Automatica 101 (2019) 290–295

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Brief paper

Complexity of detectability, opacity and A-diagnosability for modular discrete event systems ☆

Tomáš Masopust [a,*], Xiang Yin [b,c]

[a] Department of Computer Science, Faculty of Science, Palacky University, Olomouc, Czechia
[b] Department of Automation, Shanghai Jiao Tong University, Shanghai 200240, China
[c] Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai 200240, China

ARTICLE INFO

Article history:
Received 3 October 2017
Received in revised form 8 September 2018
Accepted 6 December 2018
Available online xxxx

Keywords:
Discrete event systems
Finite automata
Detectability
Opacity
A-diagnosability
Complexity

ABSTRACT

Modular discrete event systems are modeled as a parallel composition of finite automata. While deciding weak detectability, opacity, and A-diagnosability for monolithic systems is PSPACE-complete, the complexity for modular systems is unknown. We show that for modular systems the problems are EXPSPACE-complete, and hence there is neither a polynomial-time nor a polynomial-space algorithm solving them. While the upper bound is a natural modification of the PSPACE algorithms for monolithic systems, the lower bound requires a novel and nontrivial construction. We further discuss a case where the complexity drops to PSPACE-complete.

1. Introduction

Discrete event systems (DES) are dynamical systems with discrete state spaces and event-triggered dynamics. In most applications, DES models consist of local modules, modeled as finite automata, running synchronously. This leads to the research on modular DES, where the challenge is the state-space explosion problem (the number of states in the monolithic model grows exponentially with the number of modules). Understanding the computational complexity is essential for the analysis of modular DES that has drawn considerable attention in the literature. Among others, Gohari and Wonham (2000) and Rohloff and Lafortune (2005) investigated the complexity of supervisory control problems for modular DES, Yin and Lafortune (2017) the complexity of verification of diagnosability, detectability and predictability, and Masopust (2017) the complexity of nonblockingness. Many problems tractable for monolithic DES are intractable for modular DES due to the state explosion issue, although the issue itself is not sufficient for intractability. There are many results on tractable solutions for problems of modular DES, see Feng and Wonham (2008), Gummadi, Singh, and Sreenivas (2011), Hill, Cury, de Queiroz, Tilbury, and Lafortune (2010), Komenda, Masopust, and van Schuppen (2014), Leduc, Lawford, and Wonham (2005), Saboori and Hadjicostis (2010) and Schmidt and Cury (2012).

Detectability, opacity, and diagnosability are important system-theoretic properties of DES. Detectability defined in Shu, Lin, and Ying (2007) arises in state estimation and asks whether the current state of the system can be determined unambiguously after a finite number of observations. Detectability is closely related to opacity, a property of interest in the privacy and security analysis, see Jacob, Lesage, and Faure (2016). The system has a secret modeled as a set of states and an intruder is modeled as a passive observer with limited observations. The system is opaque if the intruder never knows for sure that the system is in a secret state. Diagnosability defined in Sampath, Sengupta, Lafortune, Sinnamohideen, and Teneketzis (1995) is another important task requiring that an occurrence of a fault can always be detected within a finite delay. A-diagnosability is a relaxation of diagnosability requiring that there always exists a possibility to detect the fault. For more details, Jacob et al. (2016) give an overview of opacity in DES, and Zaytoon and Lafortune (2013) of fault diagnosis.

Deciding weak detectability, opacity, and A-diagnosability is PSPACE-complete for monolithic DES as shown in Bertrand, Haddad, and Lefaucheux (2014), Cassez, Dubreil, and Marchand (2012), Chen, Keroglou, Hadjicostis, and Kumar (2018), Masopust (2018), Zhang (2017), and hence the problems are polynomially reducible to each other. In particular, Lin (2011) gives links among opacity,

☆ T. Masopust was supported by the GAČR, Czechia project GA15-02532S and by RVO 67985840. X. Yin was supported by the National Natural Science Foundation of China (61803259, 61833012). The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Christoforos Hadjicostis under the direction of Editor Christos G. Cassandras.

* Corresponding author.
E-mail addresses: tomas.masopust@upol.cz (T. Masopust), yinxiang@sjtu.edu.cn (X. Yin).

https://doi.org/10.1016/j.automatica.2018.12.019
0005-1098/

anonymity, secrecy, observability, diagnosability, and detectability.

For modular DES, the complexity is open. Indeed, the modular problems are PSPACE-hard and a natural modification of the monolithic results gives that they are in EXPSPACE. However, do they belong to PSPACE or are they EXPSPACE-hard? We show, using a novel and nontrivial construction, that the modular problems are EXPSPACE-hard, and hence EXPSPACE-complete. Consequently, there is neither a polynomial-time nor a polynomial-space algorithm verifying the modular properties. Our results are obtained in a uniform manner in the sense that a similar construction is used. In particular, A-diagnosability may seem different from weak detectability and opacity at the first glance. Note that Saboori and Hadjicostis (2010) present an algorithm checking modular opacity in exponential time under some restrictions. However, our results show that there is unlikely an exponential-time algorithm in general.

We also discuss the case where unobservable events are private. In this case, the projection commutes with parallel composition, and the modular problems can be reduced to the composition of monolithic problems. The complexity thus drops to PSPACE-complete.

2. Preliminaries and definitions

For a set A, $|A|$ denotes the cardinality of A and 2^A its power set. An *alphabet* Σ is a finite nonempty set of *events*. A *word* over Σ is a sequence of events. Let Σ^* denote the set of all finite words over Σ; the *empty word* is denoted by ε. For a word $u \in \Sigma^*$, $|u|$ denotes its length. As usual, Σ^+ stands for $\Sigma^* \setminus \{\varepsilon\}$.

A *nondeterministic finite automaton* (NFA) over an alphabet Σ is a structure $A = (Q, \Sigma, \delta, I, F)$, where Q is a finite nonempty set of states, $I \subseteq Q$ is a nonempty set of initial states, $F \subseteq Q$ is a set of marked states, and $\delta\colon Q \times \Sigma \to 2^Q$ is a transition function that can be extended to the domain $2^Q \times \Sigma^*$ by induction. The *language generated by A* is the set $L(A) = \{w \in \Sigma^* \mid \delta(I, w) \neq \emptyset\}$ and the *language recognized by A* is the set $L_m(A) = \{w \in \Sigma^* \mid \delta(I, w) \cap F \neq \emptyset\}$.

A *discrete event system* (DES) is modeled as an NFA G with all states marked. Therefore we simply write $G = (Q, \Sigma, \delta, I)$ without specifying the marked states. The alphabet Σ is partitioned into two subsets Σ_o and $\Sigma_{uo} = \Sigma \setminus \Sigma_o$ called the set of *observable* and *unobservable* events, respectively.

The problems under investigation are based on the observation of events described by a projection $P\colon \Sigma^* \to \Sigma_o^*$. The *projection* P is a morphism defined by $P(a) = \varepsilon$ for $a \in \Sigma \setminus \Sigma_o$, and $P(a) = a$ for $a \in \Sigma_o$. The action of P on a word $\sigma_1\sigma_2\cdots\sigma_n$ with $\sigma_i \in \Sigma$ for $1 \leq i \leq n$ is to erase all events that do not belong to Σ_o; namely, $P(\sigma_1\sigma_2\cdots\sigma_n) = P(\sigma_1)P(\sigma_2)\cdots P(\sigma_n)$. The definition can readily be extended to infinite words and languages.

Let $G = (Q, \Sigma, \delta, I)$ be a DES, and let P be a projection from Σ to $\Delta \subseteq \Sigma$. We use the notation $P(G)$ to denote the DES $P(G) = (Q, \Delta, \delta', I)$, where the function $\delta' = \{(p, P(a), q) \mid (p, a, q) \in \delta\}$. Intuitively, $P(G)$ has the same structure as G with unobservable transitions labeled with ε.

As usual when partially-observed DES are studied, see Sampath et al. (1995) and Shu and Lin (2011), we assume that $G = (Q, \Sigma, \delta, I)$ is *deadlock free*, that is, the system can always make a transition: for every $q \in Q$, there is $\sigma \in \Sigma$ such that $\delta(q, \sigma) \neq \emptyset$.

A system G is often modeled as a parallel composition of a set of local modules $\{G_1, \ldots, G_n\}$, where G_i is a DES, i.e., $G = G_1 \| \cdots \| G_n$, where "$\|$" denotes the parallel composition operator (Cassandras & Lafortune, 2008, p. 78). We call such a system a *modular DES*.

A *decision problem* is a yes–no question. A decision problem is *decidable* if there is an algorithm solving it. Complexity theory classifies decidable problems into classes based on time or space an algorithm needs to solve the problem. Considered classes in this work are PSPACE and EXPSPACE denoting the classes of problems solvable by a deterministic polynomial-space algorithm and by a deterministic exponential-space algorithm, respectively. A decision problem is PSPACE-complete (EXPSPACE-complete) if it belongs to PSPACE (EXPSPACE) and every problem from PSPACE (EXPSPACE) can be reduced to it by a deterministic polynomial-time algorithm. By the space hierarchy theorem given in Stearns, Hartmanis, and Lewis I.I. (1965), PSPACE is a strict subclass of EXPSPACE. Thus, for an EXPSPACE-complete problem, there is neither a polynomial-space nor a polynomial-time algorithm.

3. Modular detectability

In this section, we investigate the complexity of deciding modular detectability. Let Σ be an alphabet, $\Sigma_o \subseteq \Sigma$ be the set of observable events, and P be the projection from Σ to Σ_o. Let $\mathbb{N}$ denote the set of all natural numbers. The set of infinite sequences of events generated by a DES G is denoted by $L^\omega(G)$. For $w \in L^\omega(G)$, we denote the set of its finite prefixes by $Pr(w)$.

By Shu et al. (2007), a DES $G = (Q, \Sigma, \delta, I)$ is *weakly detectable* with respect to Σ_{uo} if we can determine, after a finite number of observations, the current and subsequent states of the system for some trajectories, i.e.,

$$(\exists n \in \mathbb{N})(\exists s \in L^\omega(G))(\forall t \in Pr(s))[|P(t)| > n \Rightarrow |R_G(t)| = 1]\,,$$

where $R_G(t) = \{x \in Q \mid \exists\, t' \in L(G)$ such that $P(t) = P(t')$ and $x \in \delta(I, t')\}$, and it is *weakly periodically detectable* if we can periodically determine the current state of the system for some trajectories, i.e.,

$$(\exists n \in \mathbb{N})(\exists s \in L^\omega(G))(\forall t \in Pr(s))(\exists t' \in \Sigma^*)$$
$$[tt' \in Pr(s) \wedge |P(t')| < n \wedge |R_G(tt')| = 1]\,.$$

Given a modular DES $\{G_1, \ldots, G_n\}$ and a set of unobservable events Σ_{uo}. The *weak (periodic) modular detectability* problem asks whether $G_1 \| \cdots \| G_n$ is weakly (periodically) detectable with respect to Σ_{uo}.

Yin and Lafortune (2017) and Zhang (2017) showed that deciding weak modular detectability is PSPACE-hard and in EXPSPACE, but its complexity is open. PSPACE-hardness does not rule out polynomial-space solvability of the problem. We show that the problem requires exponential space. To this aim, we first formulate an auxiliary lemma.

Lemma 1. *Let Σ be an alphabet and $n \geq 1$ be an integer. There are n six-state automata A_i such that $P(L_m(\|_{i=1}^n A_i)) = \Sigma^{2^n-1}$ for P being a projection to Σ.*

Proof. Let $\Gamma = \{a_1, a_2, \ldots, a_n\}$. For $i = 1, \ldots, n$, we define the automaton $A_i = (\{0, 1, p, q, r, s\}, \Gamma, \delta_i, 0, \{1\})$ where

$$\delta_i = \{(0, a_j, p), (p, b, 0), (1, a_j, q), (q, b, 1) \mid j < i,\ b \in \Sigma\}$$
$$\cup\, \{(0, a_i, r), (r, b, 1) \mid b \in \Sigma\}$$
$$\cup\, \{(1, a_j, s), (s, b, 0) \mid j > i,\ b \in \Sigma\}\,,$$

see Fig. 1 or Masopust and Yin (2017, Example 9) for an illustration. Let $A = \|_{i=1}^n A_i$. Intuitively, A counts from 0 to $2^n - 1$ in binary; the initial state is $(0, 0, \ldots, 0)$ representing 0 in binary, which is modified step by step to state $(1, 1, \ldots, 1)$ representing $2^n - 1$ in binary (this explains why we write the composition from right to left). Every odd transition under an event from Γ is used to count the number of steps, and every even transition under an event from Σ is to give the required language Σ^{2^n-1} in the projection to Σ.

We prove by induction on $n \geq 1$ that $A_n \| \cdots \| A_1$ accepts a language $L_n \subseteq (\Gamma\Sigma)^{2^n-1}$ such that the projection of L_n to Γ is a singleton. For $n = 1$, $L_1 = \{a_1 b \mid b \in \Sigma\}$, and the claim holds.

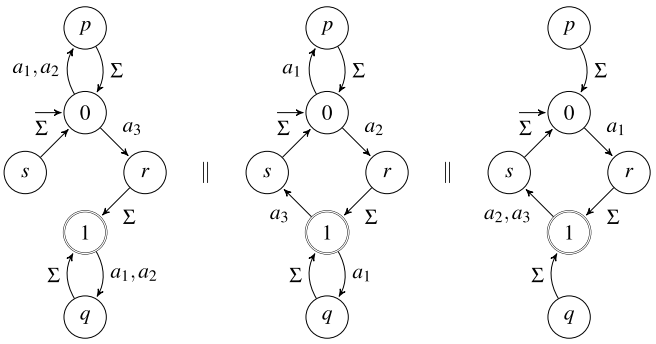

Fig. 1. Automaton $A = A_3 \| A_2 \| A_1$.

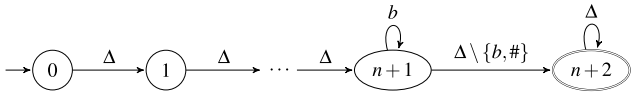

Fig. 2. An NFA for the subexpression $\Delta^{n+1} \cdot b^* \cdot (\Delta \setminus \{b, \#\}) \cdot \Delta^*$.

Assume that the claim holds for n, and prove it for $n+1$. In this case, $\Gamma = \{a_1, \ldots, a_n, a_{n+1}\}$. Let $w \in L_n$. Then w does not contain a_{n+1}, and the automaton A_{n+1} cycles between states 0 and p when reading w. Thus, in $A_{n+1} \| A_n \| \cdots \| A_1$, we have $(0, 0, \ldots, 0) \xrightarrow{w} (0, 1, \ldots, 1) \xrightarrow{w'} (1, 0, \ldots, 0) \xrightarrow{w} (1, 1, \ldots, 1)$, where $w' = a_{n+1} b$ for some $b \in \Sigma$, i.e., the projection of w' to Γ is the singleton $\{a_{n+1}\}$. The parallel composition therefore accepts the word $ww'w$, which is of the form $(\Gamma\Sigma)^{2^{n+1}-1}$, and where the projection of $ww'w$ to Γ is a unique word by the induction hypothesis. □

We now prove our main result.

Theorem 2. *Deciding weak (periodic) modular detectability is EXPSPACE-complete.*

Proof. Membership in EXPSPACE follows by adapting the membership in PSPACE for monolithic DES, see Masopust and Yin (2017) for more details.

To show EXPSPACE-hardness, we reduce the EXPSPACE-complete problem asking whether a regular expression with squaring is universal. A regular expression with squaring may use the usual operations $\cup$, $\cdot$, *, as well as the squaring operations $s^2 = s \cdot s$. Meyer and Stockmeyer (1972) showed that it is sufficient to consider an expression E over $\Delta = \{\#\} \cup T \cup Q \times T$, where T and Q are finite disjoint sets, of the form

$$((\Delta \setminus \#) \cup \# \cdot ((\Delta \setminus (q_o, x_1)) \cup (q_o, x_1) \cdot ((\Delta \setminus x_2)$$
$$\cup x_2 \cdot ((\Delta \setminus x_3) \cup \cdots (\Delta \setminus x_n))) \cdots) \cdot \Delta^* \quad (1)$$
$$\cup \Delta^{n+1} \cdot b^* \cdot (\Delta \setminus \{b, \#\}) \cdot \Delta^* \quad (2)$$
$$\cup \# \cdot (\Delta \cup \varepsilon)^{2^n-1} \cdot \# \cdot \Delta^* \quad (3)$$
$$\cup \# \cdot \Delta^{2^n} \cdot (\Delta \setminus \#) \cdot \Delta^* \quad (4)$$
$$\cup (\Delta \setminus (\cup_{t \in T}(q_a, t)))^* \quad (5)$$
$$\cup \bigcup_{c_1, c_2, c_3 \in \Delta} \Delta^* \cdot c_1 c_2 c_3 \cdot \Delta^{2^n-1} \cdot (\Delta \setminus N(c_1, c_2, c_3)) \cdot \Delta^* \quad (6)$$

where $q_o, q_a \in Q$, $x_1, \ldots, x_n \in T$, and $N(c_1, c_2, c_3) \subseteq \Delta$. The expression consists of unions of structurally simpler expressions, most of which can be translated to an NFA in polynomial time by a direct transformation. For instance, an NFA for subexpression (2) is depicted in Fig. 2.

However, the construction of an NFA is not easy for a subexpression E' that contains Δ^{2^n-1} (subexpressions (3), (4), and (6)), because the direct transformation would require $2^n - 1$ transitions labeled with events of Δ, which cannot be done in polynomial time. Instead, we construct a modular system H consisting of n NFAs $B_1, \ldots, B_n$ such that the language of H projected to Δ is $L(E')$, that is, $P(L_m(H)) = P(L_m(B_1 \| \ldots \| B_n)) = L(E')$. The core of the construction of $B_1, \ldots, B_n$ is formalized in Lemma 1.

For every subexpression of E, we now construct a (possibly modular) system G_i as follows. For (1), (2), and (5), NFAs G_1, G_2, and G_5 can directly be constructed, see Fig. 2.

For (3), we construct G_3 as a modular DES $\{B_1^3, \ldots, B_n^3\}$ such that $L_m(B_i^3) = \# \cdot L_m(A_i) \cdot \# \cdot \Delta^*$, where A_i is as in Lemma 1 over the alphabet $\Sigma \cup \Gamma_3$, where Γ_3 is a set of new events and $\Sigma = \Delta \cup \{e\}$ with e being a new unobservable event. Then, by Lemma 1, (3) is a projection to Δ of the composition $B_n^3 \| \cdots \| B_1^3$, that is, $P(L_m(B_n^3 \| \cdots \| B_1^3)) = \# \cdot (\Delta \cup \{\varepsilon\})^{2^n-1} \cdot \# \cdot \Delta^*$.

For (4), we construct G_4 as a modular DES $\{B_1^4, \ldots, B_n^4\}$ such that $L_m(B_i^4) = \# \cdot \Delta \cdot L_m(A_i) \cdot (\Delta \setminus \#) \cdot \Delta^*$, where A_i is as in Lemma 1 over the alphabet $\Sigma \cup \Gamma_4$, where Γ_4 is a set of new events (in particular, $\Gamma_3 \cap \Gamma_4 = \emptyset$) and $\Sigma = \Delta$. Then, by Lemma 1, we have that $P(L_m(B_n^4 \| \cdots \| B_1^4)) = \# \cdot \Delta \cdot \Delta^{2^n-1} \cdot (\Delta \setminus \#) \cdot \Delta^*$.

For (6), we construct $|\Delta|^3$ modular DES $G_{c_1c_2c_3}$. Namely, for every triple $c_1c_2c_3$, we construct $G_{c_1c_2c_3}$ as a modular DES $\{C_1^{c_1c_2c_3}, \ldots, C_n^{c_1c_2c_3}\}$ such that $L_m(C_i^{c_1c_2c_3}) = \Delta^* \cdot c_1c_2c_3 \cdot L_m(A_i) \cdot (\Delta \setminus N(c_1, c_2, c_3)) \cdot \Delta^*$, where A_i is as in Lemma 1 over the alphabet $\Delta \cup \Gamma_{c_1c_2c_3}$, where $\Gamma_{c_1c_2c_3}$ is a new set of events and $\Sigma = \Delta$. Then, by Lemma 1, we have that $P(L_m(G_{c_1c_2c_3})) = P(L_m(\|_{i=1}^n C_i^{c_1c_2c_3})) = \Delta^* \cdot c_1c_2c_3 \cdot \Delta^{2^n-1} \cdot (\Delta \setminus N(c_1, c_2, c_3)) \cdot \Delta^*$.

We now denote all the systems constructed above as G_i, for $i = 1, \ldots, m$, where $m = |\Delta|^3 + 5$ is polynomial, and every G_i was constructed in polynomial time. Recall that every G_i is either an NFA, or a modular system of the form $\{B_1, \ldots, B_n\}$, where every B_j is an NFA. Moreover, by construction, we have that

$$L(E) = \cup_{i=1}^m P(L_m(G_i)) .$$

In the above constructions, we used total automata (every automaton can be made total by adding a single state and the missing transitions), that is, in every state a transition under every event is defined. Then every G_i is also total.

We now use a new event, $\diamond$, to modify every G_i by adding two new states q_{s_i} and q_{f_i} so that if a word w is accepted by $P(G_i)$, then both q_{s_i} and q_{f_i} are reachable by $w\diamond$ in $P(G_i)$, whereas if w is not accepted by $P(G_i)$, only q_{s_i} is reachable by $w\diamond$ in $P(G_i)$.

Formally, let q_{s_i} and q_{f_i}, $i = 1, \ldots, m$, be new non-marked states with self-loops under all events from $\Delta \cup \{\diamond\}$, where $\diamond$ is a new observable event. For every i, if G_i is an NFA, we modify G_i by adding q_{s_i} to the set of initial states, and by adding a transition from every state under event $\diamond$ to state q_{s_i}, and from every marked state to state q_{f_i}, see Fig. 3.

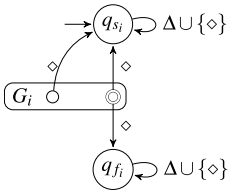

Fig. 3. Modification of an NFA G_i.

If G_i is a modular DES $\{B_1, \ldots, B_n\}$, we add a new unobservable event $\diamond_i$ and, for every B_j, we add two new states b_{s_j} and b_{f_j} to B_j; b_{s_j} is added to initial states of B_j. We add a transition under $\diamond$ from every state of B_j to b_{s_j}. Now, for every marked state t_j of B_j, we add the transitions $(t_j, \diamond_i, t_j')$ and $(t_j', \diamond, b_{f_j})$, where t_j' is a new state added to B_j. We define $q_{s_i} = (b_{s_1}, \ldots, b_{s_n})$ and $q_{f_i} = (b_{f_1}, \ldots, b_{f_n})$, see Fig. 4.

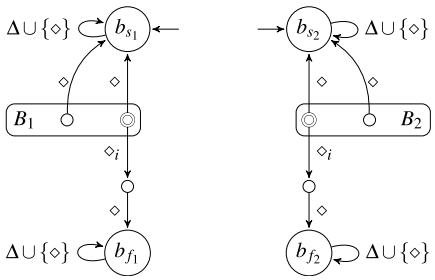

Fig. 4. Modification of G_i being a modular DES $\{B_1, B_2\}$; $q_{s_i} = (b_{s_1}, b_{s_2})$ and $q_{f_i} = (b_{f_1}, b_{f_2})$.

Notice that G_i is always in state q_{s_i}. If a reachable state $(r_1, \ldots, r_n)$ of G_i contains a non-marked state r_j of B_j, then only state q_{s_i} is reachable from $(r_1, \ldots, r_n)$ under $\diamond$ in $P(G_i)$. However, if $(r_1, \ldots, r_n)$ consists only of marked states of $B_1, \ldots, B_n$, then $(r_1, \ldots, r_n)$ leads to state q_{s_i} under $\diamond$ and to state $(r'_1, \ldots, r'_n)$ under $\diamond_i$ in G_i, and hence to states q_{s_i} and q_{f_i} in $P(G_i)$.

Summarized, after these modifications, for every G_i it holds that if $w \in P(L_m(G_i))$ and s is a marked state reached by w, then $s \xrightarrow{\diamond} \{q_{s_i}, q_{f_i}\}$, and that if $w \notin P(L_m(G_i))$, then any state s reachable by w is such that $s \xrightarrow{\diamond} \{q_{s_i}\}$.

We now consider the composition $\|_{i=1}^m G_i$. Assume that the alphabet of $\|_{i=1}^m G_i$ is Σ. We show that $\|_{i=1}^m G_i$ is weakly (periodically) detectable with respect to $\Sigma \setminus (\Delta \cup \{\diamond\})$ iff $L(E) \neq \Delta^*$.

Notice that $\|_{i=1}^m G_i$ is weakly (periodically) detectable with respect to $\Sigma \setminus (\Delta \cup \{\diamond\})$ iff $P(\|_{i=1}^m G_i)$ is weakly (periodically) detectable with respect to $\emptyset$.

Assume first that $L(E) = \Delta^*$. Then, for every $w \in \Delta^*$, there exists $i \in \{1, \ldots, m\}$ such that $w \in P(L_m(G_i))$. Then there is $w' \in P^{-1}(w)$ such that the composition $\|_{i=1}^m G_i$ is in a state $(y_1, \ldots, y_m)$ after reading w', where y_i is a marked state of G_i. This means that the system $P(\|_{i=1}^m G_i)$ is, after reading $w\diamond$, in at least two states, namely $\bar{q}_s = (q_{s_1}, \ldots, q_{s_i}, \ldots, q_{s_m})$ and $(q_{s_1}, \ldots, q_{s_{i-1}}, q_{f_i}, q_{s_{i+1}}, \ldots, q_{s_m})$, and hence the system is not weakly (periodically) detectable.

On the other hand, if $L(E) \neq \Delta^*$, then there is $w \in \Delta^*$ such that $w \notin L(E) = \cup_{i=1}^m P(L_m(G_i))$, and hence none of G_i is in a marked state after reading any $w' \in P^{-1}(w)$. Since event $\diamond$ leads every non-marked state of G_i only to state q_{s_i}, we have that $w\diamond$ leads $P(\|_{i=1}^m G_i)$ only to state $\bar{q}_s = (q_{s_1}, \ldots, q_{s_m})$. Thus, $P(\|_{i=1}^m G_i)$ is weakly (periodically) detectable. □

The algorithm of Lin (2011) to decide weak detectability is based on the computation of observer. If all unobservable events are private, the projection commutes with parallel composition, i.e., $P(L_m(\|_{i=1}^k G_i)) = \|_{i=1}^k P(L_m(G_i))$, see Feng (2007), and we can reduce the complexity of weak modular detectability by computing the parallel composition of local observers rather than the observer of the exponentially larger monolithic DES. We formalize this observation as follows.

Lemma 3. *Let $\{G_1, \ldots, G_n\}$ be a modular DES and $P: \Sigma \to \Sigma_o$ be a projection such that all shared events of any two systems are in Σ_o. Then a state is reachable in $P(\|_{i=1}^n G_i)$ by a word $P(w)$ iff it is reachable in $\|_{i=1}^n P(G_i)$ by $P(w)$.*

Proof. Let $(x_1, \ldots, x_n)$ be a state of $P(\|_{i=1}^n G_i)$ reachable by $P(w)$. Then every x_i is reachable by $P(w)$ in $P(G_i)$, and hence $(x_1, \ldots, x_n)$ is reachable by $P(w)$ in $\|_{i=1}^n P(G_i)$.

Let $(x_1, \ldots, x_n)$ be a state reachable by $P(w)$ in $\|_{i=1}^n P(G_i)$. Then there are words w_i, $i = 1, \ldots, n$, such that $P(w_i) = P(w)$, and x_i is reachable by w_i in G_i. Let $P(w) = a_1 a_2 \cdots a_m$, for some $m \geq 0$. Then $w_i = u_{1,i} a_1 u_{2,i} \cdots u_{m-1,i} a_m u_{m,i}$, where every $u_{k,i} \in E_i^*$, $k = 1, \ldots, m$, for E_i denoting the private alphabet of G_i, that is, for any $i \neq j$, $E_i \cap E_j = \emptyset$. Then the word

$$u_{1,1}u_{1,2} \cdots u_{1,n}\, a_1\, u_{2,1} \cdots u_{2,n} \cdots u_{m-1,n}\, a_m\, u_{m,1} \cdots u_{m,n}$$

leads $\|_{i=1}^n G_i$ to state $(x_1, \ldots, x_n)$. Therefore, state $(x_1, \ldots, x_n)$ is reachable in $P(\|_{i=1}^n G_i)$ by $P(w)$. □

We now have the following.

Theorem 4. *Let $\{G_1, \ldots, G_n\}$ be a modular DES and $P: \Sigma \to \Sigma_o$ be a projection such that all shared events of any two systems are in Σ_o. Then deciding weak (periodic) modular detectability is PSPACE-complete.*

Proof. By Lemma 3, $P(\|_{i=1}^n G_i)$ is weakly (periodically) detectable iff $\|_{i=1}^n P(G_i)$ is. Let H_i denote the determinization of $P(G_i)$, i.e., H_i is the observer of G_i with respect to Σ_o. To check weak detectability in PSPACE means to guess a reachable state $X = (X_1, \ldots, X_n)$ of $\|_{i=1}^n H_i$, where every X_i is a singleton, such that X is non-trivially reachable from itself by states consisting only of singletons, see Shu and Lin (2011). (Similarly for weak periodic detectability.) Since PSPACE-hardness was shown in Yin and Lafortune (2017) and Zhang (2017), the problem is PSPACE-complete. □

4. Modular opacity

By Saboori and Hadjicostis (2007), a DES $G = (Q, \Sigma, \delta, I)$ is *current-state opaque* with respect to Σ_{uo} and a set of secret states $Q_S \subseteq Q$ if

$$(\forall s \in L(G))[R_G(s) \not\subseteq Q_S]\,.$$

Given a modular DES $\{G_1, \ldots, G_n\}$, a set of unobservable events Σ_{uo}, and a set of secret states Q_S. The *modular opacity* problem asks whether $G_1 \| \cdots \| G_n$ is opaque with respect to Σ_{uo} and Q_S.

Theorem 5. *Deciding modular opacity is EXPSPACE-complete.*

Proof. Membership in EXPSPACE follows by adapting the membership in PSPACE for monolithic DES, see Masopust and Yin (2017).

To prove EXPSPACE-hardness, we reuse the proof of Theorem 2 and show that the modular DES constructed there is opaque with respect to $Q_S = \{\bar{q}_s\}$ iff it is not weakly detectable.

As shown in the proof of Theorem 2, if $\|_{i=1}^m G_i$ is weakly detectable with respect to $\Sigma \setminus (\Delta \cup \{\diamond\})$, then there is a word w such that, after reading $w\diamond$, the observer knows for sure that the modular system is in state $\bar{q}_s$. Hence the system is not opaque with respect to Q_s and $\Sigma \setminus (\Delta \cup \{\diamond\})$.

On the other hand, if $\|_{i=1}^m G_i$ is not weakly detectable with respect to $\Sigma \setminus (\Delta \cup \{\diamond\})$, then, after reading any word, we cannot distinguish state $\bar{q}_s$ from some other state, and hence the system is opaque with respect to $\{\bar{q}_s\}$ and $\Sigma \setminus (\Delta \cup \{\diamond\})$. □

A similar case to Theorem 4 applies to modular opacity.

Theorem 6. *Let $\{G_1, \ldots, G_n\}$ be a modular DES and $P: \Sigma \to \Sigma_o$ be a projection such that all shared events of any two systems are in Σ_o. Then deciding modular opacity is PSPACE-complete.*

Proof. By Lemma 3, $P(\|_{i=1}^n G_i)$ is opaque iff $\|_{i=1}^n P(G_i)$ is opaque. Let H_i denote the determinization of $P(G_i)$. To check *non*-opacity with respect to the set of secret states Q_S, we guess a reachable state $(X_1, \ldots, X_n)$ of $\|_{i=1}^n H_i$ such that $X_1 \times \cdots \times X_n \subseteq Q_S$. Since PSPACE is closed under complement, checking opacity is in PSPACE. Since PSPACE-hardness was shown in Cassez et al. (2012), the problem is PSPACE-complete. □

5. Modular A-diagnosability

Let $\Sigma_F \subseteq \Sigma$ be a set of faults, and let $L_F = \Sigma^* \Sigma_F \Sigma^*$ be the set of all trajectories that contain a fault. A DES $G = (Q, \Sigma, \delta, I)$ is *A-diagnosable* with respect to Σ_{uo} and Σ_F if for any fault trajectory, there is an extension under which a fault has occurred, i.e.,

$$(\forall s \in L(G) \cap L_F)(\exists t \in L(G)/s)[P^{-1}P(st) \cap L(G) \subseteq L_F]\,,$$

where $L(G)/s = \{t \in \Sigma^* \mid st \in L(G)\}$.

Remark 7. A-diagnosability is a property originally defined in Thorsley and Teneketzis (2005) for stochastic DES. Let $p\colon Q \times \Sigma \times Q \to [0, 1]$ be a probability function that assigns to each transition of G a probability. Then the stochastic version of A-diagnosability requires that

$$(\forall \epsilon > 0)(\exists K \in \mathbb{N})(\forall s \in L(G) \cap L_F)$$
$$[Prob(t : P^{-1}P(st) \cap L(G) \not\subseteq L_F \mid t \in L(G)/s \wedge |t| = K) < \epsilon]\,,$$

where $Prob(\cdot)$ denotes the probability of continuations of s with length K under which a fault cannot be detected unambiguously, i.e., the miss-detection rate. However, as pointed out in Bertrand et al. (2014) or Chen et al. (2018), A-diagnosability does not depend on the specific value of the probability function p; our definition is thus equivalent to the stochastic definition. In particular, for each miss-detection rate ϵ, the transition probability only affects the value of the delay K but not the *existence* of such a delay. Therefore, we use the equivalent logical definition to simplify our proof.

Given a modular DES $\{G_1, \ldots, G_n\}$, a set of unobservable events Σ_{uo}, and a set of faults Σ_F. The *modular A-diagnosability* problem asks whether $G_1 \| \cdots \| G_n$ is A-diagnosable with respect to Σ_{uo} and Σ_F.

Bertrand et al. (2014) and Chen et al. (2018) showed that testing A-diagnosability is PSPACE-complete for monolithic systems. We show that it is EXPSPACE-complete for modular systems.

Theorem 8. *Deciding modular A-diagnosability is EXPSPACE-complete.*

Proof. Membership in EXPSPACE follows by adapting the membership in PSPACE for monolithic DES, see Masopust and Yin (2017).

To show EXPSPACE-hardness, we reuse and slightly modify the proof of Theorem 2. Let G_i be the systems constructed there, f be a new unobservable event, which is the sole fault, $\Box$ be a new observable event, and, for $i = 1, \ldots, m$, $\Box_i$ be a new unobservable event. We modify every G_i by adding transitions

(1) (q_{s_i}, f, q'_{s_i}), where q'_{s_i} is a new state,
(2) $(q'_{s_i}, \Box, I_i)$, where I_i are the initial states of G_i,
(3) $(q_{s_i}, \Box_j, q'_{s_i})$, for $j \neq i$, and
(4) $(q_{f_i}, \Box_j, q'_{s_i})$, for $j = 1, \ldots, m$.

Intuitively, having read a word $w\diamond$, for some $w \in \Delta^*$, the modular system is in state $\bar{q}_s = (q_{s_1}, q_{s_2}, \ldots, q_{s_m})$ and perhaps also in a state $q = (\ldots, q_{f_i}, \ldots)$. From state $\bar{q}_s$, it can go to state $\bar{q}'_s = (q'_{s_1}, q'_{s_2}, \ldots, q'_{s_m})$ under f, where the fault occurs. But the system can also go to state $\bar{q}'_s$ from q under $\Box_i$, for some i, which is a word with the same projection but without the fault f. Notice that $\Box_i$ is possible only if there is state q_{f_i} indicating that G_i marks word w. This mechanism prevents q from going to state $\bar{q}'_s$ if none of G_i marks w. A conceptual illustration is provided in Fig. 5.

We show that $L(E) \neq \Delta^*$ iff $G = \|_{i=1}^m G_i$ is A-diagnosable with respect to fault $\{f\}$ and unobservable events $\Sigma \setminus (\Delta \cup \{\diamond, \Box\})$.

Suppose that $L(E) = \Delta^*$. By the proof of Theorem 2, for every $w \in \Delta^*$, $P(w)\diamond$ ends up in at least two states, namely $\bar{q}_s$ and states of the form $q = (\ldots, q_{f_i}, \ldots)$, where "…" are either q_{f_j} or q_{s_j}. Notice

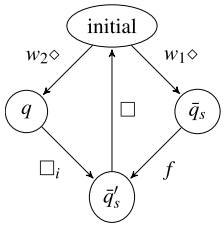

Fig. 5. An illustration of the proof of Theorem 8.

that there is an unobservable transition from q under $\Box_i$ to $\bar{q}'_s = (q'_{s_1}, \ldots, q'_{s_m})$, i.e., there are w_1 and w_2 such that $P(w_1) = P(w_2) = P(w)$ and $w_1\diamond$ leads to state $\bar{q}_s$ and $w_2\diamond$ to state q. Then the words $w_1 \diamond f$ containing the fault and $w_2 \diamond \Box_i \in P^{-1}P(w_1 \diamond f)$ both end up in state $\bar{q}'_s$. Now, only event $\Box$ is possible, which leads the system to the initial states. The proof now follows by induction. Therefore, for any extension of $w_1 \diamond f$, there is always a path that bypasses the fault f due to some event $\Box_k$, and hence $P^{-1}P(w_1 \diamond f w') \cap L(G) \not\subseteq L_F$ for any extension w' of $w_1 \diamond f$ in the system. Therefore, the system is not A-diagnosable.

On the other hand, if $L(E) \neq \Delta^*$, then there is w such that, observing $P(w)\diamond$, the system reaches only states $\bar{q}_s$ and $\bar{q}'_s$. Let $s \in L(G) \cap L_F$ be a fault trajectory. We now fix a word t' such that $st'\Box$ is defined in the system; notice that such a word exists. Then $t = t'\Box w \diamond f \Box \in L(G)$ is an extension of s such that all words of $L(G)$ with the projection equal to $P(st)$ contain the fault f. Indeed, after observing $P(st')\Box$, the observer of the system is in the initial state, and $P(w)\diamond$ leads the observer only to state $\{\bar{q}_s, \bar{q}'_s\}$. Now, when the observer sees event $\Box$, it is sure that the fault f occurred, that is, $P^{-1}P(st) \cap L(G) \subseteq L_F$. Since the fault trajectory s was chosen arbitrarily, the system is A-diagnosable. □

A case similar to Theorem 4 applies to A-diagnosability.

Theorem 9. *Let $\{G_1, \ldots, G_n\}$ be a modular DES and $P\colon \Sigma \to \Sigma_o$ be a projection such that all shared events of any two systems are in Σ_o. Then deciding modular A-diagnosability is PSPACE-complete.*

Proof. We assume that faults are unobservable; for observable faults the problem is trivial. By the assumption, all faults are private, i.e., each fault can only occur locally. Let $\Sigma_{F_i} = \Sigma_F \cap \Sigma_i$ be the set of all local faults, $i = 1, \ldots, n$.

Since A-diagnosability is an event-based property, faults are erased in $P(G_i)$. Therefore, we reformulate A-diagnosability as a state-based property. To this end, we assume, without loss of generality, that for each G_i, its state-space Q_i is partitioned as $Q_i = Q_{N_i} \dot\cup Q_{F_i}$ so that the system is in states of Q_{N_i} as long as no fault has occurred and it is in states of Q_{F_i} from the moment on a fault has occurred. This can be easily fulfilled in polynomial time by computing the product of G_i with a two-state deterministic automaton marking the language L_F. Thus, we can reformulate A-diagnosability as follows:

$$(\forall s \in L(G) : \delta(I, s) \cap Q_F \neq \emptyset)(\exists t \in L(G)/s)[R_G(st) \subseteq Q_F]\,,$$

where $Q_F = \bigcup_{i=1}^n Q_1 \times \cdots \times Q_{i-1} \times Q_{F_i} \times Q_{i+1} \times \cdots \times Q_n$ is the set of all states where at least one component indicates that a fault has occurred.

Using Lemma 3 and letting H_i denote the determinization of $P(G_i)$, to verify A-diagnosability means to check that for every reachable state $(X_1, \ldots, X_n)$ of $\|_{i=1}^n H_i$, if there is i such that $X_i \cap Q_{F_i} \neq \emptyset$, then there is a state $(Y_1, \ldots, Y_n)$ reachable from $(X_1, \ldots, X_n)$ with the property that there is j such that $Y_j \subseteq Q_{F_j}$. Since PSPACE-hardness was shown in Bertrand et al. (2014) and Chen et al. (2018), the problem is PSPACE-complete. □

6. Conclusions

Using a novel and nontrivial construction, we proved that the problems of deciding weak detectability, opacity, and A-diagnosability for modular DES are EXPSPACE-complete. Our results reveal that the properties are significantly more difficult to verify in the modular setting compared with their monolithic counterparts. A special case was identified where the complexity of the properties drops down to polynomial space. Our results also reveal the connections and similarities among these properties from the structural point of view.

Yin and Lafortune (2017) showed that deciding strong modular detectability as defined in Shu et al. (2007) is PSPACE-hard and, to the best of our knowledge, the membership in PSPACE has not yet been discussed in the literature. However, adapting the detector construction of Shu and Lin (2011) shows that deciding strong (periodic) modular detectability is PSPACE-complete, see Masopust and Yin (2017) for details. Moreover, if the number of components in a modular DES is bounded a priori by a constant, then the problem is NL-complete; NL is the class of problems efficiently solvable on a parallel computer. By the space hierarchy theorem of Stearns et al. (1965), NL is a strict subclass of PSPACE, and hence deciding strong modular detectability is significantly simpler if the number of systems is bounded a priori.

Acknowledgments

The authors acknowledge valuable comments and suggestions of anonymous referees.

References

Bertrand, N., Haddad, S., & Lefaucheux, E. (2014). Foundation of diagnosis and predictability in probabilistic systems. In *FSTTCS* In *LIPIcs*: *Vol. 29*, (pp. 417–429).
Cassandras, C. G., & Lafortune, S. (2008). *Introduction to discrete event systems* (2nd ed.). Springer.
Cassez, F., Dubreil, J., & Marchand, H. (2012). Synthesis of opaque systems with static and dynamic masks. *Formal Methods in System Design*, *40*(1), 88–115.
Chen, J., Keroglou, C., Hadjicostis, C. N., & Kumar, R. (2018). Revised test for stochastic diagnosability of discrete-event systems. *IEEE Transactions on Automation Science and Engineering*, *15*(1), 404–408.
Feng, L. (2007). *Computationally efficient supervisor design for discrete-event systems* (Ph.D. thesis), University of Toronto.
Feng, L., & Wonham, W. M. (2008). Supervisory control architecture for discrete-event systems. *IEEE Transactions on Automatic Control*, *53*(6), 1449–1461.
Gohari, P., & Wonham, W. M. (2000). On the complexity of supervisory control design in the RW framework. *IEEE Transactions on Systems, Man and Cybernetics, Part B*, *30*(5), 643–652.
Gummadi, R., Singh, N., & Sreenivas, R. S. (2011). On tractable instances of modular supervisory control. *IEEE Transactions on Automatic Control*, *56*(7), 1621–1635.
Hill, R. C., Cury, J. E. R., de Queiroz, M. H., Tilbury, D., & Lafortune, S. (2010). Multi-level hierarchical interface-based supervisory control. *Automatica*, *46*(7), 1152–1164.
Jacob, R., Lesage, J. -J., & Faure, J. -M. (2016). Overview of discrete event systems opacity: models, validation, and quantification. *Annual Reviews in Control*, *41*, 135–146.
Komenda, J., Masopust, T., & van Schuppen, J. H. (2014). Coordination control of discrete-event systems revisited. *Discrete Event Dynamic Systems: Theory & Applications*, *25*(1–2), 65–94.
Leduc, R., Lawford, M., & Wonham, W. M. (2005). Hierarchical interface-based supervisory control-part ii: parallel case. *IEEE Transactions on Automatic Control*, *50*(9), 1336–1348.
Lin, F. (2011). Opacity of discrete event systems and its applications. *Automatica*, *47*(3), 496–503.
Masopust, T. (2017). Complexity of verifying nonblockingness in modular supervisory control. *IEEE Transactions on Automatic Control*, *63*(2), 602–607.
Masopust, T. (2018). Complexity of deciding detectability in discrete event systems. *Automatica*, *93*, 257–261.
Masopust, T., & Yin, X. (2017). Complexity of detectability, opacity and a-diagnosability for modular discrete event systems, ArXiv report, abs/1710.02877, URL http://arxiv.org/abs/1710.02877.
Meyer, A. R., & Stockmeyer, L. J. (1972). The equivalence problem for regular expressions with squaring requires exponential space. In *SWAT* (pp. 125–129). Maryland, USA.
Rohloff, K., & Lafortune, S. (2005). PSPACE-completeness of modular supervisory control problems. *Discrete Event Dynamic Systems: Theory & Applications*, *15*(2), 145–167.
Saboori, A., & Hadjicostis, C. N. (2007). Notions of security and opacity in discrete event systems. In *IEEE conference on decision and control* (pp. 5056–5061).
Saboori, A., & Hadjicostis, C. N. (2010). Reduced-complexity verification for initial-state opacity in modular discrete event systems. In *WODES* (pp. 78–83).
Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K., & Teneketzis, D. (1995). Diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, *40*(9), 1555–1575.
Schmidt, K., & Cury, J. E. R. (2012). Efficient abstractions for the supervisory control of modular discrete event systems. *IEEE Transactions on Automatic Control*, *57*(12), 3224–3229.
Shu, S., & Lin, F. (2011). Generalized detectability for discrete event systems. *Systems & Control Letters*, *60*(5), 310–317.
Shu, S., Lin, F., & Ying, H. (2007). Detectability of discrete event systems. *IEEE Transactions on Automatic Control*, *52*(12), 2356–2359.
Stearns, R. E., Hartmanis, J., & Lewis I.I., P. M. (1965). Hierarchies of memory limited computations. In *FOCS* (pp. 179–190).
Thorsley, D., & Teneketzis, D. (2005). Diagnosability of stochastic discrete-event systems. *IEEE Transactions on Automatic Control*, *50*(4), 476–492.
Yin, X., & Lafortune, S. (2017). Verification complexity of a class of observational properties for modular discrete events systems. *Automatica*, *83*, 199–205.
Zaytoon, J., & Lafortune, S. (2013). Overview of fault diagnosis methods for Discrete Event Systems. *Annual Reviews in Control*, *37*(2), 308–320.
Zhang, K. (2017). The problem of determining the weak (periodic) detectability of discrete event systems is PSPACE-complete. *Automatica*, *81*, 217–220.

Tomáš Masopust received M.Sc. in computer science from Masaryk University, Brno, Czechia in 2004, and Ph.D. in computer science from Brno University of Technology, Brno, Czechia in 2007. He worked at CWI Amsterdam The Netherlands, in the Systems and Control Group, at University of Bayreuth, Germany, in the Theoretical Computer Science Group, and at TU Dresden, Germany, in the Knowledge-Based Systems Group. Since 2017 he is a researcher at Institute of Mathematics, Czech Academy of Sciences, Brno, Czechia, and since 2018 he is assistant professor of computer science at Palacky University, Olomouc, Czechia. His research interest includes verification and control of discrete-event systems and theoretical computer science. He is an editor of Kybernetika journal.

Xiang Yin was born in Anhui, China, in 1991. He received the B.Eng degree from Zhejiang University in 2012, the M.S. degree from the University of Michigan, Ann Arbor, in 2013, and the Ph.D degree from the University of Michigan, Ann Arbor, in 2017, all in electrical engineering.

Since 2017, he has been with the Department of Automation, Shanghai Jiao Tong University, where he is an Associate Professor. His research interests include formal methods, control of discrete-event systems, model-based fault diagnosis, security and their applications to cyber and cyber–physical systems. He received the Outstanding Reviewer Awards from Automatica, the IEEE Transactions on Automatic Control and the Journal of Discrete Event Dynamic Systems. He also received the IEEE Conference on Decision and Control (CDC) Best Student Paper Award Finalist in 2016. He is the co-chair of the IEEE CSS Technical Committee on Discrete Event Systems.