Effective Verification of Weak Diagnosability

Anoopam Agarwal,* Agnes Madalinski,** Stefan Haar***

* Student, IIT Delhi, India (e-mail: anoopamagarwal@gmail.com)
** University Austral de Chile, Campus Mirafores, Valdivia, Chile
(e-mail: amadaliniuach.cl)
*** INRIA and LSV (CNRS and ENS Cachan)
61, avenue du Président Wilson
94235 CACHAN Cedex, France
(e-mail: haar@lsv.ens-cachan.fr,stefan.haar@inria.fr).

Abstract: The diagnosability problem can be stated as follows: does a given labeled Discrete Event System allow for an outside observer to determine the occurrence of the “invisible” fault, no later than a bounded number of events after that unobservable occurrence, and based on the partial observation of the behaviour? When this problem is investigated in the context of concurrent systems, partial order semantics induces a separation between classical or strong diagnosability on the one hand, and weak diagnosability on the other hand. The present paper presents the first solution for checking weak diagnosability, via a verifier construction.

Keywords: Discrete event systems, diagnosis, Petri nets, events, observability, partial order semantics, Event structures.

1. INTRODUCTION

Diagnosis under partial observation is a classical problem in automatic control in general, and has received considerable attention in discrete event system (DES) theory, among other fields. In the DES setting, the approach that we will call “classical” here supposes that the observed system is an automaton with transition set \( T \), prefix-closed language \( L \subseteq T^* \), and a set of observable transition labels \( \mathcal{O} \). The associated labeling map \( \lambda : T \rightarrow \mathcal{O} \) may not be required injective, and leaves some transitions from \( T \) unobservable, in particular fault \( \phi \). The observations have the form of words \( w \in \mathcal{O}^* \) obtained by applying \( \lambda \) to words in \( T^* \). A classical definition of diagnosability is given in Sampath et al. (1995); we follow the equivalent presentation of Cassandras and Lafortune (1999). Write \( s \sim_\lambda s' \) iff \( \lambda(s) = \lambda(s') \), and call any sequence \( s \) such that \( \phi \) occurs in \( s \) a faulty sequence, and all other sequences healthy. Then:

Definition 1. (Sequential Diagnosability). A prefix-closed language \( L \subseteq T^* \) is not (strongly) diagnosable iff there exist sequences \( s_N, s_Y \in L \) such that:

1. \( s_Y \) is faulty, \( s_N \) is healthy, and \( s_N \sim_\lambda s_Y \);
2. \( s_Y \) with the property 1 can be chosen arbitrarily long after the first fault, i.e. for every \( k \in \mathbb{N} \) there exists a choice of \( s_N, s_Y \in L \) with the above properties and such that the suffix \( s_Y/\phi \) of \( s_Y \) after the first occurrence of fault \( \phi \) in \( s_Y \) satisfies \( |s_Y| \geq k \).

Concurrent systems are difficult to supervise using the classical approach because of the state explosion problem. For intrinsically asynchronous distributed systems, such as encountered in telecommunications or more generally in networked systems, the use of models that reflect the local and distributed nature of the observed system, such as Petri nets or graph grammars, is helpful not only in terms of computational efficiency, but also conceptually. Putting these ideas together, Benveniste et al. (2003) extends diagnosis to asynchronous models and their non-interleaved semantics. This generalized methodology for fault diagnosis is based on the non-sequential executions of labeled Petri nets, that is, the partial order semantics in occurrence nets and event structures. Theoretical aspects of partial order diagnosability for Petri nets, in the spirit of the above definition, have been developed in Haar et al. (2003); Haar (2007, 2009, 2010a,b). While the sequential case is embedded and generalized in these results, new features emerge in partial ordered runs that have no counterpart in sequential behaviour; this led to the distinction between strong and weak observability and diagnosability properties in Haar et al. (2003); Haar (2010a).

2. PETRI NETS AND UNFOLDINGS

Definition 2. A net is a tuple \( N = (P, T, F) \) where

- \( P \neq \emptyset \) is a set of places,
- \( T \neq \emptyset \) is a set of transitions such that \( P \cap T = \emptyset \),
- \( F \subseteq (P \times T) \cup (T \times P) \) is a set of flow arcs.

A marking is a multiset \( M \) of places, i.e. a map from \( P \) to \( N \). A Petri net is a tuple \( N = (P, T, F, M) \), where (i) \( (P, T, F) \) is a finite net, and (ii) \( M : P \rightarrow \mathbb{N} \) is an initial marking.

Elements of \( P \cup T \) are called the nodes of \( N \). For a transition \( t \in T \), we call \( \bullet t = \{ p \mid (p, t) \in F \} \) the preset
of $t$, $t^* = \{ p \mid (t,p) \in F \}$ the postset of $t$. In Figure 1, we represent as usual places by empty circles, transitions by squares, $F$ by arrows, and the marking of a place $p$ by putting the corresponding number of black tokens into $p$.

A transition $t$ is enabled in marking $M$, written $M \xrightarrow{t} M'$, if $\forall p \in t^* , M(p) > 0$; otherwise write $M \xleftarrow{t} M'$. An enabled transition $t$ can fire, resulting in a new marking $m' = m - t^* + t^*$; this firing relation is denoted by $M \xrightarrow{t} M'$. A marking $m$ is reachable if there exists a firing sequence, i.e. transitions $t_0 \ldots \ t_m$ and markings $M_0, \ldots, M_m$ such that $M_0 \xrightarrow{t_0} M_1 \xrightarrow{t_1} \ldots \xrightarrow{t_m} M_m$. A Petri net is safe if for all reachable markings $M$, $M(p) \in \{0,1\}$ for all $p \in P$; all Petri nets considered here are safe.

Occurrence nets and unfoldings. In a net $N = (P, T, F)$, let $<_N$ the transitive closure of $F$, and $\leq_N$ the reflexive closure of $<_N$. For $t_1, t_2 \in T$, set $t_1 \#_{im} t_2$ and $t_1 \ll t_2$ if $t_1 \neq t_2$ and $\#_{im} t_1 \cap \#_{im} t_2 \neq \emptyset$, and define $\equiv = \#_N \cap \equiv_N$ by

$$ a \# b \iff \exists t, a \in t \iff \exists t, b \in t : t \wedge t \leq_N a \wedge t \leq_N b. $$

Define $co = co_N$ by setting, for any $a, b \in P \cup T$,

$$ a co b \iff \neg(\neg b < a) \land \neg(\neg a < b). $$

Definition 3. Let $ON = (B, E, G)$ be a net, and define the closed and open prime configurations for $E$ in $B$ by:

$$ [e] = \{ y \in B \cup E \mid y \leq_{ON} e \} \text{ and } \langle e \rangle = [e] \setminus \{ e \}. $$

Then $ON$ is an occurrence net if and only if it satisfies:

1. $\leq_{ON}$ is a partial order;
2. for all $b \in B$, $\{ \# b \} \in \{0,1\}$;
3. for all $e \in E$, the set $[e]$ is finite;
4. no self-conflict, i.e. there is no $x \in B \cup E$ such that $x \#_{ON} x$;
5. the set $cut_0$ of $\leq_{ON}$-minimal nodes is contained in $B$ and finite.

In occurrence nets, the nodes of $E$ are called events, and occurrence nets constitute particular cases of prime event structures (PES) in the sense of Winskel et al and Nielsen et al. (1981):

Definition 4. A prime event structure (over alphabet $\alpha$) is a tuple $E = (E, \leq, \#)$, where $E$ is a set of events,

1. $\leq \subseteq E \times E$ is a partial order satisfying the property of finite causes, i.e. for all $e \in E$, $|\{ e \}| < \infty$, and
2. $\# \subseteq E \times E$ an irreflexive symmetric conflict relation satisfying the property of conflict heredity, i.e. $\forall e, e', e'' \in E : e \# e' \land e' \leq e'' \Rightarrow e \# e''$.

Prefixes and Configurations. Restricting $\leq$ and $\#$ to the event set $E$, the "forgetting" conditions of $ON$, yields an event structure. A prefix of $E$ is any downward closed subset $V \subseteq E$, i.e. such that for every $e \in V$, $[e] \subseteq V$. Prefixes of $E$ induce, in the obvious way, sub-event structures of $E$ in the sense of the above definition. Denote the set of $E$'s prefixes as $V(E)$. Prefix $c \in V(E)$ is a configuration if and only if it is conflict-free, i.e. if $e \in c$ and $e \# e'$ imply $e' \not\in c$. Denote as $C(E)$ the set of $E$'s configurations, and as $C^\text{fin}(E) \subseteq C(E)$ the set of all finite configurations. Call any $\leq$-maximal element of $C(E)$ a run of $E$; denote the set of $E$'s runs as $\Omega(E)$, or simply $\Omega$ if no confusion can arise.

Definition 5. If $N_i = (P_i, T_i, F_i)$ and $N_2 = (P_2, T_2, F_2)$ are nets, a homomorphism is a mapping $h : P_1 \cup T_1 \rightarrow P_2 \cup T_2$ such that (i) $h(P_1) \subseteq P_2$ and (ii) for every $t \in T_1$, the restriction to $t^*$ of $t_1$ is a bijection between the set $\#_1 t_1$ in $N_1$ and the $\#_2 (h(t_1))$ in $N_2$, and similarly for $t^*$ and $(h(t_1))^*$. A branching process of safe Petri net $N = (M_0, \pi)$ is a pair $\beta = (ON, \pi)$, where $ON = (B, E, G)$ is an occurrence net, and $\pi$ is a homomorphism from $ON$ to $N$ such that:

1. The restriction of $\pi$ to $cut_0$ is a bijection from $cut_0$ to $M_0$, and
2. for every $e_1, e_2 \in E$, if $e_1 = e_2$ and $\beta(e_1) = \beta(e_2)$ then $e_1 = e_2$.

The unique (up to isomorphism) maximal branching process $\beta_{Unf} = (ON_{Unf}, \pi_{Unf})$ of $N$ is called the unfolding of $N$; see Esparza and Vogler (2002) for a canonical algorithm to compute the unfolding of $N$. We will assume that all transitions $t \in T$ have at least one output place, i.e. $t^*$ is not empty. In this case, every finite configuration $c$ of $ON_{Unf}$ spans a conflict free subset $c_{Unf} = (E_c, B_c, G_{(E_c \times B_c) \cup (B_c \times E_c)})$ of $ON_{Unf}$ by setting

$$ B_c \triangleq \bigcup_{e \in E_c} (e \cup e^*). $$

The following results (see e.g. Esparza and Vogler (2002)) justify the use of unfoldings: The set $cut(c)$ of $\leq$-maximal nodes of $c_{Unf}$ is contained in $B_c$. Moreover, $cut(c)$ is a coset, that is, for all distinct conditions $b, b' \in cut(c)$, $b \# b'$ holds; and $cut(c)$ is $\leq$-maximal with this property, and such sets in occurrence nets are called cuts. By setting, for any cut $cut$ and place $p$,

$$ M_{cut}(p) \triangleq \{ b \mid b \in cut : \pi(b) = p \}, $$

we obtain a marking of $N$. Now, for $cut(c)$ as above, $M_c \triangleq M_{cut(c)}$ is a reachable marking of $N$, more precisely the marking that $N$ is in after executing firable transitions in a sequence compatible with $c$. Conversely, for every reachable marking $M$ of $N$ there exists (at least) one configuration $c$ in $ON_{Unf}$ such that $M_c = M$.

Progressive configurations. For any finite configuration $c$ and event $e \in E \setminus c$ such that $c \cup \{ e \}$ is a configuration (in particular, there is no conflict between $e$ and any event in $c$ and all predecessors of $e$ are contained in $c$), we have that $M_c \supseteq \pi(c)$. We therefore denote this situation by $c \rightleftharpoons$. Now, let the height of an event $e$ be the longest $\subseteq$-chain of events leading to and including $e$:

1. $H(\emptyset) \triangleq 0$,
2. $H(e) \triangleq 1 + \max\{ H(e') : e' \in (e) \}$,

and for any configuration $c$, let

$$ H(c) \triangleq \sup\{ H(e) : e \in c \}. $$

Then configuration $c$ is called progressive iff for every $e \in E \setminus c$ such that $c \rightleftharpoons$, one has $H(c) < H(e)$. Denote by $c_{prog}$ the set of progressive configurations.
3. OBSERVABILITY AND DIAGNOSABILITY

Let $\mathcal{N} = (P, T, F, M_0)$ a safe Petri net, $\lambda : T \to A$ a labeling mapping into an alphabet $A$ that contains the empty symbol $\varepsilon$. $\text{Unf}_N = (B, E, G, \text{cut}_0)$ its unfolding net, with labeling morphism $\alpha : E \to T$ given by the unfolding morphism. Denote as $\mathcal{U} \equiv \lambda^{-1}(\{\varepsilon\})$ the set of unobservable transitions, and as $\mathcal{O} \equiv T \setminus \mathcal{U}$ the set of observable transitions; accordingly, let $E_{\mathcal{U}} \equiv \alpha^{-1}(\mathcal{U})$ and $E_{\mathcal{O}} \equiv \alpha^{-1}(\mathcal{O})$ be the set of unobservable and observable events of $\text{Unf}_N$, respectively.

Due to partial observation, different configurations can be equivalent in terms of the observable behaviour. The following notations formalize this fact.

Definition 7. Write $c \sim_0 c'$ iff for the restrictions of $\subseteq$ to $c_0 \equiv c \cap E_0$ and $c'_0 \equiv c' \cap E_0$, there exists a label-preserving order isomorphism $I : c_0 \to c'_0$. If $c_1 \subseteq c_2$ and $c_2 \sim_0 c_3$, then write $c_1 \subseteq_0 c_3$.

Definition 8. Let $\sigma = t_1 t_2 ... \in T^\omega \equiv T^* \cup T^\infty$ be a transition sequence that is enabled in $M_0$, i.e. assume there exist reachable markings $M_1, M_2, ...$ of $\mathcal{N}$ such that

$$M_0 \xrightarrow{t_1} M_1 \xrightarrow{t_2} M_2 \xrightarrow{t_3} ...$$

Then $\sigma$ is weakly fair if for any $t \in T$ and $i \in \mathbb{N}$ for which $M_i \xrightarrow{t} \neq \emptyset$, there exists $j > i$ such that $M_j \xrightarrow{t} \neq \emptyset$.

In other words, weakly fair executions are such that no transition remains enabled "forever": after any transition $t$’s enabling on $\sigma$, $t$ must eventually become disabled, either by its own firing, or by the firing of a conflicting transition. In the unfolding of $\mathcal{N}$, a fair run corresponds to a set of events $\omega$ such that for any event $e$, either $e \in \omega$, or there exists $e' \in \omega$ such that $e \# e'$. Of course, this is equivalent to $\omega$ being a maximal configuration, i.e. $\omega \in \Omega$. Let $\phi \in \mathcal{U}$ be a fault transition, and let $E_\phi \equiv \alpha^{-1}(\phi)$. With these preparations, we are ready to define:

Definition 9. We say that $\mathcal{N}$ is weakly observable w.r.t. $\lambda$ iff for every $\omega \in \Omega(\mathcal{N})$, $|\omega \cap E_0| = \infty$. A weakly observable (w.r.t. $\lambda$) $\mathcal{N}$ is weakly diagnosable w.r.t. $\lambda$ and $\phi$ iff for every faulty run $\omega_0 \in \Omega(\mathcal{N})$, it holds that any $\omega \in \Omega(\mathcal{N})$ such that $\omega \sim_0 \omega_0$ satisfies $|\omega \cap E_0| < \infty$.

Example. In the net $\mathcal{N}$ in Figure 1 on the left , let the fault be $\phi = v$, and assume that $a$ is the only observable transition. Then:

a) In sequential semantics, the run which consists only of occurrences of $u$ and $v$ is infinite but produces no observation; $\mathcal{N}_*$ is therefore not (strongly) observable in the classical sense. Moreover, $\mathcal{N}_*$ is not (strongly) diagnosable, since all runs without an occurrence of $v$ are observationally indiscernable from the run $\omega'$ formed only by occurrences of $a$ and $\delta$; there exist thus observationally equivalent runs some of which are faulty, and some healthy.

b) However, with the same assumptions, $\mathcal{N}_*$ is both weakly observable and weakly diagnosable. In fact, every run $\omega$ is fault-definite since $v$ must have occurred.

The next section will make these intuitions more precise. Here, let us make one further observation in the context of the example. In fact, in decentralized systems with weak synchronization between subsystems, faults may elude diagnosis under the interleaved viewpoint, while being weakly captured under partial order semantics. In the example, consider now $b$ the fault event, instead of $v$, and let still $a$ be observable. Then, the new system is neither
classically observable nor classically diagnosable. However, in a workshop discussion with the third author, thanks to A. Guia who made us discover this aspect by a remark about the fault occurrence, that blocks diagnosis of the fault.

Thus, the partial order approach actually increases precision for partial observation of highly concurrent systems.

4. VERIFICATION OF WEAK DIAGNOSABILITY

The Verifier Net. For the practical verification, we propose to use an extension of the unfolding-based verifier method developed in Madalinski et al. (2010). The basic idea is to synchronize, via the observable labels, two copies of the supervised net \( \mathcal{N} \) and to check for the existence of executions of the product net in which the projection to the first component is faulty while that to the second component is healthy. Formally, with the setup of Definition 7, let \( \mathcal{V} \approx \mathcal{N}_1 \times \mathcal{N}_2 \) be the \( \alpha \)-synchronized product of two isomorphic copies \( \mathcal{N}_1 \) and \( \mathcal{N}_2 \) of \( \mathcal{N} \), i.e. \( \mathcal{N}_i = (P_i, T_i, F_i, M_0^i) \). That is, with

(1) \( P_0 = p_1 \uplus p_2 \),
(2) for \( i \in \{1, 2\} \), \( T_i^\sigma = \{ t \in T_i \mid \alpha(t) = \varepsilon \} \),
(3) \( T_{12} = \{ t \in T_1 \mid \alpha(t) \neq \varepsilon \} \),
(4) \( F_1 = \bigcup_{i=1}^n (F_1 \cap T_i^\sigma) \cup \bigcup_{i=1}^n (T_1 \cap T_i^\sigma \times P_i) \),
(5) \( F_{12} = \bigcup_{i=1}^n (F_1 \cap P_i \times T_1 \cap T_i^\sigma) \cup \bigcup_{i=1}^n (T_1 \cap T_1 \times T_i^\sigma) \),
(6) \( T_0 = T_1^\sigma \uplus T_2 \uplus T_{12} \) and \( F_0 = F_1 \uplus F_{12} \),
(7) \( M_0 = M_0^1 \uplus M_0^2 \),

\( \mathcal{V} \) is the Petri net \( \mathcal{N}_0 = (p_0, T_0, F_0, M_0) \), with the labeling \( \alpha \) inherited from \( \mathcal{N} \). The verifier of the running example is depicted in Figure 2.

**Lemma 1.** The configurations of \( \mathcal{V} \) are given by pairs \( (c_1, c_2) \) of configurations of \( \mathcal{N}_1, \mathcal{N}_2 \), respectively, where

(1) \( c_i \) is the projection of \( c \) to the occurrences and conditions for \( \mathcal{N}_i \), and
(2) there exists a partial mapping \( \psi : c \rightarrow c' \) such that
   - setting \( c_\psi = E_{c_1} \cap c \) and \( c_{\psi(t)} = E_{\psi(t)} \cap c \) (and analogously for \( c' \)), \( \psi(e) \) is defined for all \( e \in c_\psi \), and undefined for all \( e \in c_{\psi(t)} \);
   - the restriction \( \psi|_{c_\psi} \) defines a bijection \( \psi|_{c_\psi} : c_\psi \rightarrow c_\psi \).

\footnote{Thanks to A. Guia who made us discover this aspect by a remark in a workshop discussion with the third author.}

**Proof:** The decomposition of \( c \) follows from the synchronized product and the construction of \( \text{Unf}\mathcal{V} \); since \( c \) is free of cycles, it follows that \( c_1 < c_2 \) implies.

For the construction of a verifier, we follow Madalinski et al. (2010) in using a fault indicator variable whose value is one for all configurations on which a fault occurs, and 0 otherwise. For this, let \( \Phi : E \rightarrow \{0, 1\} \) be such that \( \Phi(c_1) = 1 \) if \( e \in e_\Phi \), and 0 otherwise; then, define recursively \( \nu : E \rightarrow \{0, 1\} \) by \( \nu(\text{cut}n) = 0 \) and

\[
\nu(e) \equiv \max \left[ \Phi(e), \max_{e' \leq e} \nu(e') \right]
\]

Mapping \( \nu \) extends naturally to a mapping \( \nu : C \rightarrow \{0, 1\} \) by setting \( \nu(e) \equiv \sup_{e' \leq e} \nu(e') \). Moreover, recall that every configuration \( c \) of \( \text{Unf}\mathcal{V} \) is given as a pair \((c_1, c_2)\) of configurations of \( \text{Unf}\mathcal{N} \); we therefore have a 2-vector valued mapping \( \nu : C \rightarrow \{0, 1\}^2 \) given by \( \nu(c) \equiv (\nu(c_1), \nu(c_2)) \).

The canonical prefix \( \mathcal{V} \). For the practical verification of weak diagnosability, we need to adapt our choice of cutting context to obtain a sufficient finite prefix of the verifier. The crucial point is the choice of the collection \( C_e \subseteq \text{CInv} \) for each event. Denote by

\[
\mathcal{C}_e \equiv \{ e \in \text{CInv} \mid e \in e \}
\]

the set of \textit{progressive} configurations containing event \( e \), i.e. the progressive extensions of \( [e] \), and by

\[
\mathcal{C}_e \equiv \{ e \in \mathcal{C}_e \text{ s.t. } e' \subseteq e \Rightarrow e' = e \}
\]

the set of progressive \( [e] \)-extensions that are minimal with this property. First, we note that for \( e \in E \), \( \mathcal{C}_e \neq \emptyset \); in fact, one obtains all configurations of \( \mathcal{C}_e \) by the following non-deterministic algorithm:

- Set \( N \equiv \mathcal{H}(e) \) and \( c_0 \equiv [e] \).
- For \( n \geq 1 \), set \( E_N \equiv \{ e \in E \mid c_{n-1} \leq \mathcal{H}(e) \leq n \} \).
- Choose \( e \in E_n \) such that \( e \leq c_{n-1} \) (i.e. \( c_{n-1} \sim e \)) and set \( c_n \equiv c_{n-1} \cup \{ e \} \).
- Repeat until \( E_n = \emptyset \).
Then, the definition of the cutting context for verification of weak diagnosability reads as follows:

(1) $c \sim c'$ iff (i) $M_c = M_{c'}$ and (ii) $\phi \in \pi(c)$ iff $\phi \in \pi(c')$;
(2) $c < c'$ iff $c \subseteq c'$ and
(3) $\mathcal{C} \triangleq \mathcal{C}_{prog}$.

One checks that the relations $\sim$ and $<$ thus defined satisfy the conditions of Definition 6. Moreover:

**Lemma 2.** There is no infinite $<$-chain of feasible events.

**Proof:** Assume there exist such $e_1 < e_2 < \ldots$ Since $\sim$ has only finitely many distinct classes in $\mathcal{C}$ (a fact that follows from 1-safeness), there must exist $i < j$ such that $[e_i] \sim [e_j]$. Therefore one finds $c_i \in \mathcal{C}_{e_i}$ and $c_j \in \mathcal{C}_{e_j}$ such that $c_i \sim c_j$ and $c_i \subseteq c_j$, which contradicts the feasibility of $e_j$. \qed

Therefore, by Khomenko et al. (2003), we obtain a complete canonical finite prefix $V_N$ of $\mathcal{N}$ for any safe Petri net $\mathcal{N}$. Specializing to the verifier net $\mathcal{V}$ defined above, denote $V_V$ by $V$ for simplicity.

We first observe:

**Theorem 1.** With the above notation, let $\text{Unf}_V$ be the unfolding of $\mathcal{V}$. Then $\mathcal{N}$ is weakly diagnosable iff for every progressive configuration $c = (c_1, c_2)$ of $\mathcal{V}$ such that both $c_1$ and $c_2$ are progressive for $\mathcal{N}$, either both $c_1$ and $c_2$ are faulty, or both are healthy, that is: $\nu(c) \in \{(0,0),(1,1)\}$.

**Proof:** Follows directly from the definitions. \qed

We have:

**Theorem 2.** Assume $\mathcal{N}$ is weakly observable. If for every $e \in \text{coff}(V)$, one has $\nu([e]) \in \{(0,0),(1,1)\}$, then $\mathcal{N}$ is weakly diagnosable.

**Proof:** Assume that all cut-off events $e$ satisfy $\nu([e]) \in \{(0,0),(1,1)\}$, but that there exists $c = (c_1, c_2)$ such that, w.l.o.g., $\nu(c) = (1,0)$ and $c_1$ is progressive. Choose $c \prec$-minimal with this property, and let $\phi$ be the $\prec$-minimal occurrence of a fault event $e_0$ in $c$. By construction of $\mathcal{V}$ and Theorem 1, there exists a corresponding event $e' \in V$; if $e'_0$ is a cut-off event, we have a contradiction, since $\nu(e'_0) = (1,0)$ by construction. Hence assume $e'_0$ is not cut-off; then there is $c_{e'_0} \in \mathcal{C}_c$ such that $c_{e'_0} \prec c$, contradicting the $\prec$-minimal choice of $c$, and we are done. \qed

The converse of Theorem 1 does *not* hold. In fact, note first that there are in general progressive configurations of $\mathcal{V}$ that do *not* project to progressive configurations of the components $\mathcal{N}_1$ and $\mathcal{N}_2$. This is the case for the net $\mathcal{N}$ shown in figure 3: in $\mathcal{N}$, with $a$ and $b$ the only observable transitions, take the configuration $c_1$ obtained by firing $t_1, t_3, t_4$ exactly once, and let $c_2$ be the configuration obtained by one firing each of $t_2, t_3, t_4, t_6$. Now, the verifier (which we do not draw here due to space limitations) $\mathcal{V}$ has a progressive configuration $c = (c_1, c_2)$ whose projection to $\mathcal{N}_1$ is $c_1$, and whose $\mathcal{N}_2$-image is the configuration $c_2$ obtained by firing $t_2, t_3, t_4$ exactly once. Clearly, $c_2$ is a proper prefix of $c_2$, and $c_2$ is *not* progressive. This means that, for a general net $\mathcal{N}$, the verifier $\mathcal{V}$’s verdict provides a semi-decision, which has to be complemented:

(1) If there is no ambiguous $c \in \mathcal{C}_{prog}$, then $\mathcal{N}$ is weakly diagnosable.
(2) If $\mathcal{V}$ exhibits an ambiguity witness, i.e., $c = (c_1, c_2) \in \mathcal{C}_{prog}(\mathcal{V})$ such that (w.l.o.g.) $c_1$ is a faulty configuration of $\mathcal{N}_1$ and $c_2$ a healthy configuration of $\mathcal{N}_2$, it must be verified (this can be done on finite prefixes of $\mathcal{N}$ whose size is bounded by that of $\mathcal{V}(\mathcal{V})$) whether both $c_1 \in \mathcal{C}_{prog}(\mathcal{N}_1)$ and $c_2 \in \mathcal{C}_{prog}(\mathcal{N}_2)$ hold. If so, then $\mathcal{N}$ is *not* weakly diagnosable. Otherwise, if there is another witness from $\mathcal{V}$, inspect that witness; otherwise $\mathcal{N}$ is weakly diagnosable.

The net $\mathcal{N}_*$ of the running example (Figure 1 on the left) is weakly diagnosable. This can be analyzed on the verifier’s unfolding prefix depicted in Figure 4 on the left. To avoid a lengthy enumeration, consider the following informal analysis: there exist maximal configurations of the verifier prefix with (i) one or (ii) zero occurrences of $a$. With one occurrence of $a$, we must have also, in every maximal configuration of $\mathcal{V}$, one occurrence each of $v$ and $v'$. This is reflected by the cut-off $c = \{e_1, e_2, e_3, e_4, e_5, e_7, e_9\}$ with $\nu(c) = (1,1)$. Finally, if $a$ does not occur, then we must have occurrence of the highest (in the figure) instances of $y$ and $y'$, which is only possible if there is exactly one occurrence each of $v$ and $v'$. This is illustrated by the cut-off $c' = \{e_1, e_2, e_3, e_4, e_5, e_6, e_8, e_{12}, e_{13}\}$ with $\nu(c') = (1,1)$. Consider $\mathcal{N}_w$ from Figure 4. On the right hand side, $c = \{e_2, e_3, e_4, e_6, e_{10}, e_{13}, e_{19}, e_{21}\}$ with $\nu(c) = (1,0)$ witnesses a violation of weak diagnosability. In fact, in
the entire example one cannot distinguish between runs on which only $w$ occurs - that is, healthy runs - from the faulty ones that contain occurrences of $v$; $\mathcal{N}_w$ is not weakly diagnosable.

5. CONCLUSION AND OUTLOOK

We have provided a cornerstone for partial order diagnosis for safe Petri nets, by showing how weak diagnosability can be effectively verified using a finite occurrence net. The main construction is that of a complete finite prefix of the unfolding of the verifier net obtained as the product of to copies of the system model $\mathcal{N}$, synchronized by fusing only observable transitions.

In Madalinski et al. (2010), the verifier construction with Petri net unfoldings, on which our approach builds up, had been developed in the context of verification of strong diagnosability. Moving to the problem of weak diagnosability required a subtle modification of the cutting context. In fact, unfoldings are most frequently exploited, and cut off, using prime configurations [e] only; this was shown in Madalinski et al. (2010) to capture efficiently violations of (strong) diagnosability. However, these configurations are in general not progressive, and do not allow to detect faults in unsynchronized parts of the net, such as in $\mathcal{N}_v$ above. For analyzing nets that are not strongly diagnosable but might still allow weak diagnosis (“based on the observation, $v$ is eventually inevitable”), like $\mathcal{N}_v$, the system of prime configurations is not adequate. The key to extending the verifier approach was therefore the adaptation of the cutting context, in the sense of Khomenko et al. (2003), so that the cut-off criteria could be based on a suitable collection of finite progressive configurations. Showing the validity of the adapted verifier approach for weak diagnosability is the main contribution of the paper.

The efficiency of the unfolding-based construction - which is PSPACE-complete in general - hinges upon the size of the complete prefix, and thus upon the wise choice of cut-off context. Here, a very conservative adequate order was chosen, which orders configurations merely by inclusion; exploring more sophisticated ordering relations can be a source of important space reductions. Future work will explore different choices of such cutting contexts adapted to the weak diagnosability setting.

More generally, there is room to explore further improvements in the exploration and storage of $\mathbf{V}$. In fact, the prefixes proposed above tend to have greater width that those obtained with prime configuration-based cutting criteria. We will strive to identify efficient techniques for pruning away unnecessary branches at as early a stage as possible.

Another approach to partial observation in concurrent systems, which has been introduced in Haar (2007, 2009, 2010a,b), consists in looking for inevitable occurrences that are revealed by observation, regardless of the possible time for occurrence (which may be concurrent with the observation, with no synchronization). Knowledge of such relations in the system allows to raise alarms and start countermeasures as soon as the threat becomes apparent, without waiting for evidence of its actual occurrence.

Acknowledgments: This work was partly supported by the European Community’s 7th Framework Programme under project DISC (Distributed Supervisor Control of large plants), Grant Agreement INFSO-ICT-224498, the Fondecyt project No. 11090257, and the ARCUS project "Ile de France/Inde", conv. F-68-1309/R.

REFERENCES


