The Complexity of Diagnosability and Opacity Verification for Petri Nets

Béatrice Bérard[1,2], Stefan Haar[2], Sylvain Schmitz[2(✉)], and Stefan Schwoon[2]

[1] Sorbonne Universités, UPMC University Paris 06, LIP6, Paris, France
beatrice.berard@lip6.fr

[2] INRIA and LSV, CNRS and ENS Cachan, Université Paris-Saclay, Cachan, France
stefan.haar@inria.fr, {schmitz,schwoon}@lsv.fr

Abstract. *Diagnosability* and *opacity* are two well-studied problems in discrete-event systems. We revisit these two problems with respect to expressiveness and complexity issues.

We first relate different notions of diagnosability and opacity. We consider in particular fairness issues and extend the definition of Germanos et al. [ACM TECS, 2015] of weakly fair diagnosability for safe Petri nets to general Petri nets and to opacity questions.

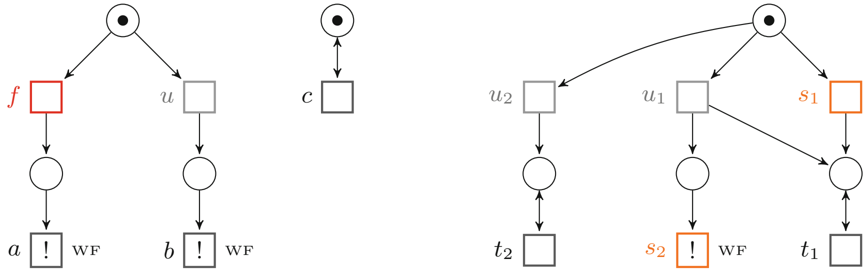
Second, we provide a global picture of complexity results for the verification of diagnosability and opacity. We show that diagnosability is NL-complete for finite state systems, PSPACE-complete for safe Petri nets (even with fairness), and EXPSPACE-complete for general Petri nets without fairness, while non diagnosability is inter-reducible with reachability when fault events are not weakly fair. Opacity is ESPACE-complete for safe Petri nets (even with fairness) and undecidable for general Petri nets already without fairness.

1 Introduction

Diagnosability and opacity are two aspects of partially observable discrete-event systems that have each received considerable attention. Although they are usually considered separately, they form a dual pair of tasks: an observer watches the current execution of a known system, where only some events are visible. As this execution evolves, the observer continually attempts to deduce whether the execution satisfies some property: in diagnosis, the observer strives to detect the occurrence of some *fault* event, while in opacity the observer may be hostile, and one requires to prevent her from being certain that a *secret* has occurred. These deductions are made on the basis of a finite prefix of the current execution; we will refer to this as the *Finite-Observation Property.*

Diagnosability. A system is *diagnosable* if, after the occurrence of a fault (which itself is invisible), it is always possible to deduce that a fault has happened after a sufficiently long observation. A formal-language framework for both diagnosis and the analysis of diagnosability was introduced by Sampath et al. [23] in the context of finite automata, for which diagnosability can be checked in polynomial time in the number of reachable states [16,27].

W. van der Aalst and E. Best (Eds.): PETRI NETS 2017, LNCS 10258, pp. 200–220, 2017.
DOI: 10.1007/978-3-319-57861-3_13



(a) Petri net that is not diagnosable but WF-disagnosable.

(b) Petri net that is opaque but not WF-opaque.

Fig. 1. Examples for diagnosis and opacity in weakly fair Petri nets.

Weak Fairness. The diagnosability framework from [23] is suitable for *sequential* but not for concurrent systems. Consider for instance the Petri net (PN) shown in Fig. 1(a), inspired by an example from [7]. It consists of two entirely independent components. We assume that an outside observer can see the actions a, b, c but not f, u, where f is a fault. If the system is eager to progress, then it is intuitively diagnosable because f will lead to the observation a, which is not possible otherwise. However, if one naively translates the Petri net into a labelled transition system (LTS) and applies the methods from [23], the net will be declared non-diagnosable because the two executions fc^ω and uc^ω are observationally equivalent. If the component on the right-hand side is removed, the system becomes diagnosable. In other words, the presence of the right-hand side component fully determines whether the system is diagnosable or not, although it is not related in any way to the faulty behaviour.

Such effects have motivated the study of diagnosability notions suitable for concurrent systems [7–11]. We focus in this paper on the *weakly fair* (WF) behaviours of the system in the sense of Vogler [26]: In a weakly fair run, no WF transition t that becomes enabled will remain idle indefinitely; either t itself eventually fires, or some conflicting transition does, thus (momentarily) disabling t. This notion of weak fairness is slightly weaker than the one studied by Jančar [14], but has the advantage that for safe Petri nets, the maximal partially ordered runs are exactly those generated by WF runs; and conversely, interleavings of such partially ordered runs yield WF firing sequences.

Under WF semantics, a fault can be diagnosed when the observations made so far can no longer be those of any fault-free WF execution. Then a net is WF-diagnosable if every infinite WF faulty execution has a prefix allowing the fault to be diagnosed. Under this characterisation, the net in Fig. 1(a) is considered WF-diagnosable. In [7,11], WF-diagnosability was shown decidable for safe PNs.

Opacity was introduced for general transition systems in [2]. The system has a secret subset of executions which is *opaque* if for any secret execution, there is a non-secret one with the same observation: an observer can never be sure whether

Table 1. Complexity results for diagnosability and opacity.

Model	Diagnosability	Opacity
Finite LTS	NL-c	PSPACE-c. [4]
Safe (WF-)PN	PSPACE-c	ESPACE-c.
PN	EXPSPACE-c	Undecidable
Strict WF-PN	PNReach $\leq_m^{\mathsf{P}}$ $\neg$Diag $\leq_m^{\mathsf{EXP}}$ PNReach	

the current execution is secret or not. State-based variants (where the observation of an execution is the associated sequence of states) were later studied for instance in [4,25] and shown in [4] to be PSPACE-complete for finite transition systems. Other language-based variants were also studied in [1,19]. Our focus here is on secret executions defined by the occurrence of some secret *transition*.

As for diagnosability, the notions of opacity developed for LTSs are not necessarily suitable for concurrent systems. Consider the net $\mathcal{W}_1$ in Fig. 1(b) and suppose that transitions s_1 and s_2 are secret, t_1 and t_2 visible for an attacker, and u_1 and u_2 invisible. Then an observation of t_2 shows that no secret has occurred, but observing occurrences of t_1 does not suffice to prove that s_1 or s_2 have occurred; therefore, according to traditional definitions, the Petri net $\mathcal{W}_1$ would be considered opaque. However, assuming that s_2 behaves in a *weakly fair* way, then, on observing t_1, the attacker can deduce with certainty that either s_1 has already fired, or s_2 will inevitably do so (or already has). We introduce a notion of *WF-opacity* that takes this into account and declares $\mathcal{W}_1$ non-opaque.

Contributions. We establish the relationships between several notions of diagnosability in the general setting of transition systems (Sect. 2). For concurrent systems, we extend in Sect. 3.3 the notion of WF-diagnosability from [7] to general Petri nets and define and study a refinement of opacity with weak fairness.

Moreover, we provide an almost complete picture of the complexity for diagnosability and opacity analysis for Petri nets with general and weakly fair semantics; see Table 1. For a start, we complete the picture for finite LTSs and show that diagnosability is complete for non-deterministic logarithmic space, while opacity had already been shown PSPACE-complete in [4]. For Petri nets, the outcome is roughly consistent with the 'rules of thumb' in Esparza's survey [5] when viewing diagnosability as a linear-time property and opacity as an inclusion problem. The salient points are as follows:

- As an auxiliary result for our lower bounds in Sect. 4, we re-discovered that trace inclusion in safe Petri nets was actually ESPACE-complete (Proposition 4.3), where ESPACE is the class of problems that can be solved in deterministic space $2^{O(n)}$. An ESPACE-complete problem is also EXPSPACE-complete—i.e., for deterministic space $2^{poly(n)}$—but the converse is not necessarily true.
- The upper bounds for safe Petri nets in Sect. 5.1 also hold for the weakly fair variants of diagnosability and opacity. Our PSPACE upper bound for

WF-diagnosability might thus come as a surprise, as this is a branching-time property (see Definition 3.3), which cannot be expressed in CTL due to its fairness aspect, while CTL* model-checking would yield an EXP upper bound. We analyse the complexity of the algorithm of Germanos et al. [7] for WF-diagnosability and give an algorithm in ESPACE for WF-opacity.

- For general Petri nets, we leave the decidability of WF-diagnosability open, but nevertheless show two positive results in Sect. 5.2 in restricted settings.

  The first one is a tight EXPSPACE upper bound for diagnosability—a considerable improvement over the original algorithm of Cabasino et al. [3], which constructed coverability graphs with worst-case Ackermann size.

  The second one is an algorithm checking for non WF-diagnosability when fault transitions are not weakly fair, i.e., when a fault is a *possible* outcome in the system but not one that is *required* to happen. We call such systems *strict*, and as illustrated in [7, Sect. 5], this is a reasonable assumption in practice. Our complexity analysis relies on a fragment of LTL studied by Jančar [14] and shares its complexity: at least as hard as reachability (noted 'PNReach' in Table 1), and at most exponentially harder; recall that the complexity of reachability in general Petri nets is a major open problem [24], with a gigantic gap between a forty years old EXPSPACE lower bound [20] and a cubic Ackermann upper bound obtained recently in [18].

Due to space constraints, several proofs are omitted, but they can be found in the full paper available from https://hal.inria.fr/hal-01484476.

2 Opacity and Diagnosability for Transition Systems

In this section, we recall and compare several notions of opacity and diagnosability for labelled transition systems (LTS), and we revisit the complexity of diagnosability for finite LTSs.

2.1 Transition Systems

Given a finite alphabet Σ, we denote by Σ^* the set of finite words over Σ, with ε the empty word, and by Σ^ω the set of infinite words over Σ. For a finite word $\sigma \in \Sigma^*$, $|\sigma|$ is its length. The (strict) *prefix ordering* is defined for two words $\sigma_1 \in \Sigma^*$ and $\sigma_2 \in \Sigma^* \cup \Sigma^\omega$ by $\sigma_1 < \sigma_2$ if there exists a non empty word σ such that $\sigma_2 = \sigma_1\sigma$; we note $\mathit{Pref}(L) \overset{\text{def}}{=} \{\hat{\sigma} \in \Sigma^* \mid \exists\sigma \in L : \hat{\sigma} \leq \sigma\}$ for the set of finite prefixes of a language $L \subseteq \Sigma^* \cup \Sigma^\omega$; this defines a tree sharing common prefixes.

Labelled Transition System. A *labelled transition system* (LTS) is a tuple $\mathcal{A} = \langle Q, q_0, \Sigma, \Delta\rangle$ where Q is a set of states with $q_0 \in Q$ the initial state, Σ is a finite alphabet, and $\Delta \subseteq Q \times \Sigma \times Q$ is the set of transitions. We note $q \xrightarrow{a} q'$ for $\langle q, a, q'\rangle \in \Delta$; this transition is then said to be *enabled* in q.

An infinite *run* over the word $\sigma = a_1a_2 \cdots \in \Sigma^\omega$ is a sequence of states $(q_i)_{i\geq 0}$ such that $q_i \xrightarrow{a_{i+1}} q_{i+1}$ for all $i \geq 0$, and we write $q_0 \overset{\sigma}{\Rightarrow}$ if such a run exists. A finite run over $\sigma \in \Sigma^*$ is defined analogously, and we write $q \overset{\sigma}{\Rightarrow} q'$ if such a run ends at state q'. A state q is *reachable* if there exists a run $q_0 \overset{\sigma}{\Rightarrow} q$ for some finite σ. An LTS $\mathcal{A}$ is *live* (aka deadlock-free) if for any reachable state there exists a transition enabled in that state.

Traces. The *finite trace language* $\mathit{Trace}^*(\mathcal{A}) \subseteq \Sigma^*$ of $\mathcal{A}$ and the *infinite trace language* $\mathit{Trace}^\omega(\mathcal{A}) \subseteq \Sigma^\omega$ of $\mathcal{A}$ are defined by:

$$\mathit{Trace}^*(\mathcal{A}) \overset{\text{def}}{=} \{\, \sigma \in \Sigma^* \mid \exists q : q_0 \overset{\sigma}{\Rightarrow} q \,\}, \qquad \mathit{Trace}^\omega(\mathcal{A}) \overset{\text{def}}{=} \{\, \sigma \in \Sigma^\omega \mid q_0 \overset{\sigma}{\Rightarrow} \,\}.$$

Note that for a live LTS $\mathcal{A}$, $\mathit{Pref}(\mathit{Trace}^\omega(\mathcal{A})) = \mathit{Trace}^*(\mathcal{A}) = \mathit{Pref}(\mathit{Trace}^*(\mathcal{A}))$. Also recall that a prefix-closed language $L = \mathit{Pref}(L)$ is *regular* if there exists a finite transition system $\mathcal{A}$ such that $L = \mathit{Trace}^*(\mathcal{A})$.

2.2 Observations

In order to formalise diagnosability and opacity, we introduce an observation mask $\mathcal{O}$. Given an LTS $\mathcal{A} = \langle Q, q_0, \Sigma, \Delta \rangle$, $\mathcal{O}$ is a mapping from Σ to $E \cup \{\varepsilon\}$, where E is a finite set of observable *events*: letters of Σ mapped to E correspond to events visible to an external observer, whereas letters mapped to ε remain invisible. We lift $\mathcal{O}$ to a homomorphism and to languages in the usual way.

When σ is an infinite trace, its observation $\mathcal{O}(\sigma)$ can be either finite or infinite; an LTS $\mathcal{A}$ is *convergent* (with respect to $\mathcal{O}$) if we forbid the former, i.e., if there is no infinite sequence of unobservable events from any reachable state. Note that it is the case in particular if $\mathcal{O}$ is *non erasing*, i.e., if $\mathcal{O}(\Sigma) \subseteq E$. Convergence and liveness are often assumed in diagnosability and opacity scenarii.

Both diagnosability and opacity fix a particular subset M of a set of executions L. Writing $\overline{M} \overset{\text{def}}{=} L \setminus M$, diagnosability requires $\mathcal{O}(M) \cap \mathcal{O}(\overline{M}) = \emptyset$, while opacity requires $\mathcal{O}(M) \subseteq \mathcal{O}(\overline{M})$. Observation sequences in $\mathcal{O}(M) \cap \mathcal{O}(\overline{M})$ are called 'ambiguous'; for opacity, all sequences in $\mathcal{O}(M)$ must be ambiguous. The negation of diagnosability can then be seen as a weak form of opacity, as defined in [19], requiring only the existence of ambiguous sequences in $\mathcal{O}(M) \cap \mathcal{O}(\overline{M})$.

2.3 Diagnosability

For diagnosability, we distinguish a special set F of *fault* letters such that $\mathcal{O}(f) = \varepsilon$ for $f \in F$. A finite (resp. infinite) sequence σ is *faulty* if it belongs to $\Sigma^* F \Sigma^*$ (resp. $\Sigma^* F \Sigma^\omega$). Otherwise σ is called *correct*. For an LTS $\mathcal{A}$, we define $\mathit{Faulty}^*(\mathcal{A}) \overset{\text{def}}{=} \mathit{Trace}^*(\mathcal{A}) \cap \Sigma^* F \Sigma^*$ for the subset of finite faulty traces and $\mathit{Faulty}^\omega(\mathcal{A}) \overset{\text{def}}{=} \mathit{Trace}^\omega(\mathcal{A}) \cap \Sigma^* F \Sigma^\omega$ for the set of infinite faulty traces. Dually, let $\mathit{Correct}^*(\mathcal{A}) \overset{\text{def}}{=} \mathit{Trace}^*(\mathcal{A}) \cap (\Sigma \setminus F)^*$ and $\mathit{Correct}^\omega(\mathcal{A}) \overset{\text{def}}{=} \mathit{Trace}^\omega(\mathcal{A}) \cap (\Sigma \setminus F)^\omega$ denote the correct traces.

We adopt the following language-based notion of diagnosability due to [21]. Although it is based on languages of infinite words, we shall see that it respects the Finite Observation Principle for all convergent LTS.

Definition 2.1 (Diagnosability [21]**).** *Given a set of faults F, an LTS $\mathcal{A}$ is* diagnosable *if*

$$\mathcal{O}(\mathit{Faulty}^{\omega}(\mathcal{A})) \cap \mathcal{O}(\mathit{Correct}^{\omega}(\mathcal{A})) = \emptyset.$$

Then $\mathcal{A}$ is *not diagnosable* if and only if there are two infinite traces σ and ρ in $\mathit{Trace}^{\omega}(\mathcal{A})$ such that σ is faulty, ρ is correct and $\mathcal{O}(\sigma) = \mathcal{O}(\rho)$. We first explain how this definition relates to other notions.

Dynamic and Finite Diagnosability. Various other notions of diagnosability were studied and discussed in [3,23]. The strongest is the notion of *K-diagnosability*: for a natural number K (that may depend on the LTS $\mathcal{A}$), it requires the faulty transition to be detected after at most K steps: for any faulty trace $\sigma f \in \mathit{Faulty}^{*}(\mathcal{A})$, and any suffix σ' with $|\sigma'| \geq K$ and $\sigma f \sigma' \in \mathit{Trace}^{*}(\mathcal{A})$, any trace $\rho \in \mathit{Trace}^{*}(\mathcal{A})$ such that $\mathcal{O}(\rho) = \mathcal{O}(\sigma f \sigma')$ is also faulty.

We use the term *dynamic diagnosability* for a less stringent notion studied in [3], which simply requires detection after a non-uniform finite number of steps $K_{\sigma f}$ that may depend on σf. Dynamic diagnosability and K-diagnosability for some K coincide if $\mathit{Trace}^{*}(\mathcal{A})$ is regular, but differ in general [3, Remark 5.5].

As we want to consider diagnosability in conjunction with fairness constraints, we shall need yet another notion of diagnosability able to take infinite runs into account while demanding that the observer diagnoses the occurrence of a fault in finite time. We say that an LTS $\mathcal{A}$ is *finitely diagnosable* if, for all $\sigma \in \mathit{Faulty}^{\omega}(\mathcal{A})$, there exists a finite prefix $\hat{\sigma} < \sigma$ such that every $\rho \in \mathit{Trace}^{\omega}(\mathcal{A})$ with $\mathcal{O}(\hat{\sigma}) < \mathcal{O}(\rho)$ is also faulty. We argue that this notion captures the Finite Observation Property. The restriction of finite diagnosability to weakly fair runs (recalled later in Definition 3.3) is exactly the definition used in [7].

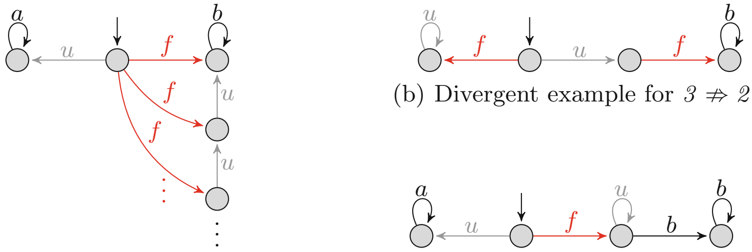
The next proposition establishes the links between these various notions in the absence of fairness constraints (and includes the result mentioned above for completeness); its proof in the full paper relies mainly on Kőnig's Lemma.

Lemma 2.2 (Comparison of Diagnosability Notions). *Let $\mathcal{A}$ be an LTS. Then we have the implications 1 $\Rightarrow$ 2 $\Rightarrow$ 3 $\Rightarrow$ 4 where:*

1. *$\mathcal{A}$ is K-diagnosable for some $K \in \mathbb{N}$;*
2. *$\mathcal{A}$ is dynamically diagnosable;*
3. *$\mathcal{A}$ is finitely diagnosable;*
4. *$\mathcal{A}$ is diagnosable.*

Moreover, 1 and 2 are equivalent if $\mathit{Trace}^{*}(\mathcal{A})$ is regular [3, Proposition 5.3]*, 2 and 3 are equivalent if $\mathcal{A}$ is finitely branching and convergent, and 3 and 4 are equivalent if $\mathcal{A}$ is convergent.*

Remark 2.3 (Counter-examples). Fig. 2(a) and (b) show that $\mathcal{A}$ must be both finitely branching and convergent for the equivalence 3 $\Leftrightarrow$ 2 to hold in Lemma 2.2. The system in Fig. 2(a) is diagnosable since $\mathcal{O}(ua^{\omega}) \neq \mathcal{O}(fu^{n}b^{\omega})$ for all n, and as it is convergent it is also finitely diagnosable, but it is not dynamically diagnosable because the faulty prefix f may require an arbitrarily long finite delay



(a) Infinitely branching example for *3* $\not\Rightarrow$ *2*.

(b) Divergent example for *3* $\not\Rightarrow$ *2*.

(c) Divergent example for *4* $\not\Rightarrow$ *3*.

Fig. 2. Counter-examples for Lemma 2.2, with $\mathcal{O}(u) = \mathcal{O}(f) = \varepsilon$, $\mathcal{O}(a) = a$, and $\mathcal{O}(b) = b$.

K before being diagnosed by $u^K b$. In contrast, the system in Fig. 2(b) is finitely branching but divergent; it is finitely diagnosable for the trivial reason that there is no infinite correct run. (We remark that there exist other examples without this particular property.) The system is not dynamically diagnosable because for the prefix f we have $\mathcal{O}(fu^K) = \mathcal{O}(u)$ for all K.

Figure 2(c) shows that $\mathcal{A}$ must be convergent for the equivalence 4 $\Leftrightarrow$ 3 to hold in Lemma 2.2. The system is diagnosable, as $\mathcal{O}(fe^\omega) \neq \mathcal{O}(ua^\omega) \neq \mathcal{O}(fe^n b^\omega)$ for all n, but is not finitely diagnosable because all the finite prefixes of the faulty fe^ω have the same observation $\varepsilon < \mathcal{O}(ua^\omega)$.

Complexity of Diagnosability for Finite LTSs. In the case of finite-state LTSs, and assuming an explicit representation with $|\mathcal{A}| \overset{\text{def}}{=} |\Delta| + |Q| + |\Sigma|$, it is easy to show that checking diagnosability takes quadratic time w.r.t. $|\mathcal{A}|$ [16,27]. This instantiates the classical squaring construction for ambiguity detection [6]. In fact, the same argument serves to show a tight complexity-theoretic upper bound (see the full paper for details). Note that under the conditions named in the following proposition all four diagnosability notions coincide.

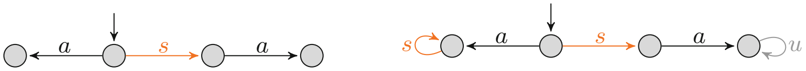
Proposition 2.4. *Verifying diagnosability for finite-state, live and convergent LTSs is* NL*-complete.*

2.4 Opacity

The classical notion of opacity, as defined in [2], deals with finite traces only. For our purpose, we distinguish a subset S of Σ containing special *secret* letters such that $\mathcal{O}(s) = \varepsilon$ for all $s \in S$. We consider as secret any sequence containing some $s \in S$, hence the set of finite secrets in an LTS $\mathcal{A}$ is $\mathit{Sec}^*(\mathcal{A}) \overset{\text{def}}{=} \mathit{Trace}^*(\mathcal{A}) \cap \Sigma^* S \Sigma^*$, while the set of infinite secrets is $\mathit{Sec}^\omega(\mathcal{A}) \overset{\text{def}}{=} \mathit{Trace}^\omega(\mathcal{A}) \cap \Sigma^* S \Sigma^\omega$; dually, the set of finite non-secret traces is $\mathit{Pub}^*(\mathcal{A}) \overset{\text{def}}{=} \mathit{Trace}^*(\mathcal{A}) \cap (\Sigma \setminus S)^*$ and the set of infinite non-secret ones is $\mathit{Pub}^\omega(\mathcal{A}) \overset{\text{def}}{=} \mathit{Trace}^\omega(\mathcal{A}) \cap (\Sigma \setminus S)^\omega$.

Definition 2.5 (Opacity [2]). *The secret S in an LTS $\mathcal{A}$ is* opaque *if*

$$\mathcal{O}(\mathit{Sec}^*(\mathcal{A})) \subseteq \mathcal{O}(\mathit{Pub}^*(\mathcal{A})).$$



(a) Convergent non live example. (b) Divergent live example.

Fig. 3. Counter-examples for Lemma 2.6, with $\mathcal{O}(u) = \mathcal{O}(s) = \varepsilon$ and $\mathcal{O}(a) = a$.

The problem of checking opacity was proven PSPACE-complete for finite LTSs [4] for a state-based variant, and this is easily seen to hold for Definition 2.5 as well.

Finite Opacity. As with diagnosability, we shall need a notion of opacity able to consider infinite runs, which we will then refine in Definition 3.5 for weakly fair opacity: we say that the secret in a LTS $\mathcal{A}$ is *finitely opaque* if, for all $\hat{\sigma} \in \mathit{Sec}^*(\mathcal{A})$, there exists an infinite non-secret trace $\rho \in \mathit{Pub}^\omega(\mathcal{A})$ such that $\mathcal{O}(\hat{\sigma}) \leq \mathcal{O}(\rho)$. By Kőnig's Lemma and arguments similar to those used for Lemma 2.2, we show that this notion coincides with opacity on live convergent LTSs in the full paper.

Lemma 2.6 (Comparison of Opacity Notions). *Let $\mathcal{A}$ be a live convergent LTS. Then the secret in $\mathcal{A}$ is opaque if and only if it is finitely opaque.*

Remark 2.7 (Counter-examples). Figure 3 shows that $\mathcal{A}$ must be live and convergent for the equivalence between opacity and finite opacity to hold in Lemma 2.6. In both Fig. 3(a) and (b) the system is opaque since $\mathcal{O}(\mathit{Sec}^*(\mathcal{A})) = \{\varepsilon, a\} = \mathcal{O}(\mathit{Pub}^*(\mathcal{A}))$, but is not finitely opaque because there exists a finite secret trace $s \in \mathit{Sec}^*(\mathcal{A})$ but there does not exist any infinite non-secret trace: $\mathit{Pub}^\omega(\mathcal{A}) = \emptyset$.

3 Opacity and Diagnosability for Petri Nets

After some reminders on Petri nets, we devote this section to the definitions of weakly fair Petri nets in Sect. 3.2 and of suitable variants of diagnosability and opacity in Sect. 3.3. We finally consider the case of weakly fair diagnosability when no faults are fair in Sect. 3.4.

3.1 Petri Nets

Syntax. A *Petri Net* (PN) is a tuple $\mathcal{N} = \langle P, T, w, \boldsymbol{m}_0 \rangle$ where P and T are finite sets of *places* and *transitions* respectively, $w\colon (P \times T) \cup (T \times P) \to \mathbb{N}$ is the *flow mapping*, and $\boldsymbol{m}_0 \in \mathbb{N}^P$ is the *initial marking*.

A *marking* is a mapping $\boldsymbol{m} \in \mathbb{N}^P$. As usual, in figures, transitions are represented as rectangles and places as circles. If $\boldsymbol{m}(p) \geq 1$, the corresponding number of black tokens are drawn in p. For a transition t, we denote its *preset* by ${}^\bullet t \overset{\text{def}}{=} \{p \in P \mid w(p,t) > 0\}$ and its *postset* by $t^\bullet \overset{\text{def}}{=} \{p \in P \mid w(t,p) > 0\}$.

Semantics. The operational semantics of a PN $\mathcal{N} = \langle P, T, w, \boldsymbol{m}_0 \rangle$ is an LTS $\mathcal{A}_\mathcal{N} = \langle \mathbb{N}^P, \boldsymbol{m}_0, T, \Delta \rangle$, whose states are the markings of $\mathcal{N}$, and whose transitions are labelled by T, where $\langle \boldsymbol{m}, t, \boldsymbol{m}' \rangle \in \Delta$ if and only if for each $p \in P$ we have $\boldsymbol{m}(p) \geq w(p,t)$, and $\boldsymbol{m}'(p) = \boldsymbol{m}(p) - w(p,t) + w(t,p)$ for all $p \in P$. Note that $\mathcal{A}_\mathcal{N}$ is 'deterministic' as no two different runs produce the same trace.

Note that adding an observation mask to a Petri net $\mathcal{N}$ results in what is usually called a 'labelled Petri net'. Then diagnosability with respect to a subset $F \subseteq T$ of fault transitions corresponds to diagnosability of the transition system $\mathcal{A}_\mathcal{N}$. As mentioned in the introduction, this notion declares the net from Fig. 1(a) to be non-diagnosable. Similarly, a Petri net $\mathcal{N}$ is opaque in the sense of Definition 2.5 with respect to a subset $S \subseteq T$ of secret transitions if $\mathcal{A}_\mathcal{N}$ is opaque. We shall abuse notations and write '$\mathit{Trace}^*(\mathcal{N})$' (resp. '$\mathit{Trace}^\omega(\mathcal{N})$', etc.) instead of '$\mathit{Trace}^*(\mathcal{A}_\mathcal{N})$' (resp. '$\mathit{Trace}^\omega(\mathcal{A}_\mathcal{N})$', etc.).

Safe Petri Nets. A Petri net $\mathcal{N}$ is *safe* if the reachable states form a subset of $\{0,1\}^P$; as a result $\mathcal{A}_\mathcal{N}$ is finite, and $\mathit{Trace}^*(\mathcal{N})$ is regular. Note however that safe Petri nets are *implicit* descriptions of $\mathcal{A}_\mathcal{N}$: the latter can be of (at most) exponential size in terms of $|\mathcal{N}|$. This immediately entails that, in safe Petri nets, diagnosis is in PSPACE by Proposition 2.4 and opacity in EXPSPACE by [4]; we shall generalise and refine these upper bounds in Sect. 5 to take weak fairness into account.

3.2 Weak Fairness

We shall employ the following generalisation of weak fairness as defined in [7,11]:

Definition 3.1 (Weak Fairness). *A* Petri net with weak fairness *(WF-PN) is a tuple $\mathcal{W} = \langle \mathcal{N}, W \rangle$, where $\mathcal{N}$ is a Petri net and $W \subseteq T$ a set of transitions called* weakly fair.

Let $\sigma = (t_i)_{i \geq 1} \in T^\omega$ be an infinite trace, and $(\boldsymbol{m}_i)_{i \geq 0}$ the (uniquely determined) infinite run of $\mathcal{A}_\mathcal{N}$ over σ. Then σ is weakly fair *if for every $t \in W$,*

WF.1 *there are infinitely many i with $t_i = t$,* ***or***
WF.2 *there are infinitely many i where t_i* conflicts with t with respect to $\boldsymbol{m}_{i-1}$*, i.e. there exists $p \in P$ s.t. $\boldsymbol{m}_{i-1}(p) < w(p, t_i) + w(p,t)$.*

Note that (WF.2) also covers the case where t is simply disabled. Informally, in a weakly fair sequence σ, each weakly fair transition t that is enabled either fires eventually, or some other transition that competes for a preset place with t fires. As shown by Jančar [14], it is decidable whether a WF-PN has at least one weakly fair trace.[1]

In drawings, we shall denote weakly fair transitions by the annotation 'WF' and a bang. For instance, in the net from Fig. 1(b), s_2 is a weakly fair transition,

[1] In Jančar's definition, (WF.2) uses the simpler condition $\boldsymbol{m}_{i-1}(p) < w(p,t)$. We could easily adapt our treatment of weak fairness to work with that definition, but we preferred to remain compatible with [7,11].

and $u_1 t_1^\omega$ is not weakly fair since s_2 is continuously enabled and never fires. (In this case, no other transition conflicts with s_2.) We shall use '*WF*' subscripts to denote the restriction of a set of infinite traces to weakly fair ones, as in '$\mathit{Trace}_{WF}^\omega(\mathcal{N})$' or '$\mathit{Faulty}_{WF}^\omega(\mathcal{N})$'.

When $\mathcal{N}$ is safe, Definition 3.1 coincides with the definition employed in [7,11,26]; see the full paper for details.

Proposition 3.2 (Weak Fairness in Safe PNs). *Let $\mathcal{W} = \langle \mathcal{N}, W \rangle$ be a safe WF-PN. An infinite trace $\sigma = (t_i)_{i \geq 1}$ with run $(\boldsymbol{m}_i)_{i \geq 0}$ is* weakly fair *if and only if, for every $i > 0$ and every $t \in W$ enabled in $\boldsymbol{m}_{i-1}$, there exists some $j \geq i$ such that ${}^\bullet t \cap {}^\bullet t_j \neq \emptyset$.*

3.3 Diagnosability and Opacity with Weak Fairness

In the context of Petri nets with weak fairness, the definitions of both notions must take into account the set of weakly fair transitions while maintaining the Finite Observation Property.

Weakly Fair Diagnosability. We restrict finite diagnosability to the set of weakly fair runs, as is done in [7], but with a generalised notion of weak fairness.

Definition 3.3 (Weakly Fair Diagnosability). *A WF-PN $\mathcal{W} = \langle \mathcal{N}, W \rangle$ is said to be* WF-diagnosable *if every infinite, weakly fair, faulty trace $\sigma \in \mathit{Faulty}_{WF}^\omega(\mathcal{N})$ has a finite prefix $\hat{\sigma}$ such that every infinite weakly fair trace $\rho \in \mathit{Trace}_{WF}^\omega(\mathcal{N})$ satisfying $\mathcal{O}(\hat{\sigma}) < \mathcal{O}(\rho)$ is faulty.*

Consider again the net from Fig. 1(a) and assume that transition a is WF. Then this net is WF-diagnosable since a weakly fair trace that contains f also eventually contains a, and a is only possible after f. Note that, as shown in [7], this definition is not equivalent to simply restricting diagnosability according to Definition 2.1 to weakly fair traces. The precise relation of WF-diagnosability with other notions was not examined in [7]; however, by Lemma 2.2, we obtain:

Lemma 3.4. *Let $\mathcal{W} = \langle \mathcal{N}, W \rangle$ be a convergent WF-PN such that $W = \emptyset$. Then $\mathcal{W}$ is WF-diagnosable if and only if $\mathcal{N}$ is diagnosable.*

Weakly Fair Opacity. We now turn to opacity and provide a definition of weakly fair opacity that also respects the Finite Observation Property, again by restricting finite opacity to weakly fair runs. Informally, Definition 3.5 means that any finite observation prefix can be extended in a way compatible with a weakly fair non-secret run, hence making the occurrence of a secret uncertain for the observer.

Definition 3.5 (Weakly Fair Opacity). *The secret in a WF-PN $\mathcal{W} = \langle \mathcal{N}, W \rangle$ is said to be* WF-opaque *if, for any trace $\hat{\sigma}$ in $\mathit{Sec}^*(\mathcal{N})$, there exists an infinite, weakly fair, non-secret trace $\rho \in \mathit{Pub}_{WF}^\omega(\mathcal{N})$ such that $\mathcal{O}(\hat{\sigma}) \leq \mathcal{O}(\rho)$.*

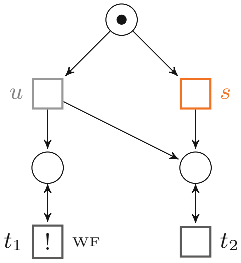


Fig. 4. WF-PN $\mathcal{W}_2$ with t_1 weakly fair, s secret and u unobservable.

Example 3.6. The WF-PN $\mathcal{W}_1 = \langle \mathcal{N}_1, \{s_2\} \rangle$ depicted in Fig. 1(b) shows that weakly fair opacity is more discriminating that standard opacity. We consider the observation mask $\mathcal{O}$ defined by $\mathcal{O}(u_1) = \mathcal{O}(u_2) = \mathcal{O}(s_1) = \mathcal{O}(s_2) = \varepsilon$, for two secret transitions s_1 and s_2, $\mathcal{O}(t_1) = a$ and $\mathcal{O}(t_2) = b$.

The net $\mathcal{N}_1$ is opaque according to Definition 2.5 because the finite secret is observed as $\mathcal{O}(\mathit{Sec}^*(\mathcal{N}_1)) = a^*$, while the non-secret executions are observed as $a^* \cup b^*$, and the former is a subset of the latter.

On the other hand, the secret is not WF-opaque in $\mathcal{W}_1$ according to Definition 3.5. Let $\hat{\sigma} = s_1 t_1 \in \mathit{Sec}^*(\mathcal{N}_1)$. Then $\mathcal{O}(\hat{\sigma}) = a$, and the set of infinite, weakly fair traces ρ such that $\mathcal{O}(\hat{\sigma}) < \mathcal{O}(\rho)$ is $s_1 t_1^\omega \cup u_1 t_1^* s_2 t_1^\omega$, and all of these executions contain a secret transition.

As with Lemma 3.4, we obtain from Lemma 2.6 that WF-opacity and opacity coincide when no transition is weakly fair, thus Definition 3.5 is a proper generalisation of Definition 2.5.

Lemma 3.7. *Let $\mathcal{W} = \langle \mathcal{N}, W \rangle$ be a live convergent WF-PN such that $W = \emptyset$. Then the secret is WF-opaque in $\mathcal{W}$ if and only if it is opaque in $\mathcal{W}$.*

Comparing Definitions 2.5 and 3.5, we see that the formulation of WF-opacity is considerably more complex than the simple inclusion required by standard opacity. It is tempting to 'simplify' Definition 3.5 by mimicking Definition 2.5, but restricting to weakly fair executions, i.e., to demand that $\mathcal{O}(\mathit{Sec}^\omega_{WF}(\mathcal{N})) \subseteq \mathcal{O}(\mathit{Pub}^\omega_{WF}(\mathcal{N}))$. However such a definition would not respect the Finite Observation Property.

Example 3.8. For the WF-PN $\mathcal{W}_2 = \langle \mathcal{N}_2, \{t_1\} \rangle$ depicted in Fig. 4, we consider the observation mask $\mathcal{O}$ defined by $\mathcal{O}(u) = \mathcal{O}(s) = \varepsilon$, $\mathcal{O}(t_1) = a$ and $\mathcal{O}(t_2) = b$.

In $\mathcal{W}_2$, the system can either fire the secret transition s and then infinitely often t_2, or it can fire u and then arbitrarily often a and b, where the weak fairness condition requires to fire a infinitely often. Thus, $\mathcal{O}(\mathit{Sec}^\omega_{WF}(\mathcal{N}_2)) = b^\omega$, and $\mathcal{O}(\mathit{Pub}^\omega_{WF}(\mathcal{N}_2)) = (b^* a)^\omega$; since the first set is not included in the second, a definition based on the above inclusion would declare $\mathcal{W}_2$ non-opaque. However, even when s is fired, no *finite* observation is sufficient to determine that this was the case; indeed an observation b^n, for any $n \geq 0$, could also be the consequence of firing u first. Definition 3.5 captures this fact: for any $\hat{\sigma} = st_2^n \in \mathit{Sec}^*(\mathcal{N}_2)$ there exists an infinite WF trace without secret, e.g. $\rho = ut_2^n t_1^\omega$ satisfying $\mathcal{O}(\hat{\sigma}) < \mathcal{O}(\rho)$, thus $\mathcal{W}_2$ is WF-opaque.

3.4 No Weakly Fair Faults: The Strict Case

We finally investigate the special case where fault transitions are not weakly fair, i.e., a fault is a *possible* outcome in the system but not one that is *required* to happen: we call *strict WF-PN* a WF-PN $\mathcal{W} = \langle \mathcal{N}, W \rangle$ where $W \cap F = \emptyset$. Under this assumption, weakly fair diagnosability has a simple characterisation, reminiscent of Definition 2.1, which generalises [7, Lemma 3.4 and 3.5] to general Petri nets. Note that this also provides an alternative proof of Lemma 3.4.

Lemma 3.9. *Let $\mathcal{W} = \langle \mathcal{N}, W \rangle$ be a strict convergent WF-PN. Then $\mathcal{W}$ is WF-diagnosable if and only if $\mathcal{O}(\mathit{Faulty}_{WF}^\omega(\mathcal{N})) \cap \mathcal{O}(\mathit{Correct}^\omega(\mathcal{N})) = \emptyset$.*

Proof. For the 'only if' part, assume there exists $\sigma \in \mathit{Faulty}_{WF}^\omega(\mathcal{N})$ and $\rho \in \mathit{Correct}^\omega(\mathcal{N})$ such that $\mathcal{O}(\sigma) = \mathcal{O}(\rho)$. If ρ is weakly fair, then $\mathcal{W}$ is not WF-diagnosable. Otherwise, consider some prefix $\hat{\sigma} < \sigma$ and let us build a suitable $\rho_{\hat{\sigma}} \in \mathit{Correct}_{WF}^\omega(\mathcal{N})$. Let $j \in \mathbb{N}$ be an index such that $\mathcal{O}(\hat{\sigma}) \leq \mathcal{O}(\hat{\rho})$ for the prefix $\hat{\rho}$ of length j of ρ.

Since ρ is not weakly fair, it must violate (WF.2) for some $t \in W$: writing $\boldsymbol{m}_0 \xRightarrow{t_1} \boldsymbol{m}_1 \xRightarrow{t_2} \cdots$ for its underlying run, this means that there are infinitely many indices i such that $\boldsymbol{m}_i(p) \geq w(p, t_{i+1}) + w(p,t)$ for all $p \in P$. Thus for infinitely many i, $\boldsymbol{m}_i(p) - w(p,t) + w(t,p) \geq w(p, t_{i+1})$ for all $p \in P$. Since $t \notin F$, this means that we can insert a transition by t in all those indices $i > j$ and still obtain a trace in $\mathit{Correct}^\omega(\mathcal{N})$; however this trace now satisfies (WF.1) for t. Applying this to all the $t \in W$ for which ρ was not weakly fair yields a weakly fair trace $\rho_{\hat{\sigma}} \in \mathit{Correct}_{WF}^\omega(\mathcal{N})$. Furthermore, since we inserted those occurrences of t (which might be observable) after the index j, $\mathcal{O}(\hat{\sigma}) \leq \mathcal{O}(\hat{\rho}) < \mathcal{O}(\rho_{\hat{\sigma}})$. Hence $\mathcal{W}$ is not WF-diagnosable.

Conversely, for the 'if' part, assume that $\mathcal{W}$ is not WF-diagnosable: there exists $\sigma \in \mathit{Faulty}_{WF}^\omega(\mathcal{N})$ such that for every prefix $\hat{\sigma} < \sigma$, there exists $\rho_{\hat{\sigma}} \in \mathit{Correct}_{WF}^\omega(\mathcal{N})$ with $\mathcal{O}(\hat{\sigma}) < \mathcal{O}(\rho_{\hat{\sigma}})$. Define the tree

$$\mathcal{T} \overset{\text{def}}{=} \mathit{Pref}(\{\hat{\rho} \mid \exists \hat{\sigma} < \sigma, \mathcal{O}(\hat{\rho}) = \mathcal{O}(\hat{\sigma}) \text{ and } \hat{\rho} < \rho_{\hat{\sigma}}\}). \tag{1}$$

Since Σ is finite, $\mathcal{T}$ has finite degree. Since $\mathcal{N}$ is assumed to be convergent, $\{\mathcal{O}(\hat{\sigma}) \mid \hat{\sigma} < \sigma\}$ is infinite, and therefore $\mathcal{T}$ is infinite as well. By Kőnig's Lemma, it has an infinite branch $\rho \in \Sigma^\omega$ such that every finite prefix $\hat{\rho} < \rho$ satisfies

- $\hat{\rho} < \rho_{\hat{\sigma}}$ thus $\hat{\rho} \in \mathit{Correct}^*(\mathcal{N})$ and therefore $\rho \in \mathit{Correct}^\omega(\mathcal{N})$, and
- $\mathcal{O}(\hat{\rho}) \leq \mathcal{O}(\hat{\sigma}) < \mathcal{O}(\sigma)$ and therefore $\mathcal{O}(\sigma) = \mathcal{O}(\rho)$.

Thus $\mathcal{W}$ satisfies $\mathcal{O}(\mathit{Faulty}_{WF}^\omega(\mathcal{N})) \cap \mathcal{O}(\mathit{Correct}^\omega(\mathcal{N})) \neq \emptyset$. □

4 Lower Bounds

In this section, we give reductions that yield lower bounds for the problems of diagnosability and opacity. Notice that we first study the problem variants *without* weak fairness. Thanks to Lemmas 3.4 and 3.7, these lower bounds also apply to the WF variants of both problems: checking diagnosability/opacity for the special case of a WF-PN $\langle \mathcal{N}, \emptyset \rangle$ is equivalent to checking WF-diagnosability/WF-opacity for a PN $\mathcal{N}$. For the hardness of WF-diagnosability, we show a reduction from the reachability problem for PNs.

Live and Convergent Nets. As we saw in Lemmas 2.2 and 2.6, in the absence of weak fairness constraints, (most of) the various definitions of diagnosability and opacity turn out to be equivalent when the transition systems under consideration are finitely branching, live, and convergent. As we wish our results to have the widest possible applicability, we shall require these properties of all the systems we study in lower bound proofs—but not necessarily in upper bound proofs. Because Petri nets yield finitely branching LTSs, we only need our nets to be live and convergent.

Remark 4.1. A Petri net can always be made live by adding an observable 'clock tick' transition connected back-and-forth to a single, initially marked place (like the transition c in Fig. 1(a)). Intuitively, such a transition can be understood as modelling the passage of time marked by an observer when nothing else happens in the system. Importantly, the addition of a 'clock tick' transition does not change the properties of diagnosability and opacity in our constructions.

4.1 Diagnosability

For diagnosability, we reduce from the *coverability problem*: Given a PN $\mathcal{N}$ and a place p, is there a reachable marking $\boldsymbol{m}$ such that $\boldsymbol{m}(p) \geq 1$?

Proposition 4.2 (Hardness of Diagnosability). *Diagnosability is* PSPACE-*hard for safe Petri nets and* EXPSPACE-*hard in general, already for live convergent nets.*

Proof. We exhibit a polynomial time reduction from the coverability problem to non diagnosability. The coverability problem is known to be PSPACE-complete for safe Petri nets [17] and EXPSPACE-hard in general [20]. The statement follows because these two complexity classes are closed under complement.

Let $\mathcal{N} = \langle P, T, w, \boldsymbol{m}_0 \rangle$ be a PN and let $p \in P$. We construct a live and convergent PN $\mathcal{N}'$ and an observation $\mathcal{O}$ such that a marking $\boldsymbol{m}$ with $\boldsymbol{m}(p) \geq 1$ can be reached in $\mathcal{N}$ if and only if $\mathcal{N}'$ is not diagnosable; furthermore $\mathcal{N}'$ is safe whenever $\mathcal{N}$ is safe.

The construction consists in adding to $\mathcal{N}$ a single new place $q \notin P$, initially marked, and a single unobservable faulty transition $f \notin T$ taking one token from p and q to fire and putting the token back into p afterwards (see left part

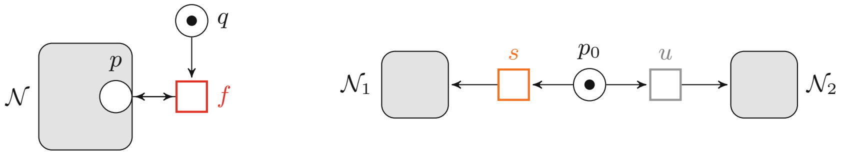


Fig. 5. Constructions for the nets $\mathcal{N}'$ in Proposition 4.2 (left) and Proposition 4.4 (right).

of Fig. 5). Thus $\mathcal{N}' \overset{\text{def}}{=} \langle P', T', w', \boldsymbol{m}_0 \rangle$ with $P' \overset{\text{def}}{=} P \cup \{q\}$, $T' \overset{\text{def}}{=} T \cup \{f\}$ and w' coincides with w on $P \times T \cup T \times P$, with $w'(q, f) = w'(p, f) = w'(f, p) = 1$ in addition. For the observation mask $\mathcal{O}$, we let $E \overset{\text{def}}{=} T$ and all transitions from T are observable with $\mathcal{O}(t) \overset{\text{def}}{=} t$ and $\mathcal{O}(f) \overset{\text{def}}{=} \varepsilon$. The faulty transition f can fire once in $\mathcal{N}'$ if and only if there is a reachable marking $\boldsymbol{m}$ in $\mathcal{N}$ with $\boldsymbol{m}(p) \geq 1$. In this case, all the infinite runs in $\mathcal{N}'$ reaching $\boldsymbol{m}$ have ambiguous observations.

The construction ensures that if $\mathcal{N}$ is safe then it is also the case for $\mathcal{N}'$. Since f can fire only once and no transition from $\mathcal{N}$ is erased, $\mathcal{N}'$ is convergent. It is not necessarily live since $\mathcal{N}$ may contain a deadlock; however, $\mathcal{N}'$ can be made live by adding a 'clock tick' transition (cf. Remark 4.1) without affecting the validity of the reduction. □

4.2 Opacity

For the opacity problem, we prove our hardness results by reducing from the *trace inclusion problem* for Petri nets: Given two PNs $\mathcal{N}_1$ and $\mathcal{N}_2$ with associated observation masks $\mathcal{O}_1$ and $\mathcal{O}_2$ into the same E, is $\mathcal{O}_1(\mathit{Trace}^*(\mathcal{N}_1)) \subseteq \mathcal{O}_2(\mathit{Trace}^*(\mathcal{N}_2))$? This problem is well-known to be undecidable for general Petri nets and EXPSPACE-complete for safe Petri nets [5].

However, because we insist on our systems being convergent, some additional care is required: in our main reduction (c.f. Proposition 4.4), we need the two PNs $\mathcal{N}_1$ and $\mathcal{N}_2$ to be convergent, hence we need to show that the trace inclusion problem remains hard even for convergent instances. Along the way, we re-discovered that its complexity in the safe case can be refined and shown to be ESPACE-complete (see Proposition 4.3), based on a reduction from the universality problem for shuffle expressions (SE) studied by Mayer and Stockmeyer [22].

Shuffle Expressions. Recall that the *shuffle* of two words σ and ρ in E^* is the language $\sigma \sqcup\!\sqcup \rho \overset{\text{def}}{=} \{\sigma_1 \rho_1 \sigma_2 \rho_2 \cdots \sigma_n \rho_n \mid n \in \mathbb{N}, \sigma_1 \cdots \sigma_n = \sigma, \rho_1 \cdots \rho_n = \rho\}$ (σ_i and ρ_i are words in E^*); this is lifted to $L \sqcup\!\sqcup M \overset{\text{def}}{=} \bigcup_{\sigma \in L, \rho \in M} \sigma \sqcup\!\sqcup \rho$ for two languages L and M.

Shuffle expressions in SE are built according to the abstract syntax

$$e := \varepsilon \mid a \mid e + e \mid e \cdot e \mid e \sqcup\!\sqcup e \mid e^*,$$

where a ranges over some alphabet E. The language of an expression in SE is defined inductively by $L(\varepsilon) \overset{\text{def}}{=} \{\varepsilon\}$, $L(a) \overset{\text{def}}{=} \{a\}$ for all $a \in E$, $L(e_1 + e_2) \overset{\text{def}}{=}$

$L(e_1) \cup L(e_2)$, $L(e_1 \cdot e_2) \overset{\text{def}}{=} L(e_1) \cdot L(e_2)$, $L(e_1 \sqcup\!\sqcup\, e_2) \overset{\text{def}}{=} L(e_1) \sqcup\!\sqcup\, L(e_2)$, and $L(e^*) \overset{\text{def}}{=} L(e)^*$, where e_1 and e_2 are two expressions.

The *universality problem* for shuffle expressions asks, given e a shuffle expression over E, whether $E^* \subseteq L(e)$. This problem is ESPACE-complete since its complement is ESPACE-complete [22, Theorem 7.1, where it is called NEC] and since ESPACE is closed under complement.

We provide in the full paper an inductive construction of a safe PN $\mathcal{N}(e)$ with coverability language $L(e)$ for e in SE. This is basically Thompson's inductive construction of a finite-state automaton from a regular expression with an extra case for shuffles, but some additional care is required in order to ensure that $\mathcal{N}(e)$ is convergent. One last pitfall is that we work with trace languages instead of coverability languages; this is handled using an additional endmarker symbol.

Proposition 4.3. *The trace inclusion problem is* ESPACE*-complete for safe convergent Petri nets.*

Reduction from the Trace Inclusion Problem. We wrap-up our lower bound proof using a reduction from the trace inclusion problem in convergent nets to the opacity problem.

Proposition 4.4 (Hardness of Opacity). *Opacity is* ESPACE*-hard for safe Petri nets, and undecidable in general, already for live convergent nets.*

Proof. We exhibit a polynomial time reduction from the trace inclusion problem for convergent PNs to the opacity problem, which preserves safety. As seen in Proposition 4.3, the trace inclusion problem is ESPACE-hard for safe convergent Petri nets. In the general case, it is undecidable by the generic proof of Jančar [15] for equivalence and preorder problems in Petri nets: given a 2-counter machine, his proof builds two Petri nets $\mathcal{N}_1$ and $\mathcal{N}_2$ with non erasing observation functions $\mathcal{O}_1$ and $\mathcal{O}_2$—thus those nets are convergent—, such that the machine halts if and only if $\mathcal{O}_1(\mathit{Trace}^*(\mathcal{N}_1)) \neq \mathcal{O}_2(\mathit{Trace}^*(\mathcal{N}_2))$.

For the reduction, let $\mathcal{N}_1 = \langle P_1, T_1, w_1, \boldsymbol{m}_{0,1}\rangle$ and $\mathcal{N}_2 = \langle P_2, T_2, w_2, \boldsymbol{m}_{0,2}\rangle$ be two convergent PNs, with observation masks $\mathcal{O}_1$ and $\mathcal{O}_2$ into the same alphabet E; without loss of generality they have disjoint sets of places and transitions.

We first build a convergent PN $\mathcal{N}'$ by adding a new place $p_0 \notin P_1 \cup P_2$, initially marked, and two new transitions s and u not in $T_1 \cup T_2$. The observation mask $\mathcal{O}'$ of $\mathcal{N}'$ extends $\mathcal{O}_1$ and $\mathcal{O}_2$ by $\mathcal{O}'(s) = \mathcal{O}'(u) = \varepsilon$. The construction (see right part of Fig. 5) consists in linking p_0 to $\mathcal{N}_1$ and $\mathcal{N}_2$ through the transitions s and u respectively, making them produce the initial markings of $\mathcal{N}_1$ and $\mathcal{N}_2$. The convergence of $\mathcal{N}'$ results from that of $\mathcal{N}_1$ and $\mathcal{N}_2$. The construction ensures that if $\mathcal{N}_1$ and $\mathcal{N}_2$ are safe, so is $\mathcal{N}'$. Now the set of secret words in $\mathcal{N}'$ is observed as $\mathcal{O}_1(\mathit{Trace}^*(\mathcal{N}_1))$ while the set of non-secret words is observed as $\mathcal{O}_2(\mathit{Trace}^*(\mathcal{N}_2))$. Thus, the secret is opaque in $\mathcal{N}'$ if and only if the inclusion $\mathcal{O}_1(\mathit{Trace}^*(\mathcal{N}_1)) \subseteq \mathcal{O}_2(\mathit{Trace}^*(\mathcal{N}_2))$ holds.

Finally, adding a 'clock tick' as in Remark 4.1 to $\mathcal{N}'$ with a fresh observation $\flat \notin E$ yields the desired $\mathcal{N}$ and $\mathcal{O}$. Indeed, $\mathcal{O}(\mathit{Sec}^*(\mathcal{N})) = \mathcal{O}'(\mathit{Sec}^*(\mathcal{N}')) \sqcup\!\sqcup\, \{\flat^n \mid n \in \mathbb{N}\}$ and $\mathcal{O}(\mathit{Pub}^*(\mathcal{N})) = \mathcal{O}'(\mathit{Pub}^*(\mathcal{N}')) \sqcup\!\sqcup\, \{\flat^n \mid n \in \mathbb{N}\}$, and inclusion holds between these two languages if and only if $\mathcal{O}'(\mathit{Sec}^*(\mathcal{N}')) \subseteq \mathcal{O}'(\mathit{Pub}^*(\mathcal{N}'))$. □

4.3 Weakly Fair Diagnosability

We prove that WF-diagnosability is at least as hard as reachability—and thus EXPSPACE-hard [20]. The reduction itself is inspired by a hardness proof by Howell et al. [13, Theorem 4.9] for deciding the existence of a weakly fair run.

Proposition 4.5 (Hardness of WF-Diagnosability). *There is a polynomial time reduction from the reachability problem in Petri nets to non WF-diagnosability, which outputs live convergent nets with $W \cap F = \emptyset$.*

Proof. Consider an instance $\langle \mathcal{N}, \boldsymbol{m} \rangle$ of the reachability problem where $\mathcal{N} = \langle P, T, w, \boldsymbol{m}_0 \rangle$ and $\boldsymbol{m} \in \mathbb{N}^P$. Define $n_0 \stackrel{\text{def}}{=} 1 + \sum_{p \in P} \boldsymbol{m}_0(p)$ and $n \stackrel{\text{def}}{=} 1 + \sum_{p \in P} \boldsymbol{m}(p)$.

We start by constructing a net $\mathcal{N}' \stackrel{\text{def}}{=} \langle P \uplus \{\mathit{sum}, \mathit{active}\}, T, w', \boldsymbol{m}'_0 \rangle$ that extends $\mathcal{N}$ with a 'checksum' place *sum* and a control place *active*. The initial marking $\boldsymbol{m}'_0$ extends $\boldsymbol{m}_0$ with $\boldsymbol{m}'_0(\mathit{sum}) \stackrel{\text{def}}{=} n_0$ and $\boldsymbol{m}'_0(\mathit{active}) \stackrel{\text{def}}{=} 1$. The flow w' is defined as w extended for all $t \in T$ with

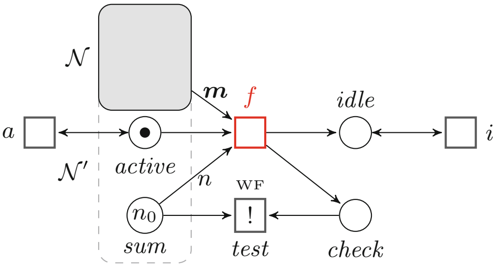


Fig. 6. The Petri net $\mathcal{N}''$ in the proof of Proposition 4.5.

- $w(\mathit{sum}, t) \stackrel{\text{def}}{=} \sum_{p \in P} w(p, t)$ and $w(t, \mathit{sum}) \stackrel{\text{def}}{=} \sum_{p \in P} w(t, p)$, which ensures that, in any reachable marking $\boldsymbol{m}'$ of $\mathcal{N}'$, $\boldsymbol{m}'(\mathit{sum}) = 1 + \sum_{p \in P} \boldsymbol{m}'(p)$;
- $w(\mathit{active}, t) \stackrel{\text{def}}{=} w(t, \mathit{active}) \stackrel{\text{def}}{=} 1$, which ensures that the original transitions in T can only be fired if *active* is marked; we call such markings 'active'.

We now construct $\mathcal{N}''$ extending $\mathcal{N}'$ as shown in Fig. 6. It features:

- a fault transition f that can be fired at most once, from an active marking $\boldsymbol{m}'$ that covers $\boldsymbol{m}$, and the projection of $\boldsymbol{m}'$ to P was equal to $\boldsymbol{m}$ if and only if *sum* is empty as a result of firing f;
- a weakly fair transition *test* that can be fired at most once, necessarily at some point after f was fired, and whose purpose is to test whether *sum* is empty;
- two transitions a and i, idling respectively when *active* or *idle* is marked.

We define $E \stackrel{\text{def}}{=} \{a, e\}$ and let our observation mask $\mathcal{O}$ map every transition to a, except for $\mathcal{O}(\mathit{test}) \stackrel{\text{def}}{=} e$ and $\mathcal{O}(f) \stackrel{\text{def}}{=} \varepsilon$; we set $W \stackrel{\text{def}}{=} \{\mathit{test}\}$ and $F \stackrel{\text{def}}{=} \{f\}$. Observe that $\mathcal{N}''$ is live and convergent with $W \cap F = \emptyset$.

Claim. The marking $\boldsymbol{m}$ is reachable in $\mathcal{N}$ if and only if $\mathcal{N}''$ is not WF-diagnosable.

Since $W \cap F = \emptyset$, by Lemma 3.9, $\mathcal{N}''$ is not WF-diagnosable if and only if there exist $\sigma \in \mathit{Faulty}^{\omega}_{WF}(\mathcal{N}'')$ and $\rho \in \mathit{Correct}^{\omega}(\mathcal{N}'')$ such that $\mathcal{O}(\sigma) = \mathcal{O}(\rho)$.

For the 'only if' direction, assume $\boldsymbol{m}_0 \overset{\hat{\sigma}}{\Rightarrow} \boldsymbol{m}$ in $\mathcal{N}$. Then the same transition sequence $\hat{\sigma}$ leads in $\mathcal{N}''$ to an active marking equal to $\boldsymbol{m}$ over P, with n tokens in *sum*. Then $\sigma \overset{\text{def}}{=} \hat{\sigma}\, f\, i^{\omega}$ can be fired in $\mathcal{N}''$, and is weakly fair because *sum* becomes empty once f has fired. Defining $\rho \overset{\text{def}}{=} a^{\omega}$, we get $\mathcal{O}(\sigma) = a^{\omega} = \mathcal{O}(\rho)$ and $\mathcal{N}''$ is therefore not WF-diagnosable.

For the 'if' direction, let us first consider any $\rho \in \mathit{Correct}^{\omega}(\mathcal{N})$: as *check* cannot be marked in any correct run, *test* cannot be fired, and $\mathcal{O}(\rho) = a^{\omega}$. Turning our attention to $\sigma \in \mathit{Faulty}^{\omega}_{WF}(\mathcal{N}'')$, since it is faulty, f has been fired, hence the run on σ is of the form $\boldsymbol{m}''_0 \overset{\hat{\sigma}}{\Rightarrow} \boldsymbol{m}' \overset{f}{\Rightarrow} \boldsymbol{m}'' \overset{\sigma'}{\Longrightarrow}$ in $\mathcal{N}''$. We know that $\boldsymbol{m}'(p) \geq \boldsymbol{m}(p)$ for all $p \in P$ because f could be fired from $\boldsymbol{m}'$. Assume for the sake of contradiction that $\boldsymbol{m}'(p) > \boldsymbol{m}(p)$ for some $p \in P$, and let us show that it implies that σ is not weakly fair; this will prove that $\boldsymbol{m}$ was reachable in $\mathcal{N}$.

By the invariant on *sum*, $\boldsymbol{m}'(p) > \boldsymbol{m}(p)$ for some $p \in P$ entails $\boldsymbol{m}''(\mathit{sum}) > 0$ and therefore that *test* is enabled in $\boldsymbol{m}''$. However, if *test* were fired in σ', this would entail $\mathcal{O}(\sigma) \in a^{*}ea^{\omega} \neq \mathcal{O}(\rho)$ (thus σ does not satisfy (WF.1)). Furthermore, σ does not satisfy (WF.2) either, since, once f has fired, *test* is the only fireable transition with either *sum* or *check* in its preset. □

5 Upper Bounds

In this section, we give upper complexity bounds in Sect. 5.1 for safe WF-PNs, that match the lower bounds of the previous section. For general Petri nets in Sect. 5.2, since opacity is undecidable, we only consider diagnosability and show that the problem is EXPSPACE-complete in the absence of weak fairness. We also consider strict WF-PNs and show an exponential time reduction to the reachability problem in this case. The general case of WF-PN remains open.

5.1 Safe Petri Nets

In the case of safe Petri nets, our upper complexity bounds for checking diagnosability and opacity *with weak fairness* match the lower bounds of Sect. 4 for the variants without weak fairness. From this viewpoint, weak fairness can be included 'for free' in diagnosability and opacity checking for concurrent systems.

WF-Diagnosability. Germanos et al. [7] show that, given a convergent WF-PN $\mathcal{W} = \langle \mathcal{N}, W \rangle$, one can construct in polynomial time a PN $\mathcal{N}'$ and a state-based LTL formula φ, such that $\mathcal{W}$ is WF-diagnosable if and only if $\mathcal{N}'$ has an infinite run satisfying φ. Since LTL model-checking of safe PNs is in PSPACE [5], the same upper bound applies to WF-diagnosis, which shows that the lower bound in Proposition 4.2 is tight.

Proposition 5.1. *WF-diagnosability is in* PSPACE *for safe convergent Petri nets.*

Weakly Fair Opacity. In the case of WF-opacity, we argue directly that there is an ESPACE algorithm for safe Petri nets, matching the lower bound from Proposition 4.4.

Proposition 5.2. *WF-opacity is in* ESPACE *for safe Petri nets.*

Proof (sketch). Let $\mathcal{W}$ be a safe WF-PN with n places. We sketch a nondeterministic algorithm $\mathcal{M}$ working in space $2^{O(n)}$ that checks for the negation of Definition 3.5 in $\mathcal{W}$. The result then follows from Savitch's Theorem showing NESPACE=ESPACE and the fact that ESPACE is deterministic.

We must look for a finite prefix $\hat{\sigma}$ of a run that uses a secret transition, and such that there exists no infinite WF trace $\rho \in \mathit{Pub}^{\omega}_{WF}(\mathcal{W})$ satisfying that $\mathcal{O}(\hat{\sigma}) < \mathcal{O}(\rho)$. The algorithm works in two phases:

1. the first phase nondeterministically picks a suitable prefix $\hat{\sigma}$ 'on the fly', along with the set $M \subseteq 2^n$ of possible markings reachable by some $\hat{\rho} \in \mathit{Pub}^*(\mathcal{W})$ with $\mathcal{O}(\hat{\sigma}) = \mathcal{O}(\hat{\rho})$—this can be carried in space $2^{O(n)}$—and
2. the second phase checks whether any marking $\boldsymbol{m} \in M$ can start a weakly fair infinite run; this can be verified by a model-checking algorithm for LTL—in PSPACE [5]. □

5.2 General Petri Nets

Because opacity is undecidable for general Petri nets by Proposition 4.4, we shall focus on (WF-)diagnosability. We rely for our results on decidable fragments of LTL on Petri net executions. The first step in the following reductions is to build (in polynomial time) a suitable *verifier net* $\mathcal{V}(\mathcal{W})$ from the input WF-PN $\mathcal{W}$; this consists simply in synchronising two copies $\mathcal{W}_1$ and $\mathcal{W}_2$ of $\mathcal{W}$ on their observations while letting unobservable transitions run asynchronously, and discarding fault transitions from the second copy—see the full paper for the precise construction, variants were used for instance in [3,7,21]. Then $\mathcal{W}$ is not diagnosable according to Definition 2.1 (thus ignoring weak fairness constraints for the moment) if and only if there exists an infinite run σ in $\mathcal{V}(\mathcal{W})$ that eventually visits some fault transition $f \in F$ (thus in the first copy):

$$\exists \sigma \in \mathit{Trace}^{\omega}(\mathcal{V}(\mathcal{W})), \exists i \in \mathbb{N} : \bigvee_{f \in F_1} \sigma(i) = f\,; \tag{2}$$

here the '$_1$' subscript denotes the fact that we are looking for a transition from the first copy $\mathcal{W}_1$ of $\mathcal{W}$.

Diagnosability. The characterisation of non diagnosability in (2) translates immediately into the existence of an infinite trace of $\mathcal{V}(\mathcal{W})$ satisfying the *action-based* LTL formula

$$\Diamond\Big(\bigvee_{f\in F_1} f\Big). \tag{3}$$

Model-checking of action-based LTL formulæ in general Petri nets can be performed in EXPSPACE [12], hence in the absence of weakly fair transitions the lower bound from Proposition 4.2 is tight. This result dramatically improves the procedure proposed in [3], which relies on the construction of the coverability graph for the verifier net, producing an Ackermannian complexity.

Proposition 5.3. *Diagnosability for Petri nets is in* EXPSPACE*.*

Strict Case. By Lemma 3.9, if no fault is weakly fair in a WF-PN, then non WF-diagnosability is equivalent to the existence of a run satisfying (2) and whose projection on transitions from the first copy is weakly fair. In order to check those conditions, we are going to use another fragment of LTL proven decidable over Petri nets by Jančar [14]. The fragment LTL($\Box\Diamond$) can use both actions and states in its atomic propositions, but only allows positive Boolean combinations of 'infinitely often' $\Box\Diamond$ formulæ at top-level.

As LTL($\Box\Diamond$) does not feature $\Box$ on its own, we cannot use (3) directly, and we first modify $\mathcal{V}(\mathcal{W})$ so that all the fault transitions add a token to a new place *fault*, which is initially empty; once *fault* is marked, it remains so forever. Then non WF-diagnosability is equivalent to the existence of an infinite run of $\mathcal{V}(\mathcal{W})$ satisfying

$$\Box\Diamond(\mathit{fault} > 0) \wedge \bigwedge_{t\in W_1} \big((\Box\Diamond t) \vee (\Box\Diamond \bigvee_{t'\in T_1} \bigvee_{p\in P_1} t' \wedge (p < w(t,p) + w(t',p))\big). \tag{4}$$

Because Jančar [14] proved existential LTL($\Box\Diamond$) model checking of Petri nets to reduce in exponential time to the reachability problem, by Proposition 4.5 we get an equivalence between non WF-diagnosability when $W \cap F = \emptyset$ and reachability, modulo exponential-time many-one reductions.

Proposition 5.4. *There is an exponential time reduction from non WF-diagnosability in strict convergent WF-PNs to the reachability problem.*

6 Concluding Remarks

We have revisited the problems of diagnosability and opacity with a focus on expressivity for concurrent systems, and introduced a new notion of opacity for Petri nets under weakly fair semantics.

We have conducted a comparative study of complexity for both diagnosability and opacity analysis. Not surprisingly, opacity is always harder than diagnosability, and complexity also increases when moving from automata to safe Petri nets to general Petri nets, i.e., from the sequential to the concurrent to the infinite.

Safe Petri Nets. Note that the price to pay in safe Petri nets for the extra precision of analysis under *weak fairness*—which allows to capture indirect dependencies, as seen above and in [9,11]—is not higher than for the corresponding analyses with ordinary semantics. We therefore argue that the refined notions of WF-diagnosability from [7,11], and of WF-opacity that we have introduced in this paper, are valid and important contributions to the design and monitoring of concurrent systems. Future work should investigate efficient algorithms for the analysis of partially observed Petri nets.

General Petri Nets. For strict WF-PNs, Proposition 4.5 leaves an exponential complexity gap with our upper bound in Proposition 5.4. It might be worth investigating whether this gap could be filled by considering a reduction from reachability in *succinctly* presented Petri nets. In the general case, the main difficulty is that Definition 3.3 is essentially a branching-time property, which are generally undecidable in Petri nets. It is however quite a specific property, as can be seen in the case of safe Petri nets where it can be reduced to a linear-time property [7, Lemma 3.4]—unfortunately this reduction does not hold in general Petri nets—, and this might explain why we could not prove it undecidable either.

References

1. Badouel, E., Bednarczyk, M.A., Borzyszkowski, A.M., Caillaud, B., Darondeau, P.: Concurrent secrets. Discrete Event Dyn. Syst. **17**(4), 425–446 (2007)
2. Bryans, J., Koutny, M., Mazaré, L., Ryan, P.Y.A.: Opacity generalised to transition systems. Int. J. Inf. Secur. **7**(6), 421–435 (2008)
3. Cabasino, M.P., Giua, A., Lafortune, S., Seatzu, C.: A new approach for diagnosability analysis of Petri nets using verifier nets. IEEE Trans. Autom. Control **57**(12), 3104–3117 (2012)
4. Cassez, F., Dubreil, J., Marchand, H.: Dynamic observers for the synthesis of opaque systems. In: Liu, Z., Ravn, A.P. (eds.) ATVA 2009. LNCS, vol. 5799, pp. 352–367. Springer, Heidelberg (2009). doi:10.1007/978-3-642-04761-9_26
5. Esparza, J.: Decidability and complexity of Petri net problems — an introduction. In: Reisig, W., Rozenberg, G. (eds.) ACPN 1996. LNCS, vol. 1491, pp. 374–428. Springer, Heidelberg (1998). doi:10.1007/3-540-65306-6_20
6. Even, S.: On information lossless automata of finite order. IEEE Trans. Elec. Comput. **EC-14**(4), 561–569 (1965)
7. Germanos, V., Haar, S., Khomenko, V., Schwoon, S.: Diagnosability under weak fairness. ACM Trans. Embed. Comput. Syst. **14**(4:69), 132–141 (2015)
8. Haar, S.: Qualitative diagnosability of labeled Petri nets revisited. In: Proceedings of CDC 2009 and CCC 2009, pp. 1248–1253. IEEE (2009)
9. Haar, S.: Types of asynchronous diagnosability and the reveals-relation in occurrence nets. IEEE Trans. Autom. Control **55**(10), 2310–2320 (2010)
10. Haar, S.: What topology tells us about diagnosability in partial order semantics. Discrete Event Dyn. Syst. **22**(4), 383–402 (2012)
11. Haar, S., Rodríguez, C., Schwoon, S.: Reveal your faults: it's only fair! In: Proceedings of ACSD 2013, pp. 120–129. IEEE (2013)

12. Habermehl, P.: On the complexity of the linear-time μ-calculus for Petri Nets. In: Azéma, P., Balbo, G. (eds.) ICATPN 1997. LNCS, vol. 1248, pp. 102–116. Springer, Heidelberg (1997). doi:10.1007/3-540-63139-9_32
13. Howell, R.R., Rosier, L.E., Yen, H.C.: A taxonomy of fairness and temporal logic problems for Petri nets. Theor. Comput. Sci. **82**(2), 341–372 (1991)
14. Jančar, P.: Decidability of a temporal logic problem for Petri nets. Theor. Comput. Sci. **74**(1), 71–93 (1990)
15. Jančar, P.: Nonprimitive recursive complexity and undecidability for Petri net equivalences. Theor. Comput. Sci. **256**(1–2), 23–30 (2001)
16. Jiang, S., Huang, Z., Chandra, V., Kumar, R.: A polynomial algorithm for testing diagnosability of discrete event systems. IEEE Trans. Autom. Control **46**(8), 1318–1321 (2001)
17. Jones, N.D., Landweber, L.H., Lien, Y.E.: Complexity of some problems in Petri nets. Theor. Comput. Sci. **4**(3), 277–299 (1977)
18. Leroux, J., Schmitz, S.: Demystifying reachability in vector addition systems. In: Proceedings of LICS 2015, pp. 56–67. IEEE (2015)
19. Lin, F.: Opacity of discrete event systems and its applications. Automatica **47**(3), 496–503 (2011)
20. Lipton, R.: The reachability problem requires exponential space. Technical report 62. Yale University (1976)
21. Madalinski, A., Khomenko, V.: Diagnosability verification with parallel LTL-X model checking based on Petri net unfoldings. In: Proceedings of SysTol 2010, pp. 398–403. IEEE (2010)
22. Mayer, A.J., Stockmeyer, L.J.: The complexity of word problems–this time with interleaving. Inf. Comput. **115**(2), 293–311 (1994)
23. Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K., Teneketzis, D.: Diagnosability of discrete-event systems. IEEE Trans. Autom. Control **40**(9), 1555–1575 (1995)
24. Schmitz, S.: Automata column: the complexity of reachability in vector addition systems. ACM SIGLOG News **3**(1), 3–21 (2016)
25. Tong, Y., Li, Z., Seatzu, C., Giua, A.: Verification of initial-state opacity in Petri nets. In: Proceedings of CDC 2015, pp. 344–349. IEEE (2015)
26. Vogler, W.: Fairness and partial order semantics. Inf. Process. Lett. **55**(1), 33–39 (1995)
27. Yoo, T.S., Lafortune, S.: Polynomial-time verification of diagnosability of partially observed discrete event systems. IEEE Trans. Autom. Control **47**(9), 1491–1495 (2002)