Divergence properties of labeled Petri nets and their relevance for diagnosability analysis*

Alessandro Giua, Stéphane Lafortune, Carla Seatzu

Abstract

In this note we focus on labeled Petri nets and formalize two properties, *language divergence* and *marking divergence*, discussing their relevance for diagnosability analysis. In particular, we review the results for diagnosability and K-diagnosability presented in a paper titled "A new approach for diagnosability analysis of Petri nets using verifier nets" that we coauthored. We show that these results apply to nets that are language divergence-free, an assumption that was not explicitly mentioned in that paper. In addition, we also provide an alternative *structural* assumption — which does not require testing the *behavioral* property of divergence-freeness — under which the above results hold.

Published as: A. Giua, S. Lafortune, C. Seatzu, "Divergence properties of labeled Petri nets and their relevance for diagnosability analysis," *IEEE Trans. on Automatic Control*, Vol. 65, No. 7, pp. 3092-3097, 2020. DOI: 10.1109/TAC.2019.2947650

*A. Giua and C. Seatzu are with the Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari 09124, Italy (email: giua@unica.it, carla.seatzu@unica.it). S. Lafortune is with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109-2122 USA (e-mail: stephane@umich.edu).

This work was partially supported by Project RASSR05871 MOSIMA financed by Region Sardinia, FSC 2014-2020, annuity 2017, Subject area 3, Action Line 3.1.

1 Introduction

In paper [3], which we co-authored with M.P. Cabasino, necessary and sufficient conditions for diagnosability and K-diagnosability of labeled Petri nets were presented. It was pointed out to us by Béatrice Bérard, Stefan Haar, Sylvain Schmitz, and Stefan Schwoon, that two key results in [3] — Theorems 6.4 and 6.7 — are incorrect as stated. More precisely, both the necessity and the sufficiency parts of each theorem do not hold in general and examples to that effect were provided to us by Bérard *et al.*

From these examples we realized that an important assumption was missing in [3]. The results contained therein, in fact, apply to nets that are *divergent-free* but the requirement for this property was never explicitly mentioned. On the contrary, we point out that a sufficient condition ensuring such a property, namely the acyclicity of the unobservable subnet, was explicitly mentioned in [2], where some of the results in [3] were preliminarily introduced.

In a partially observed discrete event system, *divergence* [4] is an undesirable property. It describes the possibility for a system of concealing an infinite sequence of activities, thereby renouncing to engage in any further communication with the environment. As lucidly explained by Hoare [4]: "It is a shame to devote so much attention to divergence, when divergence is always something we do not want. Unfortunately, it seems to be an inevitable consequence of any efficient of (*sic*) even computable method of implementation."

In the case of labeled Petri nets, very few works have been devoted to the analysis of divergence and to investigate how it may affect diagnosis and diagnosability. Two recent contributions in this framework are [1, 7]. In these papers, the authors focus on the problem of determining the computational complexity of diagnosability analysis in labeled Petri nets. Bérard *et al.* [1] show that, in the case of unbounded nets, the analysis is EXSPACE-hard due to some sequences (the so called *twin-fair traces*) that appear in a structure called *Verifier*. Yin and Lafortune [7] show that the diagnosability verification problem can be reduced to a model checking problem for unbounded Petri nets called the "satisfiability problem of Yen's formula", and draw analogous conclusions in terms of complexity (see also [8] for some clarifications).

In this paper, motivated by the above results and by the fact that divergence is an undesirable property, we aim to characterize nets that are divergence-free and discuss a structural condition which implies divergence-freeness.

We start by presenting in Section 2 the definition of partially observed Petri nets and some properties related to repetitive sequences, that characterize the infinite behaviour of this model, and thus are fundamental in the study of divergence and diagnosability. Section 3 introduces two important notions, called *language divergence-freeness* and *marking divergence-freeness*. It is shown that these properties characterize nets such that, respectively, the set of sequences and the set of markings that are consistent with a finite observation is always finite. In Section 4 we recall the definitions of diagnosability and K-diagnosability, and clarify the considered framework. In Section 5 we first recall the main results presented in [3]

concerning the analyis of diagnosability and K-diagnosability. Then, we discuss the counterexamples by Bérard *et al.*, which show that such results are not correct for divergent nets. Finally, in Section 6 we show that the results in [3] are indeed correct for divergence-free nets. In this section we also discuss the alternative assumption presented in [2] which requires the acyclicity of the unobservable subnet. We show that for the purpose of diagnosability analysis this structural assumption provides sufficient conditions for divergence-freeness with the important computational advantage of not requiring the analysis of the system behavior.

2 Preliminaries and notations

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; and $Pre : P \times T \to \mathbb{N}$ and $Post : P \times T \to \mathbb{N}$ are the *pre–* and *post–* incidence functions that specify the arcs. $C = Post - Pre$ denotes the incidence matrix of the net. A *marking* (i.e., net state) is a vector $M : P \to \mathbb{N}$ that assigns to each place of a P/T net a non–negative integer number of tokens, represented by black dots in diagrams. We denote by $M(p)$ 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. Hereafter we refer to a P/T net as a Petri net, often abbreviated as PN.

A transition t is said to be enabled at M iff $M \geq Pre(\cdot\,, t)$; an enabled transition t may fire yielding the marking $M' = M + C(\cdot\,, t)$. We write $M[\sigma\rangle$ to denote that the sequence of transitions $\sigma = t_{j_1} \cdots t_{j_k}$ is enabled at M, and we write $M\ [\sigma\rangle\ M'$ to denote that the firing of σ yields M'.

The set of all finite sequences that are enabled at the initial marking M_0 is denoted by $L(N, M_0)$, i.e., $L(N, M_0) = \{\sigma \in T^* \mid M[\sigma\rangle\}$, where T^* is the Kleene closure of T, namely the set of all possible finite sequences that can be obtained combining elements in T. Moreover, T^ω and $L^\omega(N, M_0)$, denote respectively, the set of infinite sequences that can be obtained combining elements in T and the set of infinite length sequences that can be generated at M_0. We use λ to denote an empty sequence of transitions, i.e., $\sigma\lambda = \lambda\sigma = \sigma$, $\forall \sigma \in T^*$.

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

A Petri net having no directed circuits is called *acyclic*.

A net system $\langle N, M_0 \rangle$ is *bounded* if there exists a positive constant k such that, for all $M \in R(N, M_0)$, and for all $p \in P$, $M(p) \leq k$. If this is not the case, namely, if the number of tokens in one or more places can grow arbitrarily large, then the Petri net system is *unbounded*.

A non-empty sequence $\sigma \in T^* \setminus \{\lambda\}$ is called *repetitive* if there exists a marking $M_1 \in R(N, M_0)$ such that

$$M_1[\sigma\rangle M_2[\sigma\rangle M_3[\sigma\rangle \cdots \tag{1}$$

i.e., if it can fire infinitely often starting from M_1. It is possible to distinguish two different types of repetitive sequences:

– *stationary* sequence: if in (1) $M_i = M_{i+1}$ for all $i = 1, 2, \ldots$.

– *increasing* sequence: if in (1) $M_i \lneq M_{i+1}$ for all $i = 1, 2, \ldots$.

A *labeling function* $\mathcal{L} : T \to L \cup \{\varepsilon\}$ assigns to each transition $t \in T$ either a symbol from a given alphabet L or the empty string ε. We denote by T_u the set of transitions whose label is ε, i.e., $T_u = \{t \in T \mid \mathcal{L}(t) = \varepsilon\}$. Transitions in T_u are called *unobservable* or *silent*. We denote by T_o the set of transitions labeled with a symbol in L. Transitions in T_o are called *observable* because when they fire their label can be observed.

We extend the labeling function to define the *projection operator* $\mathcal{L} : T^* \to L^*$ recursively as follows:

(i) if $t_j \in T_o$ then $\mathcal{L}(t_j) = l$ for some $l \in L$;

(ii) if $t_j \in T_u$ then $\mathcal{L}(t_j) = \varepsilon$;

(iii) if $\sigma \in T^* \wedge t_j \in T$ then $\mathcal{L}(\sigma t_j) = \mathcal{L}(\sigma)\mathcal{L}(t_j)$;
Moreover, $\mathcal{L}(\lambda) = \varepsilon$.

Using the extended labeling function, the language of transition labels is therefore denoted by $\mathcal{L}(L(N, M_0))$.

Finally, given a net $N = (P, T, Pre, Post)$, and a subset $T' \subseteq T$ of its transitions, we define the $T'-$*induced subnet of* N as the new net $N' = (P, T', Pre', Post')$ where $Pre', Post'$ are the restrictions of $Pre, Post$ to T'.

In the following, the unobservable subnet, i.e., the T_u-induced subnet of N, is denoted as N_u.

3 Divergence-free nets

In this section we formalize two key definitions related to divergence. Similar notions can be found in the framework of sequential processes [4].

Definition 1 *A labeled PN* $\langle N, M_0, \mathcal{L}\rangle$ *is called* language divergence-free *if for all* $M \in R(N, M_0)$ *it holds that* $\mid L(N_u, M) \mid < \infty$, *i.e., any reachable marking* M *enables a finite number of sequences of unobservable transitions.* $\Diamond$

Definition 2 *A labeled PN* $\langle N, M_0, \mathcal{L}\rangle$ *is called* marking divergence-free *if for all* $M \in R(N, M_0)$ *it holds that* $\mid R(N_u, M) \mid < \infty$, *i.e., any reachable marking* M *has a finite unobservable reach.* $\Diamond$

The following result, which trivially derives from the above definitions, provides a test to verify the above two properties looking at repetitive sequences.

Fact 1 *A labeled PN $\langle N, M_0, \mathcal{L}\rangle$ is:*
(1) language divergence-free if and only if it admits no repetitive sequence of unobservable transitions;
(2) marking divergence-free if and only if it admits no increasing repetitive sequence of unobservable transitions. ◊

Remark 1 *From the previous result it also follows that language divergence-freeness implies marking divergence-freeness, while the converse does not hold in general.* ◊

We now prove a result that will be used in the following, namely that in a language divergence-free net the set of firing sequences consistent with a given observation is finite.

Proposition 1 *A labeled PN $\langle N, M_0, \mathcal{L}\rangle$ is language divergence-free if and only if for all observations $\sigma_o \in T_o^*$ it holds that*

$$| \{\sigma \in L(N, M_0) \mid \mathcal{L}(\sigma) = \sigma_o\} | < \infty. \tag{2}$$

Proof:

If. Consider an evolution $M_0[\sigma\rangle M$ which reaches a generic marking M and let $\sigma_o = \mathcal{L}(\sigma)$ be the corresponding observation. If (2) holds, then only a finite number of unobservable transitions can fire after σ. This implies that the net is language divergence-free according to Definition 1.

Only if. This implication can be proved by induction on the length k of σ_o.

If σ_o has length $k = 0$, i.e., $\sigma_o = \varepsilon$, then $\{\sigma \in L(N, M_0) \mid \mathcal{L}(\sigma) = \varepsilon\} = L(N_u, M_0)$ which is finite by Definition 1.

Assume the result holds for all σ_o of length k and consider a sequence $\sigma_o t \in T_o^*$ of length $k + 1$. Then

$$\begin{aligned}&\{\sigma \in L(N, M_0) \mid \mathcal{L}(\sigma) = \sigma_o t\} = \\ &\{\sigma' t \sigma'' \mid \mathcal{L}(\sigma') = \sigma_o, M_0[\sigma'\rangle M'[t\rangle M'', \\ &\qquad\qquad \sigma'' \in L(N_u, M'')\}\end{aligned}$$

which is also finite by the assumption and by Definition 1. □

With a similar reasoning, it can be shown that in a marking divergence-free net the set of markings consistent with a given observation is finite. This is formalized in the next result, whose proof is omitted.

Proposition 2 *A labeled PN $\langle N, M_0, \mathcal{L}\rangle$ is marking divergence-free if and only if for all observation $\sigma_o \in T_o^*$ it holds*

$$| \{M \in \mathbb{N}^m \mid M_0[\sigma\rangle M, \mathcal{L}(\sigma) = \sigma_o\} | < \infty. \tag{3}$$

■

4 Diagnosability definitions

We now recall two fundamental definitions, namely *diagnosability* and *K-diagnosability* of labeled Petri nets. In particular, we provide them under the same general setting considered in [3], where the labeling function is arbitrary and thus two or more observable transitions may share the same label. Furthermore, as in [3], we assume that the system does not enter a deadlock after the firing of a fault transition: the latter condition, which is purely technical and common in the literature, is introduced to ensure that the notion of diagnosability is well posed. However, to simplify the analysis presented in the following sections, the definitions of diagnosability and K-diagnosability are rewritten in slightly different terms with respect to [3]. Finally, to avoid a cumbersome notation we consider a single fault class containing all transitions in the set of fault transitions T_f. It holds that $T_f \subseteq T_u$, i.e., all fault transitions are labeled with the empty string ε.

Definition 3 *A labeled PN $\langle N, M_0, \mathcal{L}\rangle$ is diagnosable iff condition $\mathcal{A}$ holds, where*

$\mathcal{A}$: There does not exist an infinite transition sequence $\sigma = \sigma_1 t_f \sigma_2 \in L^\omega(N, M_0)$ such that $\sigma_1 \in T^*, t_f \in T_f, \sigma_2 \in T^\omega$ and for all finite prefixes $\hat{\sigma} \preceq \sigma$ there exists a sequence $\hat{\sigma}' \in L(N, M_0) \cap (T \setminus T_f)^*$ such that $\mathcal{L}(\hat{\sigma}') = \mathcal{L}(\hat{\sigma})$. ◊

Definition 4 *A labeled PN $\langle N, M_0, \mathcal{L}\rangle$ is K-diagnosable iff condition $\mathcal{A}'$ holds, where*

$\mathcal{A}'$: There does not exist a transition sequence $\sigma = \sigma_1 t_f \sigma_2 \in L(N, M_0)$ such that $\sigma_1 \in T^*, t_f \in T_f, \sigma_2 \in T^*$, the length of σ_2 is $|\sigma_2| > K$, and for all prefixes $\hat{\sigma} \preceq \sigma$ there exists a sequence $\hat{\sigma}' \in L(N, M_0) \cap (T \setminus T_f)^*$ such that $\mathcal{L}(\hat{\sigma}') = \mathcal{L}(\hat{\sigma})$. ◊

In simple words, diagnosability implies that the occurrence of a fault can be detected after a finite number of transition firings; diagnosability in K steps implies that the occurrence of a fault can be detected after a finite number K of transition firings.

5 Main results in [3] and counterexamples

In this section we first recall the key results in [3], namely Proposition 6.3 [3] and Theorems 6.4 [3] and 6.7 [3]. Then we provide two counterexamples to them.

All such results use the notion of Verifier Net (VN) [3]. The VN is a labeled Petri net obtained by composing the unfaulty subnet $\langle N', M'_0, \mathcal{L}' \rangle$, namely the $(T \setminus T_f)$-induced subnet, and the original system $\langle N, M_0, \mathcal{L} \rangle$, assuming that the synchronization is performed on the observable transition labels. The set $F(\text{VN})$ is the set of faulty nodes in the reachability/coverability graph (RG/CG) of the VN, namely the nodes that can be reached from the initial node by a path that contains a transition (λ, t_f), with $t_f \in T_f$.

Proposition 6.3 [3]: Given a labeled Petri net system $\langle N, M_0, \mathcal{L} \rangle$ and its VN, if a sequence

$$\tilde{\sigma} = (t'_{i_1}, t_{i_1})(t'_{i_2}, t_{i_2}) \dots (t'_{i_k}, t_{i_k})$$

is repetitive in the VN, then there exists a repetitive sequence $\sigma' = t'_{i_1} t'_{i_2} \dots t'_{i_k}$ in $\langle N', M'_0 \rangle$ and a repetitive sequence $\sigma = t_{i_1} t_{i_2} \dots t_{i_k}$ in $\langle N, M_0 \rangle$ and both sequences σ and σ' have the same observable projection. ■

Finally, let us recall Theorems 6.4 [3] and 6.7 [3].

Theorem 6.4 [3]: A labeled PN system $\langle N, M_0, \mathcal{L} \rangle$ is diagnosable iff there does not exist a cycle in the RG/CG graph of its Verifier Net which is associated with a firable repetitive sequence and is reachable from a node in the set $F(\text{VN})$. ■

Theorem 6.7 [3]: Let $\langle N, M_0, \mathcal{L} \rangle$ be a labeled Petri net system. There exists a finite K such that the system is diagnosable in K steps iff in the RG/CG of its VN no node in the set $F(\text{VN})$ belongs to a cycle. ■

Let us now discuss two counterexamples to Theorem 6.4 [3] provided to us by Bérard *et al.* The first one is relative to the necessary (*only if*) condition of the theorem, the second one to the sufficient (*if*) condition. The second example also shows an exception to the validity of Proposition 6.3 [3].

The first labeled Petri net system, taken from [1], is shown in Fig. 1.a where t_1 is an unobservable transition and $\mathcal{L}(t_2) = a$. Such a net, which is divergent due to the presence of the selfloop (t_1, p_1), is clearly diagnosable. Indeed, after the fault occurs, only transition t_2 can fire and an a is observed: the fault occurrence is thus reconstructed. However, the condition in Theorem 6.4 [3] does not hold. The VN is shown in Fig. 1.b. Here places marked with a prime are those of the fault-free net, while the others are the places of the original net; the two nets are composed synchronizing transitions with the same label. The reachability graph of the VN is shown in Fig. 1.c where, for sake of clarity, markings are represented by multisets: as an example, $p'_1 + p_1$ denotes the marking with only one token in place p'_1 and one in p_1.

As it can be seen, in the reachability graph of the VN there exists a cycle associated with a firable repetitive sequence of the VN, i.e., the self-loop $\tilde{\sigma} = (t'_1, \lambda)$, which can fire from a node in $F(\text{VN})$, i.e., the node $p'_1 + p_2$.

This example also allows us to highlight an exception to the validity of Proposition 6.3 [3]: in this case the repetitive sequence of the VN $\tilde{\sigma} = (t'_1, \lambda)$ projected on the two nets gives $\sigma' = t'_1$ and $\sigma = \lambda$ but the latter, being the empty string, is not a repetitive sequence as

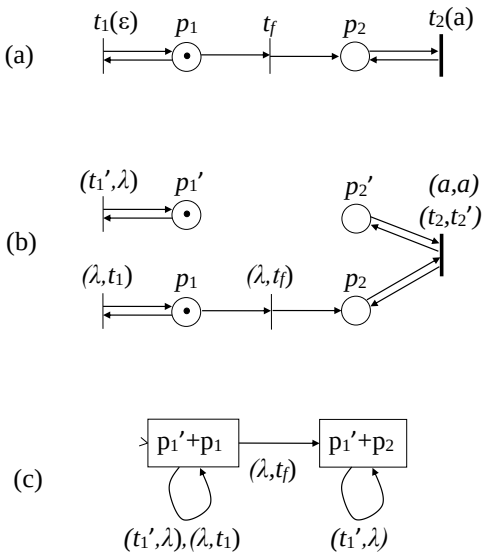


Figure 1: A counterexamle to the *only if* condition of Theorem 6.4 [3]: (a) a Petri net, (b) its Verifier Net, (c) the reachability graph of the Verifier Net.

prescribed and does not correspond to an evolution of the unfaulty net.

The second counterexample is reported in Fig. 2 where t_5 is an unobservable transition, $\mathcal{L}(t_2) = \mathcal{L}(t_4) = a$ and $\mathcal{L}(t_1) = \mathcal{L}(t_3) = b$. Such a net, which is divergent due to the presence of the selfloop (ε_5, p_1), is not diagnosable according to Definition 3. In fact, each faulty sequence $\hat{\sigma} = t_3 t_f t_4^k$, for $k \in \mathbb{N}$, which is a prefix of $\sigma = t_3 t_f t_4^\omega$, produces the observation $\mathcal{L}(\hat{\sigma}) = ba^k$, which may also be produced by the firing of sequence $\hat{\sigma}' = {t_5}^k t_1 t_2^k$. However, Theorem 6.4 [3] would lead to the opposite conclusion. To show this we compute the VN associated with the Petri net in Fig. 2 and its coverability graph. The VN is reported in Fig. 3.a. For sake of clarity, in order to avoid intersections among arcs, places are often repeated but represented with a unique different color. A part of the coverability graph of the VN is reported in Fig. 3.b. In particular, this figure only shows the root node and nodes in the set $F(\text{VN})$ reachable after the occurrence of the fault, while the other nodes are omitted. Again, in Fig. 3.c, as well as in the previous Fig. 1.b, markings are not represented as vectors but as multisets: as an example, $p_2' + \omega p_3 + p_5$ denotes an ω-marking assigning one token to place p_2' and p_5 and an arbitrarily large number of tokens to place p_3. In Fig. 3 one can see two cycles at two nodes in $F(\text{VN})$, both involving only transition (t_2', t_4). However, as it clearly appears from Fig. 3.b, such cycles do not correspond to repetitive sequences in the VN since transition (t_2', t_4) reduces the number of tokens in p_3' whenever it fires.

6 Revised diagnosability analysis

In this section we show how divergence properties are relevant for diagnosability analysis.

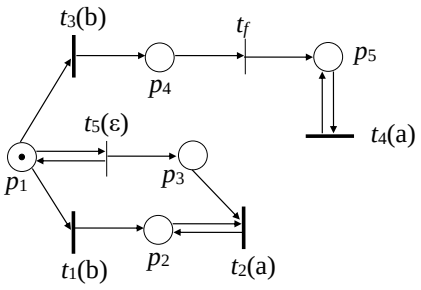


Figure 2: A counterexample to the *if* condition of Theorem 6.4 [3].

In particular, we show which additional assumption in Theorems 6.4 [3] and 6.7 [3] allows one to obtain a correct test for diagnosability and K-diagnosability analysis.

6.1 A behavioral assumption

We first introduce a new condition, denoted as $\mathcal{B}$, which allows us to provide a revised formulation of Theorems 6.4 [3] and 6.7 [3]. In particular, this can be easily done putting condition $\mathcal{B}$ in relationship with condition $\mathcal{A}$ introduced above.

$\mathcal{B}$: There does not exist an infinite transition sequence $\sigma = \sigma_1 t_f \sigma_2 \in L^\omega(N, M_0)$ such that: (a) $\sigma_1 \in T^*, t_f \in T_f, \sigma_2 \in T^\omega$ and (b) there exists an infinite transition sequence $\sigma' \in L^\omega(N, M_0) \cap (T \setminus T_f)^\omega$ such that $\mathcal{L}(\sigma') = \mathcal{L}(\sigma)$.

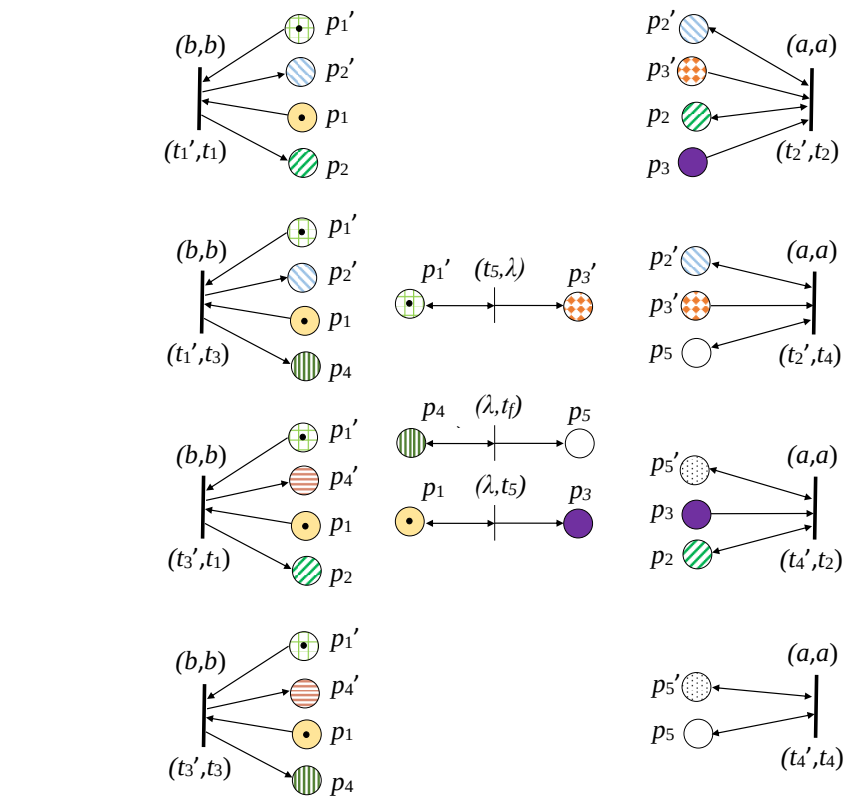
Obviously $\mathcal{A} \Longrightarrow \mathcal{B}$ but the reverse implication does not necessarily hold. This can be seen considering the net in Fig. 2. Consider for instance the infinite faulty sequence $\sigma = t_3 t_f t_4^\omega$ producing observation $\mathcal{L}(\sigma) = ba^\omega$. Obviously condition $\mathcal{A}$ does not hold since for any prefix $\hat{\sigma} = t_3 t_f t_4^k$ there exists a fault-free sequence $\hat{\sigma}' = {t_5}^k t_1 t_2^k$ such that $\mathcal{L}(\hat{\sigma}') = \mathcal{L}(\hat{\sigma}) = ba^k$. By Definition 3, we conclude that the net is not diagnosable. However, condition $\mathcal{B}$ holds because there exists no infinite sequence σ' as defined in the statement of the condition. In fact the only infinite fault-free sequence of this net is ${t_5}^\omega$ which produces observation $\mathcal{L}({t_5}^\omega) = \varepsilon$.

We now show that language divergence-freeness implies that the two conditions $\mathcal{A}$ and $\mathcal{B}$ are equivalent[1].

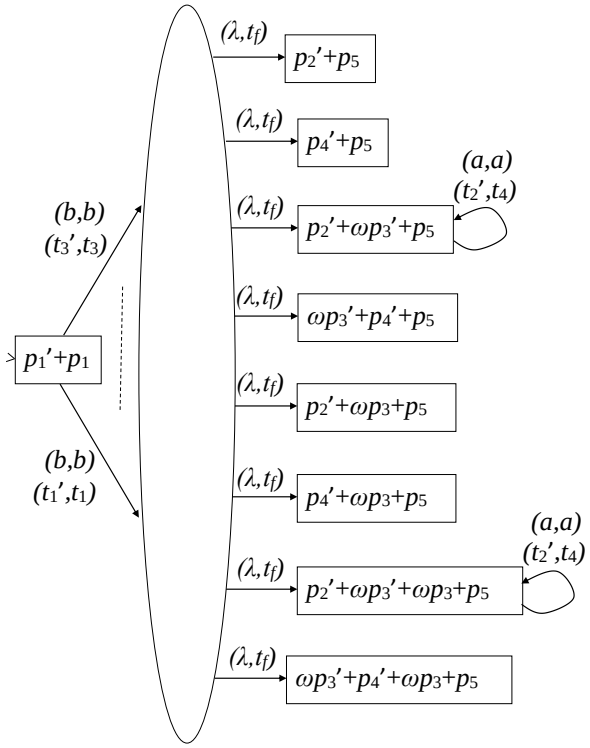
Proposition 3 *For a language divergence-free labeled PN $\langle N, M_0, \mathcal{L}\rangle$ it holds that $\mathcal{A} \Longleftrightarrow \mathcal{B}$.*

Proof: As we have mentioned above, the implication $\mathcal{A} \Longrightarrow \mathcal{B}$ follows immediately from the definition of the two conditions. We are left to prove that for language divergence-free

[1]The result of Proposition 3 also follows from the more general setting in [1] (see Lemma 2.6) where condition $\mathcal{A}$ is called "finitely diagnosable" and condition $\mathcal{B}$ is called "trace diagnosable".



(a)



(b)

Figure 3: (a) Verifier Net for the net in Fig. 2, (b) coverability graph of the Verifier Net for the net in Fig. 2.

nets the reverse implication $\mathcal{B} \Longrightarrow \mathcal{A}$ holds. This will be shown by contraposition, namely proving that $\neg\mathcal{A} \Longrightarrow \neg\mathcal{B}$.

The language divergence-free assumption (see eq. (2)) implies that

$$\begin{aligned} &\forall \hat{\sigma} \in L(N, M_0) : \\ &\quad | \{\hat{\sigma}' \in L(N, M_0) \mid \mathcal{L}(\hat{\sigma}') = \mathcal{L}(\hat{\sigma})\} | < \infty. \end{aligned} \tag{4}$$

Now consider an infinite transition sequence $\sigma = \sigma_1 t_f \sigma_2 \in L^\omega(N, M_0)$ such that $\sigma_1 \in T^*, t_f \in T_f, \sigma_2 \in T^\omega$ which violates condition $\mathcal{A}$. We can also write this sequence as:

$$\sigma = \sigma_1 t_f \sigma_2 = \sigma_1 t_f \sigma_{uo,1} t_{j_1} \sigma_{uo,2} t_{j_2} \cdots \tag{5}$$

where for $i \in \{1, 2, \cdots\}$ it holds $\sigma_{uo,i} \in T_u^*$ and $t_{j_i} \in T_o$.

Consider the set of sequences

$$\Sigma_0 = \{\hat{\sigma}' \in L(N, M_0) \cap (T \setminus T_f)^* \ \mid \ \mathcal{L}(\hat{\sigma}') = \mathcal{L}(\sigma_1 t_f)\}$$

which is finite by (4). We construct a forest that has as root nodes (tier 0) the elements of Σ_0. The set of nodes in tier i (for $i = \{1, 2, \ldots\}$) is

$$\begin{aligned} \Sigma_i = \{&\hat{\sigma}' \in L(N, M_0) \cap (T \setminus T_f)^* \ \mid \\ &\mathcal{L}(\hat{\sigma}') = \mathcal{L}(\sigma_1 t_f \sigma_{uo,1} t_{j_1} \ldots \sigma_{uo,i} t_{j_i})\} \end{aligned}$$

and we add a directed arc from a node $\hat{\sigma}'_{i-1}$ in tier $i-1$ to a node $\hat{\sigma}'_i$ in tier i if $\hat{\sigma}'_{i-1} \preceq \hat{\sigma}'_i$. Such a forest has a finite branching by (2) but, since it violates condition $\mathcal{A}$, has an infinite number of nodes. By König's lemma [5] the forest must have an infinite path. Such a path corresponds to an infinite transition sequence σ' that violates condition $\mathcal{B}$. □

We point out that it is possible to prove that the above proposition also holds under the weaker assumption that the net is marking divergence-free. However, in this case the proof is more involved and goes beyond the scope of this note.

From the above Proposition 3, Definition 3 can be particularized to language divergence-free labeled PN as formalized by the following corollary.

Corollary 1 *A language divergence-free labeled PN $\langle N, M_0, \mathcal{L}\rangle$ is diagnosable iff condition $\mathcal{B}$ holds.* ◊

Another consequence of language divergence-freeness is the following.

Proposition 4 *Proposition 6.3 [3] holds for a language divergence-free labeled PN $\langle N, M_0, \mathcal{L}\rangle$.*

Proof: *First from the definition of VN we know that the fault-free sequence $\sigma' \in L(N', M'_0)$ and the sequence $\sigma \in L(N, M_0)$ have the same observable projection $\mathcal{L}'(\sigma') = \mathcal{L}(\sigma)$. If*

sequence $\tilde{\sigma}$ is repetitive in the VN, then there exists a reachable marking $\tilde{M} = [M'^T, M^T]^T$ such that

$$\begin{bmatrix} M' \\ M \end{bmatrix} \; [\tilde{\sigma}\rangle_{VN} \; \begin{bmatrix} \bar{M}' \\ \bar{M} \end{bmatrix} \geq \begin{bmatrix} M' \\ M \end{bmatrix}$$

which implies

$$M' \, [\sigma'\rangle_{N'} \, \bar{M}' \geq M' \qquad \textit{and} \qquad M \, [\sigma\rangle_{N} \, \bar{M} \geq M. \tag{6}$$

Now, consider the assumption that system $\langle N, M_0, \mathcal{L}\rangle$ is divergence-free, which obviously implies that also the fault-free system $\langle N', M'_0, \mathcal{L}'\rangle$ is divergence-free.

By the definition of VN, at least one between σ' and σ must be different from the empty string λ. Assume, with no loss of generality, that σ' is non-empty: since it satisfies (6) *it is repetitive, hence due to the divergence-freeness assumption must contain an observable transition. This implies that also σ contains at least an observable transition, i.e., it is non-empty: since σ satisfies* (6) *it is also repetitive.* □

The last two results presented above have the following implication, which can be expressed in a compact form preliminarily introducing the new condition below.

$\mathcal{C}$: There does not exist a cycle in the RG/CG graph of its Verifier Net which is associated with a firable repetitive sequence and is reachable from a node in the set F(VN).

Theorem 6.4 rev1: A language divergence-free labeled PN system $\langle N, M_0, \mathcal{L}\rangle$ is diagnosable iff condition $\mathcal{C}$ holds.

Proof: By Corollary 1, it is sufficient to prove that $\mathcal{B} \Longleftrightarrow \mathcal{C}$ for language divergence-free labeled PN systems.

• $\mathcal{B} \Longleftarrow \mathcal{C}$. In the proof of the *if* part of Theorem 6.4 [3] it was shown that **if** condition $\mathcal{C}$ holds **then** also condition $\mathcal{B}$ holds. Indeed, this implication does not even require language divergence-freeness.

• $\mathcal{B} \Longrightarrow \mathcal{C}$. The proof of the *only if* part of Theorem 6.4 [3] used the result of Proposition 6.3 [3] to show that **if** $\mathcal{B}$ holds **then** $\mathcal{C}$ holds. Proposition 4 above ensures that Proposition 6.3 [3] holds for language divergence-free nets. □

Finally, similarly to Theorem 6.4 [3], Theorem 6.7 [3] can be revised as follows.

Theorem 6.7 rev1: Let $\langle N, M_0, \mathcal{L}\rangle$ be a language divergence-free labeled Petri net system. There exists a finite K such that the system is diagnosable in K steps iff in the RG/CG of its VN no node in the set F(VN) belongs to a cycle. ■

The proof follows from the fact that, as shown in [3], Theorem 6.7 derives from Theorem 6.4.

6.2 A structural alternative assumption

We conclude this section proving that the language divergence-freeness assumption can be replaced by the following structural assumption, in order to guarantee the validity of Theorem 6.4 [3].

Assumption. *The T_u-induced subnet is acyclic.*

To this aim we first provide the following result.

Proposition 5 *If the unobservable subnet of a given labeled PN $\langle N, M_0, \mathcal{L}\rangle$ satisfies the following two assumptions:*

(i) it has no source transitions,

(ii) it is acyclic,

then $\langle N, M_0, \mathcal{L}\rangle$ is language divergence-free.

Proof: Follows from Propositition 3 in [9]. □

Thanks to the above proposition, an additional revised version of Theorem 6.4 [3] can be provided.

Theorem 6.4 rev2: A labeled PN system $\langle N, M_0, \mathcal{L}\rangle$ whose T_u-induced subnet is acyclic is diagnosable iff condition $\mathcal{C}$ holds.

Proof: This result follows from the following considerations. Under the assumption that the T_u-induced subnet is acyclic we have to consider two cases.

• Case 1: there exists no unobservable source transition. In this case thanks to Proposition 5 the net is language divergence-free and the result follows from Theorem 6.4 rev1.

• Case 2: there exists an unobservable source transition t. In such a case after a fault occurs this transitions can fire infinitely often and thus the system is not diagnosable. In addition a source transition (λ, t) will also be present on the VN which will necessarily cause in its reachability graph a cycle associated with such a firable repetitive sequence. □

Finally, Theorem 6.7 [3] can be similarly revised as follows.

Theorem 6.7 rev2: Let $\langle N, M_0, \mathcal{L}\rangle$ be a labeled Petri net system whose T_u-induced subnet is acyclic. There exists a finite K such that the system is diagnosable in K steps iff in the RG/CG of its VN no node in the set $F(\text{VN})$ belongs to a cycle. ■

Also in this case the proof follows from the fact that, as shown in [3], Theorem 6.7 derives from Theorem 6.4.

7 Conclusions

The contribution of this paper is twofold. First, we formalized two properties in the framework of labeled Petri nets, namely *language divergence* and *marking divergence*, and provided some characterizations that are fundamental for diagnosability analysis. Then, we fixed a technical problem in [3] where a diagnosability analysis approach for labeled Petri nets is proposed. Indeed, as shown in the paper via two simple examples, Theorems 6.4 and 6.7 in [3], providing necessary and sufficient conditions for diagnosability and K-diagnosability, respectively, are not correct in general. We solved this issue proving that the two theorems in [3] are correct if applied to nets that are language divergence-free. Finally, we proposed an alternative *structural* assumption — requiring the acyclicity of the unobservable subnet — and showed that it also ensures that the above two theorems hold.

Acknowledgments

We thank again B. Bérard, S. Haar, S. Schmitz, and S. Schwoon for sharing their results and insights with us. This work was inspired by them.

References

[1] B. Bérard, S. Haar, S. Schmitz, and S. Schwoon. The Complexity of Diagnosability and Opacity Verification for Petri Nets. *Fundamenta Informaticae*, 161 (4): 317–349, April 2018.

[2] M.P. Cabasino, A. Giua, S. Lafortune, and C. Seatzu. Diagnosability analysis of unbounded Petri nets. In *Proc. Joint 48th IEEE Conf. on Decision and Control and 28th Chinese Control Conf.*, pages 1267–1272, Shanghai, China, December 2009.

[3] M.P. Cabasino, A. Giua, S. Lafortune, and C. Seatzu. A new approach for diagnosability analysis of Petri nets using verifier nets. *IEEE Trans. Automatic Control*, 57(12):3104–3117, December 2012.

[4] C.A.R. Hoare. Communicating Sequential Processes. Prentice-Hall, Int. Series in Computer Science, 1985.

[5] D. König. Über eine Schlussweise aus dem Endlichen ins Unendliche. *Acta Sci. Math.*, 3(2-3):121–130, 1927.

[6] T. Murata. Petri nets: Properties, analysis and applications. *Proc. IEEE*, 77(4):541–580, 1989.

[7] X. Yin and S. Lafortune. On the decidability and complexity of diagnosability for labeled Petri nets. *IEEE Trans. Automatic Control*, 62(11):5931-5938, November 2017.

[8] X. Yin and S. Lafortune. Correction to "On the decidability and complexity of diagnosability for labeled Petri nets". *IEEE Trans. Automatic Control*, DOI: 10.1109/TAC.2019.2897511, 2019.

[9] G. Stremersch, and R.K. Boel. Structuring acyclic Petri nets for reachability analysis and control. *Discrete Event Dynamic Systems*, 12:7–41, 2002.