightarrow{t_{j+1}\cdots t_m}_{N_\|} C_m.$$

Since $C_m = [M_\alpha^\top \; M_\beta^\top]^\top$ and $M_\alpha \neq M_\beta$, there is a place p such that $C_m(p) = M_\alpha(p) \neq M_\beta(p') = C_m(p')$. Finally, $|t_{i+1}\cdots t_j| > 0$, because $i < j$, and hence the sequence satisfies the statement of the theorem. □

To state our first result, we briefly recall a fragment of Yen's path logic, the satisfiability of which is decidable (Atig & Habermehl, 2011; Yen, 1992). Let $M_1, M_2, \ldots$ be variables representing markings and $\sigma_1, \sigma_2, \ldots$ be variables representing finite sequences of transitions. Every mapping $c \in \mathbb{N}^{|P|}$ is a term. For all $j > i$, if M_i and M_j are marking variables, then $M_j - M_i$ is a term, and if T_1 and T_2 are terms, then $T_1 + T_2$ and $T_1 - T_2$ are terms. If $c \in \mathbb{N}$ and $t \in T$, then $\#_t(\sigma_1) \le c$ and $\#_t(\sigma_i) \ge c$ are transition predicates, where $\#_t(\sigma)$ denotes the number of occurrences of t in σ. If T_1 and T_2 are terms and $p_1, p_2 \in P$ are places, then $T_1(p_1) = T_2(p_2)$, $T_1(p_1) < T_2(p_2)$, and $T_1(p_1) > T_2(p_2)$ are marking predicates. A predicate is a positive boolean combination of transition and marking predicates. A *path formula* is a formula of the form $(\exists \sigma_1, \sigma_2, \ldots, \sigma_n)(\exists M_1, \ldots, M_n)(M_0 \xrightarrow{\sigma_1} M_1 \xrightarrow{\sigma_2} \cdots \xrightarrow{\sigma_n} M_n) \wedge \varphi(M_1, \ldots, M_n, \sigma_1, \ldots, \sigma_n)$ where φ is a predicate.

Theorem 3. *Strong detectability is decidable for LPNs.*

Proof. The formula of Theorem 2 can be expressed as the following path formula:

$$\begin{aligned}&(\exists \sigma_1, \sigma_2, \sigma_3, \sigma_4)(\exists M_1, M_2, M_3, M_4)\\ &\quad (M_{0,\|} \xrightarrow{\sigma_1}_{N_\|} M_1 \xrightarrow{\sigma_2}_{N_\|} M_2 \xrightarrow{\sigma_3}_{N_\|} M_3 \xrightarrow{\sigma_4}_{N_\|} M_4)\\ &\wedge (M_2 \le M_3) \wedge |\sigma_1| = 0 \wedge |\sigma_3| > 0 \wedge \bigvee_{p \in P} M_4(p) \neq M_4(p'),\end{aligned}$$

where $|\sigma_1| = 0$ is equivalent to $\wedge_{t\in T} \#_t(\sigma_1) \le 0$ and $|\sigma_3| > 0$ is equivalent to $\vee_{t\in T} \#_t(\sigma_3) > 0$. Note that M_4 can be written as term $M_4 - M_1 + M_{0,\|}$, where $M_4 - M_1$ and $M_{0,\|}$ are terms (M_4 and M_1 are marking variables but $M_{0,\|}$ is a constant). Therefore, the last term $\bigvee_{p\in P} M_4(p) \neq M_4(p')$ is equivalent to

$$\bigvee_{p\in P} \left(\begin{array}{l} (M_4 - M_1 + M_{0,\|})(p) > (M_4 - M_1 + M_{0,\|})(p') \\ \vee \; (M_4 - M_1 + M_{0,\|})(p) < (M_4 - M_1 + M_{0,\|})(p') \end{array} \right),$$

which is a valid predicate of Yen's path logic. □

To discuss the lower bound complexity, we show that checking strong detectability requires exponential space. We reduce the *coverability problem*, which is known to be EXPSPACE-complete (Esparza, 2018).

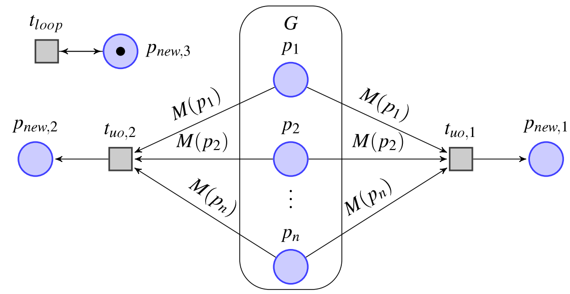

Fig. 1. Sketch of the hardness construction.

Theorem 4. *Checking strong detectability is EXPSPACE-hard.*

Proof. Given a Petri net system (N, M_0), the coverability problem asks whether there is a reachable marking that covers a given marking M.

Let (N, M_0) and M be the instance of the coverability problem. We construct a new Petri net as follows (see Fig. 1 for an illustration). We add two new unobservable transitions $t_{uo,1}$ and $t_{uo,2}$, and two new place $p_{new,1}$ and $p_{new,2}$ initialized with zero tokens to (N, M_0), and we define $Pre(p, t_{uo,1}) = Pre(p, t_{uo,2}) = M(p)$ for $p \in P$, and $Post(p_{new,i}, t_{uo,i}) = 1$ for $i = 1, 2$; unspecified mappings are defined as zero. We add a new isolated place $p_{new,3}$ initialized with one token, and define a new self-loop transition t_{loop} in $p_{new,3}$ to guarantee that the system is deadlock free. Finally, we define the labeling function $\ell : T \cup \{t_{uo,1}, t_{uo,2}, t_{loop}\} \to T \cup \{t_{loop}\}$ by $\ell(t) = t$ for $t \in T \cup \{t_{loop}\}$, and $\ell(t_{uo,1}) = \ell(t_{uo,2}) = \varepsilon$.

By the construction, unobservable transitions $t_{uo,1}$ and $t_{uo,2}$ can be fired if and only if M can be covered. Thus, if these two unobservable transitions are firable, then the modified system is not strongly detectable because we cannot distinguish between the tokens in $p_{new,1}$ and $p_{new,2}$. On the other hand, if these two unobservable transitions are not firable, then all firable transitions are observable, which directly implies that the system is strongly detectable. Overall, the original system covers M if and only if the modified system is strongly detectable. Hence, deciding strong detectability is EXPSPACE-hard. □

4. Weak detectability

In some applications, we only need to determine, after a finite number of observations, the current and subsequent states for some trajectories of the system. This property is referred to as weak detectability and is defined as follows.

Definition 5. An LPN system $G = (N, M_0, \Sigma, \ell)$ is *weakly detectable* if there is an integer $n \ge 0$ and a word $s \in L^\omega(G)$ such that $|R(G, s')| = 1$ for any prefix s' of s of length at least n.

We now show that deciding weak detectability is undecidable for LPNs.

Theorem 6. *Weak detectability is undecidable for LPNs.*

Proof. Let G_1 and G_2 be two LPNs with no unobservable transitions, i.e., $\ell(t)$ is not the empty word for any transition t. It is well-known that the inclusion problem, which asks whether $L(G_1) \subseteq L(G_2)$, is undecidable (Hack, 1976) for LPNs even when all transitions are observable. Next, we reduce the inclusion problem to the weak detectability verification problem.

From G_1 and G_2, we construct an LPN G as follows. We create 10 new places p_0 up to p_9, and we use new labels x, a, and b as depicted in Fig. 2. Place p_1 (resp. p_4, p_7) is connected by a self-loop

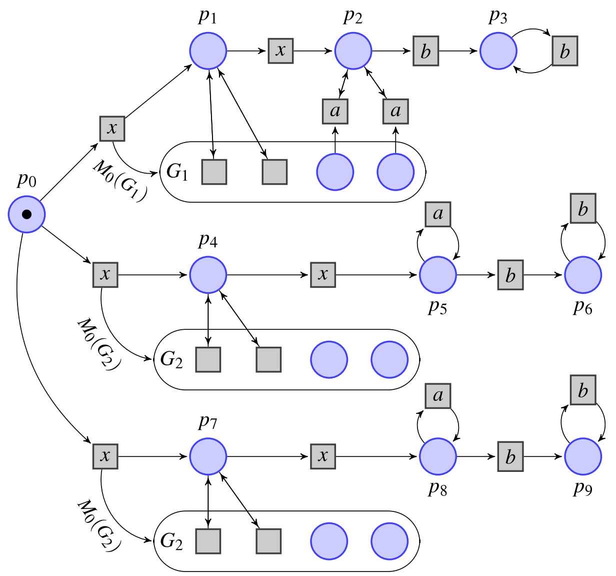

Fig. 2. Sketch of the construction; labels depicted in transitions.

to every transition of G_1 (resp. G_2). Intuitively, p_1 (resp. p_4, p_7) allows G to simulate G_1 (resp. G_2). For every place of G_1, we create a new transition labeled by a to which the place is connected, and through which there is a self-loop from place p_2 back to place p_2. The intuition is that p_2 allows G to remove tokens from the G_1 part under a word from a^*. The rest of the Petri net G is as depicted in Fig. 2.

The initial marking of G consists of a single token in place p_0. At the beginning, only the transitions connected to place p_0 are enabled. Then, after the first transition (which is labeled by x), the net G simulates either G_1 or G_2 from their corresponding initial markings, and hence the ω-language of G is

$$\{xwxa^{y(w)}b^\omega \mid w \in L(G_1)\} \cup \{xwx(a^\omega + a^*b^\omega) \mid w \in L(G_2)\} \\ \cup \{xw \mid w \in L^\omega(G_1) \cup L^\omega(G_2)\}$$

where $y(w)$ is finite and depends on the number of tokens in the net G_1 after generating the word $w \in L(G_1)$.

We show that $L(G_1) \subseteq L(G_2)$ if and only if G is not weakly detectable.

If $L(G_1) \nsubseteq L(G_2)$, then there exists a word $w \in L(G_1) - L(G_2)$. We now consider all markings of G_1 after generating the word w. There can be several, but a finite number of such markings, because the length of w is finite and there are no transitions labeled by ε in G_1. We sum the tokens in every such marking and let k denote its maximum. This means that after generating $xwxa^kb$, the marking of G is such that a single token is in place p_3, no tokens are in the part of G_1, because k is the maximum number of tokens in G_1 after generating w, so we had to use all of them to generate a^k, and the part of G_2 contains no tokens. If the net now keeps generating b^ω, we stay in this marking for ever. This is the only marking reachable by the ω-word $xwxa^kb^\omega$, because $w \notin L(G_2)$. Thus, the net is weakly detectable; the n from the definition is $n = |xwx| + k + 1$, which is a constant for such a fixed word w.

If $L(G_1) \subseteq L(G_2)$, then any word $xvxa^ub^\omega$ generated using the part with G_1, that is, $v \in L(G_1)$ and u is bounded by the number of tokens in any marking of G_1 reachable after generating v in G_1, can be simulated using the part of G_2. Moreover, any word from $\{xwx(a^\omega + a^*b^\omega) \mid w \in L(G_2)\} \cup \{xw \mid w \in L^\omega(G_2)\}$ generated by the part using G_2 always leads to at least two different markings because of the two identical parts in G simulating G_2, cf. the places p_4, p_5, p_6 and p_7, p_8, p_9, and hence G is not weakly detectable. □

5. Discussion

Our proof of Theorem 6 is similar, but more involved, than the construction of Tong, Li, Seatzu, and Giua (2017) showing that checking current-state opacity is undecidable. The secret set in their construction is infinite in general, and hence it is a natural question whether undecidability of current-state opacity follows from the infinity of the secret set. In other words, whether current-state opacity is decidable if the secret set is finite. As a consequence of Theorem 6, current-state opacity is undecidable even if the secret set consists of a single marking (Masopust & Yin, 2018).

References

Atig, M. F., & Habermehl, P. (2011). On Yen's path logic for Petri nets. *International Journal of Foundations of Computer Science*, *22*(4), 783–799.

Cabasino, M. P., Giua, A., Lafortune, S., & Seatzu, C. (2012). A new approach for diagnosability analysis of Petri nets using verifier nets. *IEEE Transactions on Automatic Control*, *57*(12), 3104–3117.

Dickson, L. (1913). Finiteness of the odd perfect and primitive abundant numbers with *n* distinct prime factors. *American Journal of Mathematics*, *35*(4), 413–422.

Esparza, J. (2018). Petri nets. In *Lecture Notes*.

Hack, M. (1976). Decidability questions for Petri nets. (PhD Thesis), Cambridge, MA, USA: MIT.

Keroglou, C., & Hadjicostis, C. N. (2017). Verification of detectability in probabilistic finite automata. *Automatica*, *86*, 192–198.

König, D. (1927). Über eine Schlussweise aus dem Endlichen ins Unendliche. *Acta Scientiarum Mathematicarum*, *3*, 121–130.

Masopust, T. (2018). Complexity of deciding detectability in discrete event systems. *Automatica*, *93*, 257–261.

Masopust, T., & Yin, X. (2018). Deciding detectability for labeled Petri nets. arxiv preprint:1802.02087.

Ozveren, C. M., & Willsky, A. S. (1990). Observability of discrete event dynamic systems. *IEEE Transactions on Automatic Control*, *35*(7), 797–806.

Peterson, J. L. (1981). Petri net theory and the modeling of systems. NJ, USA: Prentice Hall.

Ramadge, P. J. (1986). Observability of discrete event systems. In *Conference on Decision and Control (CDC)* (pp. 1108–1112).

Shu, S., & Lin, F. (2011). Generalized detectability for discrete event systems. *Systems & Control Letters*, *60*(5), 310–317.

Shu, S., & Lin, F. (2013). Delayed detectability of discrete event systems. *IEEE Transactions on Automatic Control*, *58*(4), 862–875.

Shu, S., Lin, F., & Ying, H. (2007). Detectability of discrete event systems. *IEEE Transactions on Automatic Control*, *52*(12), 2356–2359.

Tong, Y., Li, Z., Seatzu, C., & Giua, A. (2017). Decidability of opacity verification problems in labeled Petri net systems. *Automatica*, *80*, 48–53.

Yen, H.-C. (1992). A unified approach for deciding the existence of certain Petri net paths. *Information and Computation*, *96*(1), 119–137.

Yin, X. (2017). Initial-state detectability of stochastic discrete-event systems with probabilistic sensor failures. *Automatica*, *80*, 127–134.

Yin, X. (2018). Verification of prognosability for labeled Petri nets. *IEEE Transactions on Automatic Control*, *63*(6), 1828–1834.

Yin, X., & Lafortune, S. (2017). On the decidability and complexity of diagnosability for labeled Petri nets. *IEEE Transactions on Automatic Control*, *62*(11), 5931–5938.

Yin, X., & Lafortune, S. (2017). Verification complexity of a class of observational properties for modular discrete events systems. *Automatica*, *83*, 199–205.

Zhang, K. (2017). The problem of determining the weak (periodic) detectability of discrete event systems is PSPACE-complete. *Automatica*, *81*, 217–220.

Zhang, K., & Giua, A. (2018). Weak (approximate) detectability of labeled Petri nets with inhibitor arcs. In *WODES* (pp. 179–183).