Proceedings of 2018 IEEE 8th Annual International Conference
on CYBER Technology in Automation, Control, and Intelligent Systems
July 19-23, 2018, Tianjin, China

Robust Diagnosability and Robust Prognosability of Discrete-Event Systems Revisited

Xiang Yin and Shaoyuan Li

***Abstract*— In this paper, we revisit the verification of robust diagnosability and robust prognosability in the context of partially-observed discrete-event systems. In these problems, we assume that the actual system belongs to a set of possible models and the system is said to be robustly diagnosable (respectively, prognosable) if we can successfully detect (respectively, predict) the occurrences of fault events even if we do not know the actual model a priori. Previous algorithms for the verification of these two conditions require exponential complexity in the number of possible models. In the paper, we show that both robust diagnosability and robust prognosability can be tested in a *pairwise* manner. This observation leads to new approaches for the verification of these two conditions, which are polynomial in both the number of states and the number of possible models.**

I. Introduction

This paper is concerned with the problems of fault diagnosis and fault prognosis of Discrete-Event Systems (DES). In the fault diagnosis problem, the goal is to detect and isolate certain significant behaviors based on model-based inferencing driven by run-time observations, while in the fault prognosis problem, the goal is to predict certain fault behaviors and issue alarms before their occurrences. Due to their importance in many large-scale automated systems, these two problems have drawn considerable attention in the DES literature in the past years; see, e.g., some recent works [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19] and a comprehensive survey on fault diagnosis [20].

To handle uncertainty in real-world systems, in the analysis of DES, several different notions of *robustness* have been proposed. For example, in [21], [22], robustness under sensor failures was investigated. In [23], [24], the problem of fault diagnosis with incomplete model was studied. In [25], [26], [27], the reliability issue in decentralized fault diagnosis and prognosis was investigated. A more widely investigated source of uncertainty in DES is the *model uncertainty*. The model uncertainty issue was originally studied in the context of robust supervisory control [28], [29], [30], [31], [32]. In the context of fault diagnosis, in [33], the authors investigated the robust fault diagnosis problem in the presence of model uncertainty. In [34], a framework of robust fault prognosis was proposed in order to handle model uncertainty in the fault prognosis problem.

This work is supported by the National Nature Science Foundation of China (61590924, 61233004).

X. Yin and S. Li are with Department of Automation and Key Laboratory of System Control and Information Processing, Shanghai Jiao Tong University, Shanghai 200240, China. E-mail: yinxiang@sjtu.edu.cn, syli@sjtu.edu.

In this paper, we investigate the robust fault diagnosis and prognosis problems under model uncertainty in the framework of [33], [34], where it is assumed that we do not know precisely the actual system model and it belongs to a set of possible models. The goal is to detect (or predict) the occurrences of fault behaviors correctly no matter which model is true. It has been shown that the notion of robust diagnosability serves as the necessary and sufficient condition for the existence of a robust diagnoser against model uncertainty [33]. Similarly, the notion of robust prognosability was also proposed in [34] as the necessary and sufficient condition for the existence of a robust prognoser. Verification algorithms for robust diagnosability and robust prognosability were also provided in [33] and [34], respectively; both of them are polynomial in the number of states, but are exponential in the number of possible models as the product space of all possible models needs to be explored.

In this paper, we revisit the verification of robust diagnosability and robust prognosability in the framework of [33], [34]. The main contribution of this paper is to show that both of these two conditions can be verified in polynomial-time, not only in the number of states, but also in the number of all possible models. This result comes from a simple but very useful observation that both of these two conditions can be verified in a *pairwise* manner, rather than exploring the entire product space of all possible models. That is, to test whether or not a set of possible models is robustly diagnosable (respectively, robust prognosable), if suffices to test, for all pairs of models, whether or not a set of two possible models is robustly diagnosable (respectively, robust prognosable). Our results considerably improve the verification complexity of robust diagnosability and robust prognosability, in particular, when the number of possible models is relatively large.

The rest of this paper is organized as follows. In Section II, we present some necessary preliminaries and review the definitions of robust diagnosability and robust prognosability. Section III presents the main results of this paper, i.e., both robust diagnosability and robust prognosability can be verified in a pairwise manner. An illustrative example is provided in Section IV. Finally, we conclude the paper in Section V.

II. Preliminary

A. System Model

Let Σ be a finite set of events. We denote by Σ^* the set of all finite strings over Σ including the empty string ϵ. We define $\Sigma_\epsilon = \Sigma \cup \{\epsilon\}$. A language $L \subseteq \Sigma^*$ is a set

978-1-5386-7057-6/18/$31.00 © 2018 IEEE

of strings. For any string $s \in L$, $|s|$ denotes its length; we define $L/s := \{t \in \Sigma^* : st \in L\}$.

A DES is modeled by a finite-state automaton

$$G = (Q, \Sigma, \delta, q_0) \tag{1}$$

where Q is a finite set of states, Σ is a finite set of events, $\delta : Q \times \Sigma \to Q$ is the partial deterministic transition function and q_0 is the initial state. Function δ is extended to $Q \times \Sigma^*$ in the usual manner [35]. For the sake of simplicity, hereafter, we write $\delta(q_0, s)$ by $\delta(s)$, i.e., $\delta(s)$ is the state reached by string s from the initial state. The language generated by G is $\mathcal{L}(G) = \{s \in \Sigma^* : \delta(s)!\}$, where "!" means "is defined". We also assume that G is live, i.e., $\forall q \in Q, \exists \sigma \in \Sigma : \delta(q, \sigma)!$.

The event set Σ is partitioned into two disjoint sets $\Sigma = \Sigma_o \dot{\cup} \Sigma_{uo}$, where Σ_o is the set of observable events and Σ_{uo} is the set of unobservable events. The natural projection $P : \Sigma^* \to \Sigma_o^*$ is defined recursively by:

$$P(\epsilon) = \epsilon \quad \text{and} \quad P(s\sigma) = \begin{cases} P(s)\sigma & \text{if } \sigma \in \Sigma_o \\ P(s) & \text{if } \sigma \in \Sigma_{uo} \end{cases} \tag{2}$$

Natural projection is also extended to $P : 2^{\Sigma^*} \to 2^{\Sigma_o^*}$ by: for any $L \subseteq \Sigma^* : P(L) = \{t \in \Sigma_o^* : \exists s \in L \text{ s.t. } P(s) = t\}$.

In the fault diagnosis/prognosis problem, the system is subject to fault. Specifically, we assume that the normal behavior of G is modeled by an automaton $G^N = (Q^N, \Sigma, \delta^N, q_0^N)$ such that $\mathcal{L}(G^N) \subseteq \mathcal{L}(G)$, i.e., any string in $\mathcal{L}(G) \setminus \mathcal{L}(G^N)$ is a fault string and any string in $\mathcal{L}(G^N)$ is a non-fault string. For the sake of simplicity and without loss of generality, we assume that G^N is a *sub-automaton* of G [35]. Under this assumption, for any string $s \in \mathcal{L}(G)$, s is a fault string if and only if $\delta(s) \notin Q^N \subseteq Q$.

For any state $q \in Q^N$, we say that q is a boundary state if $\exists \sigma \in \Sigma : \delta(q, \sigma) \notin Q^N$, i.e., a fault can occur from this state. We denote by $\partial(G^N) \subseteq Q^N$ the set of boundary states in G^N. We say that q is a non-indicator state if $\forall K \in \mathbb{N}, \exists s \in \mathcal{L}(G^N, q) : |s| \geq K$, i.e., an arbitrary long non-fault behavior can occur from this state. We denote by $\Upsilon(G^N) \subseteq Q^N$ the set of non-indicator states in G^N.

B. Robust Fault Diagnosis and Prognosis

In the context of robust fault diagnosis and prognosis, we do not know the system model precisely. Instead, we assume that the actual system belongs to a set of n possible models

$$\mathbb{G} = \{G_1, G_2, \ldots, G_n\} \tag{3}$$

where $G_i = (Q_i, \Sigma, \delta_i, q_{0,i}), i = 1, \ldots, n$. We denote by $\mathcal{I} = \{1, 2, \ldots, n\}$ the index set. For each model $G_i, i \in \mathcal{I}$, it has its own normal model $G_i^N = (Q_i^N, \Sigma, \delta_i^N, q_{0,i}^N)$.

In [33] (respectively, [34]), the condition of robust diagnosability (respectively, prognosability) was proposed as the necessary and sufficient condition for the existence of a robust diagnoser (respectively, prognoser) under model uncertainty. We recall these two conditions as follows.

Definition 1: (Robust Diagnosability [33]). The set of possible models $\{G_i : i \in \mathcal{I}\}$ is said to be robustly diagnosable if

$$\begin{aligned} &(\forall i \in \mathcal{I})(\exists K \in \mathbb{N})(\forall s \in \mathcal{L}(G_i) \setminus \mathcal{L}(G_i^N))(\forall t \in \mathcal{L}(G_i)/s) \\ &\text{s.t. } [|t| \geq K] \Rightarrow [\forall j \in \mathcal{I}, \forall w \in \mathcal{L}(G_j^N) : P(w) \neq P(st)] \end{aligned} \tag{4}$$

Intuitively, robust diagnosability requires that no matter what the actual model is, any fault string can be distinguished, in a finite number of steps, from any non-fault strings in any possible models; hence the fault can be detected unambiguously.

Definition 2: (Robust Prognosability [34]). The set of possible models $\{G_i : i \in \mathcal{I}\}$ is said to be robustly prognosable if

$$\begin{aligned} &(\forall i \in \mathcal{I})(\forall s \in \mathcal{L}(G_i^N) : \delta_i(s) \in \partial(G_i^N)) \\ &(\forall j \in \mathcal{I})(\forall t \in \mathcal{L}(G_j^N) : \delta_j(t) \in \Upsilon(G_j^N))[P(w) \neq P(s)] \end{aligned} \tag{5}$$

Intuitively, robust prognosability requires that no matter what the true model is, a string that leads to a boundary state can always be distinguished from any strings leading to non-indicator states in any possible models; hence a fault alarm can be issued unambiguously.

In [33], the verification of robust diagnosability has been studied. Under the assumption that G_i^N is a sub-automaton of G_i and the use of natural projection, the complexity of the existing verification algorithm is

$$O(n \cdot |\Sigma| \cdot \left(\sum_{i \in \mathcal{I}} |Q_i|\right) \cdot \left(\prod_{i \in \mathcal{I}} |Q_i^N|\right))$$

which is polynomial in the number of states in each model but is exponential in the number of all possible models due to the presence of the "$\prod$" term. The verification of robust prognosability has also been investigated in [34]; the complexity of the verification algorithm is

$$O(n \cdot |\Sigma| \cdot \left(\sum_{i \in \mathcal{I}} |Q_i^N|\right) \cdot \left(\prod_{i \in \mathcal{I}} |Q_i^N|\right))$$

, which is still exponential in the number of all possible models. In the next section, we will show how to improve the verification complexity by removing the "$\prod$" term.

III. Main Results

In this section, we present the main results of this paper. That is, both robust diagnosability and robust prognosability can be verified in a pairwise manner. Specifically, we show that to verify robust diagnosability (or robust prognosability) for the set of all possible models, it suffices to verify this condition for all pairs of two models.

A. Pairwise Verification of Robust Prognosability

We start by showing that robust prognosability can be verified in a pairwise manner as this notion is easier to deal with compared with robust diagnosability. We have the following main result.

Theorem 1: The set of all possible models $\{G_i : i \in \mathcal{I}\}$ is robustly prognosable, if and only if, for any $i, j \in \mathcal{I}$, the set of two models $\{G_i, G_j\}$ is robustly prognosable.

Proof: ($\Rightarrow$) By contraposition. Suppose that there exist $i, j \in \mathcal{I}$ such that $\{G_i, G_j\}$ is not robustly prognosable. This implies that

$$\begin{aligned}&(\exists i' \in \{i,j\})(\exists s \in \mathcal{L}(G_{i'}^N) : \delta_{i'}(s) \in \partial(G_{i'}^N))\\ &(\exists j' \in \{i,j\})(\exists t \in \mathcal{L}(G_{j'}^N)) : \delta_{j'}(t) \in \Upsilon(G_{j'}^N))\\ &[P(w) = P(s)]\end{aligned} \tag{6}$$

Since $\{i, j\} \subseteq \mathcal{I}$, then we know immediately that $\{G_i : i \in \mathcal{I}\}$ is not robustly prognosable.

($\Leftarrow$) By contraposition. Suppose that $\{G_i : i \in \mathcal{I}\}$ is not robustly prognosable, i.e.,

$$\begin{aligned}&(\exists i \in \mathcal{I})(\exists s \in \mathcal{L}(G_i^N) : \delta_i(s) \in \partial(G_i^N))\\ &(\exists j \in \mathcal{I})(\exists t \in \mathcal{L}(G_j^N)) : \delta_j(t) \in \Upsilon(G_j^N))[P(w) = P(s)]\end{aligned} \tag{7}$$

Let i and j be two models satisfying Equation (7). Since the first four quantifiers in Equation (7) are all existential, we can replace $\mathcal{I}$ in Equation (7) by $\{i, j\}$. Therefore, we know that $\{G_i, G_j\}$ is not robustly prognosable. ■

Theorem 1 suggests immediately an improved approach for the verification of robust prognosability. That is, we consider all possible sets of two models $\{G_i, G_j\}$ (including the case of $i = j$) and verify whether or not $\{G_i, G_j\}$ is robustly prognosable by the algorithm in [34]. If there exists such a pair of models that is not robustly prognosable, then the set of all models is not robustly prognosable; otherwise, by Theorem 1, the set of all models is robustly prognosable. This approach is summarized as Algorithm 1.

Algorithm 1 Polynomial Test for Robust Prognosability

1: **for all** $i = 1, \ldots, n$ **do**
2: **for all** $j = i, \ldots, n$ **do**
3: Test whether or not $\{G_i, G_j\}$ is not robustly prognosable by the algorithm in [34]
4: **if** $\{G_i, G_j\}$ is not robustly prognosable **then**
5: **return** "$\{G_i : i \in \mathcal{I}\}$ is not robustly prognosable"
6: **end if**
7: **end for**
8: **end for**
9: **return** "$\{G_i : i \in \mathcal{I}\}$ is robustly prognosable"

For a set of two possible models $\{G_i, G_j\}$, recall that verifying robust prognosability by the algorithm in [34] requires

$$O(|\Sigma| \cdot |Q_i^N| \cdot |Q_j^N| \cdot \big(|Q_i^N| + |Q_j^N|\big))$$

Moreover, we only need to repeat this procedure for $n(n+1)/2$ times. Therefore, the overall complexity of Algorithm 1 is

$$O(|\Sigma| \cdot \sum_{i,j \in \mathcal{I}} \big(|Q_i^N| \cdot |Q_j^N| \cdot \big(|Q_i^N| + |Q_j^N|\big)\big))$$

which is polynomial not only in the number of states, but also in the number of all possible models.

B. Pairwise Verification of Robust Diagnosability

Hereafter, we show that robust diagnosability can also be verified in such a pairwise manner. However, showing this result is a little bit more difficult than the case of prognosability. As we can see in Equation (4), for any model $i \in \mathcal{I}$, the choice of model j that violates robust diagnosability may depend on the choice of integer $K \in \mathbb{N}$. To handle this technique issue, we first present a lemma that helps us to estimate the upper bound of K when the system is robustly diagnosable.

Lemma 1: Let G_i and G_j be two models. Let $s \in \mathcal{L}(G_i) \setminus \mathcal{L}(G_i^N)$ be a faulty string in G_i and $t \in \mathcal{L}(G_i)/s$ be its continuation such that $|t| \geq |Q_i| \cdot |Q_j|$. If there exists a string $w \in \mathcal{L}(G_j^N)$ such that $P(w) = P(st)$, then for any $K \in \mathbb{N}$,

$$(\exists t' \in \mathcal{L}(G_i)/s : |t'| \geq K)(\exists w' \in \mathcal{L}(G_j^N))[P(w') = P(st')] \tag{8}$$

Proof: Since $P(w) = P(st)$, for string $w \in \mathcal{L}(G_j)$, we can write it by $w = w_1 w_2$ such that $P(w_1) = P(s)$ and $P(w_2) = P(t)$. Therefore, there exists a string of pairs of events

$$\underbrace{(\alpha_1^1, \alpha_1^2)(\alpha_2^1, \alpha_2^2)\ldots(\alpha_m^1, \alpha_m^2)}_{=:\alpha}\underbrace{(\beta_1^1, \beta_1^2)(\beta_2^1, \beta_2^2)\ldots(\beta_l^1, \beta_l^2)}_{=:\beta} \in (\Sigma_\epsilon \times \Sigma_\epsilon)^* \tag{9}$$

such that

$$s = \alpha_1^1 \ldots \alpha_m^1, w_1 = \alpha_1^2 \ldots \alpha_m^2, t = \beta_1^1 \ldots \beta_l^1, w_2 = \beta_1^2 \ldots \beta_l^2 \tag{10}$$

and

$$[\forall k \leq m : P(\alpha_k^1) = P(\alpha_k^2)] \wedge [\forall k \leq l : P(\beta_k^1) = P(\beta_k^2)] \tag{11}$$

Essentially, α and β are strings of event paris that are obtained by inserting ϵ in s, t, w_1 and w_2. This is similar to the well-known twin-machine construction.

For any $k = 1, \ldots, l$, we define

$$q_k^1 := \delta_i(s\beta_1^1 \ldots \beta_k^1) \in Q_i$$

and

$$q_k^2 := \delta_j(w_1\beta_1^2 \ldots \beta_k^2) \in Q_j$$

Let $0 \leq \theta_1 < \theta_2 < \cdots < \theta_{|t|} \leq l$ be the indices such that $\forall k = 1, \ldots, |t| : \beta_{\theta_k}^1 \neq \epsilon$. We know that there are $|t|$ such indices since $|\beta_1^1 \ldots \beta_l^1| = |t|$. Let us consider the follow multi-set

$$\mathcal{S} = \{(q_{\theta_1}^1, q_{\theta_1}^2), (q_{\theta_2}^1, q_{\theta_2}^2), \ldots, (q_{\theta_{|t|}}^1, q_{\theta_{|t|}}^2)\} \tag{12}$$

Since $|t| \geq |Q_i| \cdot |Q_j|$, we know that there are two repeated states in $\mathcal{S}$, say $(q_{\theta_a}^1, q_{\theta_a}^2) = (q_{\theta_b}^1, q_{\theta_b}^2)$, where $1 \leq a < b \leq |t|$.

Therefore, we know that, for any $K \in \mathbb{N}$, the following strings are well-defined

$$\begin{aligned}s\beta_1^1 \ldots \beta_{\theta_a}^1(\beta_{\theta_a+1}^1 \ldots \beta_{\theta_b}^1)^K \in \mathcal{L}(G_i)\\ w_1\beta_1^2 \ldots \beta_{\theta_a}^2(\beta_{\theta_a+1}^2 \ldots \beta_{\theta_b}^2)^K \in \mathcal{L}(G_j^N)\end{aligned}$$

Recall that $\forall k \leq l : P(\beta_k^1) = P(\beta_k^2)$. Therefore, we have

$$\begin{aligned}
&(\exists \underbrace{\beta_1^1 \dots \beta_{\theta_a}^1 (\beta_{\theta_a+1}^1 \dots \beta_{\theta_b}^1)^K}_{=:t'} \in \mathcal{L}(G_i)/s : |t'| \geq K) \\
&(\exists \underbrace{w_1 \beta_2^1 \dots \beta_{\theta_a}^2 (\beta_{\theta_a+1}^2 \dots \beta_{\theta_b}^2)^K}_{=:w'} \in \mathcal{L}(G_j^N)) \qquad (13) \\
&\text{s.t. } [P(w') = P(st')]
\end{aligned}$$

Note that, $|t'| \geq K$ comes from the fact that $\beta_{\theta_b}^1 \neq \epsilon$. ■

With the help of Lemma 1, we are now ready to show that robust diagnosability can also be tested in a pairwise manner.

Theorem 2: The set of all possible models $\{G_i : i \in \mathcal{I}\}$ is robustly diagnosable, if and only if, for any $i, j \in \mathcal{I}$, the set of two models $\{G_i, G_j\}$ is robustly diagnosable.

Proof: ($\Rightarrow$) By contraposition. Suppose that there exist $i, j \in \mathcal{I}$ such that $\{G_i, G_j\}$ is not robustly diagnosable. This implies that

$$\begin{aligned}
&(\exists i' \in \{i, j\})(\forall K \in \mathbb{N})(\exists s \in \mathcal{L}(G_{i'}) \setminus \mathcal{L}(G_{i'}^N)) \\
&(\exists t \in \mathcal{L}(G_{i'})/s) \qquad (14) \\
&\text{s.t. } [|t| \geq K] \wedge [\exists j' \in \{i, j\}, \exists w \in \mathcal{L}(G_{j'}^N) : P(st) = P(w)]
\end{aligned}$$

Since $\{i, j\} \subseteq \mathcal{I}$, then we know immediately that $\{G_i : i \in \mathcal{I}\}$ is not robustly diagnosable.

($\Leftarrow$) By contraposition. Suppose that $\{G_i : i \in \mathcal{I}\}$ is not robustly diagnosable, i.e.,

$$\begin{aligned}
&(\exists i \in \mathcal{I})(\forall K \in \mathbb{N})(\exists s \in \mathcal{L}(G_i) \setminus \mathcal{L}(G_i^N))(\exists t \in \mathcal{L}(G_i)/s) \\
&\text{s.t. } [|t| \geq K] \wedge [\exists j \in \mathcal{I}, \exists w \in \mathcal{L}(G_j^N) : P(st) = P(w)] \qquad (15)
\end{aligned}$$

Let $i \in \mathcal{I}$ be a model such that Equation (15) is satisfied. Let us choose K such that

$$K \geq |Q_i| \cdot \max_{j \in \mathcal{I}} \{|Q_j|\} \qquad (16)$$

Then, for the above K, there exist $s_K \in \mathcal{L}(G_i) \setminus \mathcal{L}(G_i^N)$ and $t_K \in \mathcal{L}(G_i)/s_K$ such that $|t_K| \geq K$ and there exists $j \in \mathcal{I}$ such that $\exists w \in \mathcal{L}(G_j^N) : P(s_K t_K) = P(w)$.

Let us consider the above string s_K and model $j \in \mathcal{I}$. Next, we show that $\{G_i, G_j\}$ is not robustly diagnosable. Since $|t_K| \geq K \geq |Q_i| \cdot |Q_j|$, by Lemma 1, we know that

$$\begin{aligned}
&(\forall K' \in \mathbb{N})(\exists t' \in \mathcal{L}(G_i)/s_K : |t'| \geq K')(\exists w' \in \mathcal{L}(G_j^N)) \\
&\text{s.t. } [P(w') = P(s_K t')] \qquad (17)
\end{aligned}$$

Therefore, we have that

$$\begin{aligned}
&(\exists i \in \{i, j\})(\forall K' \in \mathbb{N})(\exists s_K \in \mathcal{L}(G_i) \setminus \mathcal{L}(G_i^N)) \\
&(\exists t' \in \mathcal{L}(G_i)/s_K) \qquad (18) \\
&\text{s.t. } [|t'| \geq K'] \wedge [\exists j \in \{i, j\}, \exists w' \in \mathcal{L}(G_j^N) : P(w') = P(s_K t')]
\end{aligned}$$

That is, $\{G_i, G_j\}$ is not robustly diagnosable. ■

Similar to the case of robust prognosability, Theorem 2 also suggests a direct way to improve the verification complexity of robust diagnosability. That is, we consider all possible sets of two models $\{G_i, G_j\}$ (including the case of $i = j$) and verify whether or not $\{G_i, G_j\}$ is robustly diagnosable using the algorithms in [33]. Then, by Theorem 2, the set of all models is not robustly prognosable if and only if one such a pair of models is not robustly diagnosable. This approach is summarized as Algorithm 2.

Algorithm 2 Polynomial Test for Robust Diagnosability

```
for all i = 1, ..., n do
    for all j = i, ..., n do
        Test whether or not is {G_i, G_j} is robustly diagonsable by the algorithm in [33]
        if {G_i, G_j} is not robustly diagonsable then
            return "{G_i : i∈I} is not robustly diagonsable"
        end if
    end for
end for
return "{G_i : i ∈ I} is robustly diagonsable"
```

Recall that, for a set of two possible models $\{G_i, G_j\}$, verifying robust diagnosability by the algorithm in [33] requires

$$O(|\Sigma| \cdot |Q_i^N| \cdot |Q_j^N| \cdot (|Q_i| + |Q_j|))$$

Also, we only need to repeat this procedure for $n(n+1)/2$ times. Therefore, the complexity of Algorithm 2 is

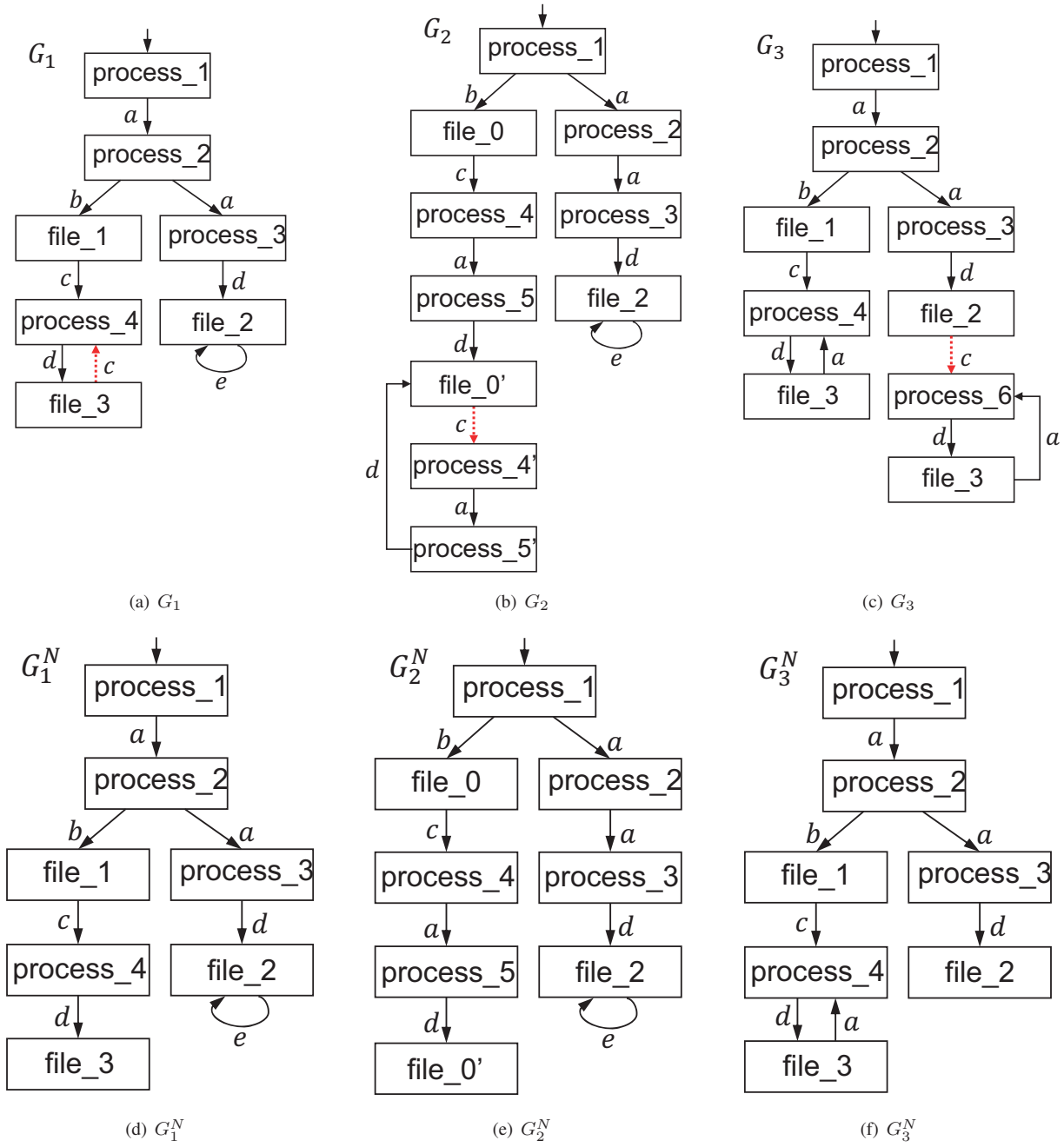
$$O(|\Sigma| \cdot \sum_{i,j \in \mathcal{I}} \left(|Q_i^N| \cdot |Q_j^N| \cdot (|Q_i| + |Q_j|)\right))$$

which is polynomial in both the number of states and the number of all possible models.

IV. Illustrative Example

In this section, we illustrate our main results by an example adopted from [1], [34].

Dependency graph (DG) is a technique used in operation systems that records the commands issued via a log file. In a DG, there are two types of states, PROCESSES and FILES, and transitions between states define the dependencies of the command issued. Let us consider an operation system with three possible dependency graphs G_1, G_2 and G_3 shown in Figures 1(a), 1(b) and 1(c), respectively. In each system, events a, b, c, d, e represent CREATE, WRITE, READ, DELETE and BUSY, respectively. We require that, for each possible model, event d representing DELETE should not happen immediately after the occurrence of event c representing READ. Therefore, the normal behaviors G_1^N, G_2^N and G_3^N are shown in Figures 1(d), 1(e) and 1(f), respectively. Note that each G_i^N is a sub-automaton of G_i. Moreover, we assume that $\Sigma_o = \{b, c, e\}$ is the set of observable events. Then we are interested in whether or not $\{G_1, G_2, G_3\}$ is robustly prognosable. To see this, let us consider models G_1 and G_2 first. We can verify according to the algorithm in [34] that $\{G_1, G_2\}$ is robustly prognosable. However, if we consider models G_2 and G_3, then we have $\delta_2(aad) = \text{FILE\_2} \in \Upsilon(G_2^N)$ $\delta_3(aad) = \text{FILE\_2} \in \partial(G_2^N)$ and $P(aad) = P(aad)$.



(a) G_1 (b) G_2 (c) G_3

(d) G_1^N (e) G_2^N (f) G_3^N

Fig. 1: Three possible dependency graphs for an operation system.

Therefore, we know that $\{G_2, G_3\}$ is not robustly prognosable and by Theorem 1, we know that the entire system $\{G_1, G_2, G_3\}$ is not robustly prognosable.

V. Discussion and Conclusion

There are some other problems in the literature whose parameter structures are similar to the robust diagnosis/prognosis problem. One related problem is the decentralized diagnosis/prognosis problem [36], [4], where a set of local agents is involved. However, it has been shown that testing codiagnosability (or coprognosability) is PSPACE-hard in the number of local agents [6]. Another related problem is the modular diagnosis/prognosis problem [37], where the monolithic model is composed by a set of local modules. It has also been shown that testing diagnosability (or prognosability) for the monolithic model is PSPACE-hard in the number of modules [38].

As in the robust diagnosis and prognosis problems, the number of possible models is also a parameter, it is natural to ask whether or not these two problems are also PSPACE-hard or they have polynomial-time algorithms. Our paper provides positive answer to the above question. The positive results come from the fact that both robust diagnosability and robust prognosability can be verified in a pairwise

manner, which allows us to leverage existing algorithms to develop polynomial-time algorithms for verifying these two conditions. In the future, we will extend our results to supervisor control problem [39], [40], [41], [42], [43].

REFERENCES

[1] T. Jéron, H. Marchand, S. Genc, and S. Lafortune. Predictability of sequence patterns in discrete event systems. In *Proc. 17th IFAC World Congress*, pages 537–543, 2008.

[2] S. Genc and S. Lafortune. Predictability of event occurrences in partially-observed discrete-event systems. *Automatica*, 45(2):301–311, 2009.

[3] X. Yin and S. Lafortune. A general approach for solving dynamic sensor activation problems for a class of properties. In *54th IEEe Conference on Decision and Control*, pages 3610–3615. IEEE, 2015.

[4] R. Kumar and S. Takai. Decentralized prognosis of failures in discrete event systems. *IEEE Transactions on Automatic Control*, 55(1):48–59, 2010.

[5] X. Yin and S. Lafortune. Codiagnosability and coobservability under dynamic observations: Transformation and verification. *Automatica*, 61:241–252, 2015.

[6] F. Cassez. The complexity of codiagnosability for discrete event and timed systems. *IEEE Transactions on Automatic Control*, 57(7):1752–1764, 2012.

[7] D. Lefebvre. Fault diagnosis and prognosis with partially observed petri nets. *IEEE Transactions on S.M.C.: Systems*, 44(10):1413–1424, 2014.

[8] J. Chen and R. Kumar. Stochastic failure prognosability of discrete event systems. *IEEE Transactions on Automatic Control*, 60(6):1570–1581, 2015.

[9] X. Yin and Z. Li. Decentralized fault prognosis of discrete event systems with guaranteed performance bound. *Automatica*, 69:375–379, 2016.

[10] R. Ammour, E. Leclercq, E. Sanlaville, and D. Lefebvre. Fault prognosis of timed stochastic discrete event systems with bounded estimation error. *Automatica*, 82:35–41, 2017.

[11] X. Yin and S. Lafortune. Minimization of sensor activation in decentralized discrete event systems. *IEEE Transactions on Automatic Control*, 2018. DOI: 10.1109/TAC.2017.2783048.

[12] A. Watanabe, A. Leal, J. Cury, and M. de Queiroz. Safe controllability using online prognosis. *IFAC World Congress*, pages 12359–12365, 2017.

[13] R. Ammour, E. Leclercq, E. Sanlaville, and D. Lefebvre. Faults prognosis using partially observed stochastic petri-nets: an incremental approach. *Discrete Event Dynamic Systems*, pages 1–21, 2017.

[14] N. Ran, S. Wang, H. Su, and C. Wang. Fault diagnosis for discrete event systems modeled by bounded petri nets. *Asian Journal of Control*, 2017.

[15] Y. Tong, Z. Li, C. Seatzu, and A. Giua. Verification of state-based opacity using Petri nets. *IEEE Transactions on Automatic Control*, 62(6):2823–2837, 2017.

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

[17] N. Ran, H. Su, A. Giua, and C. Seatzu. Codiagnosability analysis of bounded Petri nets. *IEEE Transactions on Automatic Control*, 2017.

[18] X. Yin and Z. Li. Decentralized fault prognosis of discrete-event systems using state-estimate-based protocols. *IEEE Transactions on Cybernetics*, 2018. DOI: 10.1109/TCYB.2018.2799961.

[19] X. Yin. Verification of prognosability for labeled Petri nets. *IEEE Transactions on Automatic Control*, 63(6):1738–1744, 2018.

[20] J. Zaytoon and S. Lafortune. Overview of fault diagnosis methods for discrete event systems. *Annual Reviews in Control*, 37(2):308–320, 2013.

[21] L.K. Carvalho, M.V. Moreira, J.C. Basilio, and S. Lafortune. Robust diagnosis of discrete-event systems against permanent loss of observations. *Automatica*, 49(1):223–231, 2013.

[22] N. Kanagawa and S. Takai. Diagnosability of discrete event systems subject to permanent sensor failures. *International Journal of Control*, 88(12):2598–2610, 2015.

[23] R.H. Kwong and D.L. Yonge-Mallo. Fault diagnosis in discrete-event systems: Incomplete models and learning. *IEEE Transactions on S.M.C., Part B*, 41(1):118–130, 2011.

[24] R.H. Kwong and D.L. Yonge-Mallo. Fault diagnosis in discrete-event systems with incomplete models: Learnability and diagnosability. *IEEE Transactions on Cybernetics*, 45(7):1236–1249, 2015.

[25] J.C. Basilio and S. Lafortune. Robust codiagnosability of discrete event systems. In *American Control Conference*, pages 2202–2209, 2009.

[26] S. Nakata and S. Takai. Reliable decentralized failure diagnosis of discrete event systems. *SICE Iournal of Control, Measurement, and System Integration*, 6(5):353–359, 2013.

[27] X. Yin and Z. Li. Reliable decentralized fault prognosis of discrete-event systems. *IEEE Transactions on S.M.C.: Systems*, 46(11):1598–1603, 2016.

[28] F. Lin. Robust and adaptive supervisory control of discrete event systems. *IEEE Transactions on Automatic Control*, 38(12):1848–1852, 1993.

[29] S. Takai. Robust supervisory control of a class of timed discrete event systems under partial observation. *Systems & Control Letters*, 39(4):267–273, 2000.

[30] S.E. Bourdon, M. Lawford, and W.M. Wonham. Robust nonblocking supervisory control of discrete-event systems. *IEEE Transactions on Automatic Control*, 50(12):2015–2021, 2005.

[31] A. Saboori and S.H. Zad. Robust nonblocking supervisory control of discrete-event systems under partial observation. *Systems & Control Letters*, 55(10):839–848, 2006.

[32] F. Wang, S. Shu, and F. Lin. Robust networked control of discrete event systems. *IEEE Transactions on Autom. Sci. Engineering*, 13(4):1528–1540, 2016.

[33] S. Takai. Verification of robust diagnosability for partially observed discrete event systems. *Automatica*, 48(8):1913–1919, 2012.

[34] S. Takai. Robust prognosability for a set of partially observed discrete event systems. *Automatica*, 51:123–130, 2015.

[35] C. Cassandras and S. Lafortune. *Introduction to Discrete Event Systems*. Springer, 2nd edition, 2008.

[36] R. Debouk, S. Lafortune, and D. Teneketzis. Coordinated decentralized protocols for failure diagnosis of discrete event systems. *Discrete Event Dynamic Systems: Theory & Applications*, 10(1):33–86, 2000.

[37] O. Contant, S. Lafortune, and D. Teneketzis. Diagnosability of discrete event systems with modular structure. *Discrete Event Dynamic Systems: Theory & Applications*, 16(1):9–37, 2006.

[38] X. Yin and S. Lafortune. Verification complexity of a class of observational properties for modular discrete events systems. *Automatica*, 83:199–205, 2017.

[39] X. Yin and S. Lafortune. Synthesis of maximally permissive supervisors for partially-observed discrete-event systems. *IEEE Transactions on Automatic Control*, 61(5):1239–1254, 2016.

[40] X. Yin and S. Lafortune. A uniform approach for synthesizing property-enforcing supervisors for partially-observed discrete-event systems. *IEEE Transactions on Automatic Control*, 61(8):2140–2154, 2016.

[41] X. Yin. Supervisor synthesis for mealy automata with output functions: A model transformation approach. *IEEE Transactions on Automatic Control*, 62(5):2576–2581, 2017.

[42] X. Yin and S. Lafortune. Synthesis of maximally-permissive supervisors for the range control problem. *IEEE Transactions on Automatic Control*, 62(8):3914–3929, 2017.

[43] X. Yin and S. Lafortune. Synthesis of maximally-permissive non-blocking supervisors for the lower-bound containment problem,. *IEEE Transactions on Automatic Control*, 2018. DOI: 10.1109/TAC.2018.2828098.