12th IFAC/IEEE Workshop on Discrete Event Systems
Cachan, France. May 14-16, 2014

Discriminability Analysis of Supervision Patterns by Net Unfoldings

Houssam-Eddine Gougam * **Audine Subias** * **Yannick Pencolé** †

* *CNRS; LAAS; 7 avenue du Colonel Roche, F-31400 Toulouse, France*
Univ de Toulouse, INSA, LAAS, F-31400 Toulouse, France
† *CNRS; LAAS; 7 avenue du Colonel Roche, F-31400 Toulouse, France*
Univ de Toulouse, LAAS, F-31400 Toulouse, France

Abstract: In this paper, we are interested in the discriminability of supervision patterns, in discrete event systems (DES). Discriminability — as opposed to diagnosability — is the possibility to detect the *exclusive* occurrence of a particular behavior of interest — called the supervision pattern. To this end, we propose to adapt the classical twin-plant approach to Petri nets unfolding. The usage of unfoldings permits us to avoid the combinatorial explosion associated with marking graphs. The method can also be used to solve the classical problem of discrete event systems' diagnosability.

Keywords: discriminability, diagnosability, supervision patterns, labeled Petri nets, Petri nets unfolding.

1. INTRODUCTION

In the context of discrete-event systems (DES), the supervision task consists in analyzing the sequence of observed events and determining whether an abnormal/faulty situation has occurred before deciding what kind of actions to perform in order to recover the optimal performance of the system. By the intrinsic nature of DES, an abnormal situation is characterized by a partial order of observable/non-observable events called an *event pattern* or a *supervision pattern* as introduced in Jéron et al. (2006).

In this paper, we address the problem of analysing the discriminability of a set of supervision patterns. Two supervision patterns $\mathcal{R}_1$ and $\mathcal{R}_2$ are discriminable if it is always possible to assert from the observed events that if $\mathcal{R}_1$ (resp. $\mathcal{R}_2$) has occurred then $\mathcal{R}_2$ (resp. $\mathcal{R}_1$) has not occurred and will not occur.

The notion of pattern discriminability is obviously related to the notion of pattern diagnosability and their respective analyses (Jiang et al. (2003), Jéron et al. (2006), Yoo and Garcia (2008), Gougam et al. (2013)), however the point of view is different. The result of a diagnosability analysis states whether any considered pattern is always detectable or not. If such a property holds then it is possible to design a diagnoser that will always be able to determinate which patterns have occurred in a finite amount of time. However there is a pitfall: underlying real-world systems are not and cannot be diagnosable as the diagnosability property is very restrictive (Pencolé (2005)) and requires an observability level that cannot be implemented as a set of sensors on the underlying system (physical and/or cost constraints). The classical diagnosability analyses will then conclude such a real-world system is not diagnosable, so what is next?

To cope with this problem, we propose to develop a more constructive analysis by checking the discriminability of the occurrence of a set of patterns with respect to another disjoint set of patterns. The analysis is constructive in the sense that any partial discriminability result has an outcome that can impact the design of a diagnoser for the analysed system even if the underlying system is not globally diagnosable. And finally, once the proposed discriminability analysis is completed, checking the classical diagnosability analysis is straightforward and for free.

In our proposal, the development of the discriminability analysis relies on two original choices. The first one is the use of Petri net — which were shown to be more appropriate to solve diagnosis problems Lai et al. (2008) — to model patterns as well as the system (Basile et al. (2009), Dotoli et al. (2009)) so that we benefit of the natural way to represent event concurrency. The second one is the use of net unfoldings (McMillan (1995), Esparza et al. (2002), Benveniste et al. (2003)) in order to benefit of a representation as a partial order of events. Unfoldings avoid the explicit enumeration of event sequences that is performed by techniques based on marking graphs like in Cabasino et al. (2012). Our proposed approach allows us to have some interesting properties. First, genericness, meaning that we do not impose particular patterns, we rather define a generic framework for supervision pattern, and every pattern falling in this framework can be used for supervision. Second, the supervision patterns are compact, i.e. only relevant events are included leading to more concise patterns. Finally, reusability, which is a direct consequence of the compactness, the exclusive use of relevant events yields supervision patterns which are independent from the system.

The paper is organized as follows. Section 2 introduces the problem, Section 3 presents Petri nets and their use to model the system and the patterns. The proposed analysis method is detailed in Sections 4 and 5. An example of our method is given in Section 6. Finally, we conclude in Section 7 and give some perspectives.

2. DISCRIMINABILITY OF SUPERVISION PATTERNS

Analyzing the discriminability of a system in the DES context means characterizing the performances of the diagnosis algorithm. A diagnosis algorithm, given an observable sequence produced by the system, is responsible of returning its state, i.e. is the system in a *normal* state or a *faulty* state, and in the latter case, which — faulty — behavior yielded this state. If such algorithm exists, and can determine with *certainty* after a *bounded* number of observations that *only* a particular combination of behaviors occurred, this combination is said to be *discriminable*. On the other hand, if the algorithm can detect the occurrence of a behavior with no information about the possible occurrence of other faulty behaviors, the former is said to be *detectable*.

In this paper, we consider a system modeled by a *language*, faulty behaviors are recognized by *supervision patterns* which are also languages with specific properties. More formally, the problem of supervision pattern discriminability in discrete event systems is then defined in the following context.

Let $\Sigma = \{a, b, \ldots\}$ be a finite set called an alphabet. The Kleene closure of Σ denoted Σ^* is the set of finite sequences — or words — over Σ — including the empty sequence, denoted in the following by λ. $\Sigma^+ = \Sigma^* \setminus \{\lambda\}$ is the set of non-empty finite sequences. A subset $\mathcal{S} \subseteq \Sigma^*$ is called a *language* over Σ. The continuation z of a sequence w in $\mathcal{S}$ is a sequence such that $wz \in \mathcal{S}$. So, the set of w's continuations in $\mathcal{S}$ is defined as $\mathcal{S}/w = \{z \in \Sigma^* : wz \in \mathcal{S}\}$. The classical projection of a sequence $w \in \Sigma^*$ on a subset Σ_p of Σ is denoted $\mathcal{P}_{\Sigma_p}(w)$. Finally, $\|w\|$ denotes the length of the sequence w. The behavior of the system is modeled by the prefix-closed language $\mathcal{S}$ over an alphabet Σ representing the set of events generated by the system. Some of these events are observable, while others are not. The observable events are represented by the set Σ_o and the set of non-observable events is called Σ_u. So, $\Sigma = \Sigma_o \cup \Sigma_u$. We make the assumption that the system is Σ_o-alive, meaning: $\forall w \in \mathcal{S}, \exists z \in \mathcal{S}/w : \mathcal{P}_{\Sigma_o}(z) \neq \lambda$; this hypothesis ensures that the system produces observations with some regularity. A supervision pattern $\mathcal{R}$ is a language over $\Sigma_{\mathcal{R}} \subseteq \Sigma$ that recognizes $\mathcal{R}$-faulty sequences.

Definition 1. Let $\mathfrak{R} = \{\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_n\}$ be a set of supervision patterns. A sequence $w \in \Sigma^*$ is said to be $\mathcal{R}_i$-faulty if: $\mathcal{P}_{\Sigma_{\mathcal{R}_i}}(w) \in \mathcal{R}_i$. A sequence $w \in \Sigma^*$ is said to be $\mathfrak{R}$-faulty if: $\forall \mathcal{R} \in \mathfrak{R} : w$ is $\mathcal{R}$-faulty. A sequence $w \in \Sigma^*$ is said to be faulty if: $\exists \mathcal{R} \in \mathfrak{R} : w$ is $\mathcal{R}$-faulty.

Definition 2. Let $\mathfrak{R} = \{\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_n\}$ be a set of supervision patterns. Let $\mathfrak{R}^s \in 2^{\mathfrak{R}}$ be a subset of $\mathfrak{R}$. A sequence $w \in \Sigma^*$ is said to be *exclusively* $\mathfrak{R}^s$-faulty in $\mathfrak{R}$ if: $\begin{cases} \forall \mathcal{R} \in \mathfrak{R}^s : w \text{ is } \mathcal{R}\text{-faulty} \\ \forall \mathcal{R} \notin \mathfrak{R}^s : w \text{ is not } \mathcal{R}\text{-faulty} \end{cases}$

We will simply use "exclusively $\mathfrak{R}^s$-faulty" rather than "exclusively $\mathfrak{R}^s$-faulty in $\mathfrak{R}$" when there is no ambiguity.

We can now define the discriminability of a set of supervision patterns.

Definition 3. Given a system $\mathcal{S}$ and a set of supervision patterns $\mathfrak{R} = \{\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_n\}$. A subset $\mathfrak{R}^s$ of $\mathfrak{R}$ is said to be discriminable if:

$\exists n \in \mathbb{N}, \forall w$ an exclusively $\mathfrak{R}^s$-faulty word of $\mathcal{S}, \forall z \in \mathcal{S}/w$:

$$\|\mathcal{P}_{\Sigma_o}(z)\| \geq n \implies D$$

where the discriminability condition D is:

$$\forall w^o \in \mathcal{P}_{\Sigma_o}^{-1}(\mathcal{P}_{\Sigma_o}(wz)) : w^o \text{ is exclusively } \mathfrak{R}^s\text{-faulty}$$

This property insures that one can detect with *certainty* that *only* a particular combination of patterns — namely $\mathfrak{R}^s$ — occurred.

Similarly, we define the $\mathfrak{R}$-diagnosability of a system.

Definition 4. Let $\mathfrak{R} = \{\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_n\}$ be a set of supervision patterns. A language $\mathcal{S}$ is $\mathfrak{R}$-diagnosable if:

$(\forall \mathcal{R} \in \mathfrak{R})(\exists n \in \mathbb{N}), \forall w$ an $\mathcal{R}$-faulty word of $\mathcal{S}, \forall z \in \mathcal{S}/w$:

$$\|\mathcal{P}_{\Sigma_o}(z)\| \geq n \implies D$$

where the diagnosability condition D is:

$$\forall w^o \in \mathcal{P}_{\Sigma_o}^{-1}(\mathcal{P}_{\Sigma_o}(wz)) : w^o \text{ is } \mathcal{R}\text{-faulty}$$

More intuitively, a language $\mathcal{S}$ is $\mathfrak{R}$-diagnosable if it does not contain two arbitrary long sequences, the first $\mathcal{R}$-faulty, the second non $\mathcal{R}$-faulty, which have the same observable behavior.

3. ON MODELING ASPECTS

To tackle the problem of discriminability, we propose to use labeled Petri nets to model the system and the patterns.

3.1 Labeled Petri nets

Definition 5. A *labeled Petri net* is a tuple $\langle P, T, A, \ell, L, \Sigma \rangle$ where:

- P: a set of places;
- T: a set of transitions with $P \cap T = \varnothing$;
- $A \subseteq (P \times T) \cup (T \times P)$: a binary relation representing arcs between nodes;
- $\ell : P \cup T \to L \cup \Sigma \cup \{\lambda\}$: a labeling function where L is the set of place labels, Σ is the set of transition labels and λ denotes the empty sequence.
  ℓ is naturally extended to markings and sequences of nodes. Let M be a marking: $\ell(M) = \{\ell(p) : p \in M\}$. For $s = s_1 s_2 \ldots \in (P \cup T)^*$, $\ell(s) = \ell(s_1)\ell(s_2)\ldots$.

A *marking* M is a map from P to $\mathbb{N}$ which maps any place p to the number of tokens $M(p)$ contained in it. For the sake of simplicity, a marking may sometimes be denoted as a multiset. For instance, let $P = \{p_1, p_2, p_3\}$, the marking M such that $M(p_1) = 2, M(p_2) = 0$ and $M(p_3) = 1$ can be represented as $M = \{p_1, p_1, p_3\}$. A marked and labeled Petri net is a tuple $\Theta = \langle P, T, A, \ell, L, \Sigma, M_0 \rangle$ where $\langle P, T, A, \ell, L, \Sigma \rangle$ is a labeled Petri net and M_0 an initial marking. The current state of a Petri net is defined by its current marking. The set $\bullet t = \{p \in P : (p, t) \in A\}$ is the preset of t and $t\bullet = \{p \in P : (t, p) \in A\}$ is its postset (the preset $\bullet p$ and postset $p\bullet$ of a place p are similarly defined). The transition t is *firable* from a given marking M iff: $\forall p \in \bullet t : M(p) > 0$. Firing t leads to a new marking M' such that $M' = (M \setminus \bullet t) \cup t\bullet$ and which is denoted by $M \xrightarrow{t} M'$. A marking M is reachable if there exists a firing