Online fault diagnosis in Petri net models of discrete-event systems using Fourier-Motzkin

Al-Ajeli, Ahmed ; Parker, David

DOI:
10.1109/CONTROL.2018.8516748

Online fault diagnosis in Petri net models of discrete-event systems using Fourier-Motzkin

Ahmed Al-Ajeli
College of Information Technology
University of Babylon, Iraq
Email: a.alajeli@itnet.uobabylon.edu.iq

David Parker
School of Computer Science
University of Birmingham, UK
Email: d.a.parker@cs.bham.ac.uk

***Abstract*—This paper presents a new approach for the fault diagnosis problem in partially observable discrete-event systems modelled with Petri nets. Our approach is based on the use of the Integer Fourier-Motzkin Elimination (IFME) method. The fault diagnosis problem is solved by first creating an initial set of inequalities from the state equation of a Petri net. The occurrence or absence of faults can also be expressed by inequalities. After adding these inequalities to the initial set, we apply the IFME method to eliminate the variables corresponding to unobservable transitions. The resulting set of inequalities is used for the purpose of diagnosis. We prove the correctness of our approach for both bounded and unbounded Petri nets with no cycles of unobservable transitions.**

I. Introduction

The problem of fault diagnosis in partially observable discrete-event systems (DES) has received considerable attention in the past three decades. A popular approach is to assume the existence of a formal representation of the behaviour of the system being analysed (often called the *plant*) captured in some modelling language. Two commonly used formalisms are automata and Petri nets [1]–[5]. Among others, the seminal paper by Sampath *et al*. [1] formulates the problem of fault diagnosis for systems modelled by automata. In this paper, we use Petri nets for modelling of systems as they provide a richer modelling environment than automata [3], [6]. Also, since Petri nets extend automata, the results in this paper are also applicable to automata.

The automata approach for fault diagnosis starts by creating, from the model of the system, an automaton called a *diagnoser* in which all events are observable. It is well known that the diagnoser-based approach has the *state explosion problem*. An extension of the automata approach to Petri net models has been reported in [3]. The idea of *basis marking and justifications* has been introduced, where only a subset of the states in the system being diagnosed is enumerated.

A different idea has been introduced in [5], [7], where they adopt the use of equations to address the fault diagnosis problem. In other words, the diagnoser is no longer represented as an automaton. More specifically, the fault diagnosis problem is reduced to an Integer Linear Programming (ILP) problem which is solved online every time an event is observed.

In [8], a new approach for fault diagnosis in *acyclic* Petri net has been proposed. The Integer Fourier-Motzkin Elimination (IFME) method has been adopted to detect a single fault. The Fourier-Motzkin Elimination (FME) is a method to solve a set of inequalities in real variables using variable elimination techniques [9]–[11]. IFME is an extension of classic FME to cope with integer-valued variables [12], [13].

The basic idea of using the IFME method consists of creating two sets of inequalities from the *state equation* of a Petri net [14]. Then, the IFME method is used to drop unobservable transitions and construct two sets of inequalities in variables corresponding to observable transitions. One set ensures that a fault has occurred and the other ensures that no fault has occurred. The advantage of using the constructed sets is that, since all variables relate to the observable events, it can be checked, for a given sequence of observed events, if the projection to observable events satisfies the sets. As a result, these sets of inequalities are used to decide about the occurrence of the fault as any other diagnoser would do.

In this paper, we extend the work in [8] to the case where Petri nets may contain cycles, but only comprising observable transitions. Handling this case becomes necessary as many real applications require adding cycles to Petri nets in order to model repeated behaviours of the system being diagnosed. In addition, we consider the case of multiple fault types. This extension uses a new idea based on tracking the diagnosis history. The aim is to avoid the problem of missing information about the order of firing transitions when using the state equation representation of Petri nets with cycles. In fact, this information can play an essential role in diagnosing faults.

Existing approaches to fault diagnosis have either large space requirements or need significant computation. In addition, these approaches are limited to dealing with a specific type of system. The IFME-based approach has an advantage over these approaches in that it provides a good balance between time and space complexity. This enables its application to large, complex and infinite systems.

This paper is organized as follows. Section II presents a brief introduction to Petri net theory and the IFME method. A description of the fault diagnosis problem in DES is provided in Section III. The main results, including modelling of faults via inequalities and using the IFME method for fault diagnosis, are covered in Section IV. We end the paper with conclusions.

II. PRELIMINARIES

A. Petri Nets

A *Petri net* [14] is defined as a tuple $\mathscr{N} = (P, T, pre, post)$, where $P = p_1, \ldots, p_m$ and $T = t_1, \ldots, t_n$ are non-empty finite sets of places and transitions, respectively, $pre : P \times T \to \mathbb{N}$ and $post : P \times T \to \mathbb{N}$. For a given transition $t \in T$, an *input* (*output*) place of t is a place p such that $pre(p,t)$ ($post(p,t)$) is positive, respectively. $A = [a_{ij}]$ is an $m \times n$ matrix of integers called the *incidence matrix*, where $a_{ij} = post(p,t) - pre(p,t)$, assuming that the set of places and transitions are ordered to correspond to the coordinates of the matrix.

We write ${}^\bullet t$ ($t^\bullet$) for the set of all input (output) places of a transition t, respectively, and we write ${}^\bullet p$ ($p^\bullet$) for the set of all input (output) transitions of a place p, respectively. A Petri net is called *pure* if it has no self-loops.

A *state* of a Petri net, known as a *marking*, is represented as $M : P \to \mathbb{N}$ capturing the number of tokens in each place. We sometimes represent a marking as an $m \times 1$ matrix of non-negative integers. A transition t is *enabled* at a marking M if $M(p) \geq pre(p,t)$ for each $p \in {}^\bullet t$. An enabled transition can *fire*, resulting in a new marking M', denoted by $M \xrightarrow{t} M'$. The firing vector $\mathbf{u}$ is defined as an $n \times 1$ column vector of the form $\mathbf{u} = (0, \ldots, 0, 1, 0, \ldots, 0)$, where the only 1 appears in the jth position, $j \in \{1, \ldots, n\}$, to indicate that the jth transition is currently firing. Given $\mathbf{u}$ for a firing transition on marking M, we can find the reachable marking M' by $M' = M + A\mathbf{u}$. A sequence of transitions $\sigma = t_1 \ldots t_l$ of T is called *enabled* at a marking M, if there are markings $M_1, \ldots, M_l$ so that $M \xrightarrow{t_1} M_1 \xrightarrow{t_2} M_2 \ldots \xrightarrow{t_l} M_l$. In this case, we write $M \xrightarrow{\sigma} M_l$ and refer to M_l as a state *reachable* from M and σ is the firing sequence. We write $R(\mathscr{N}, M)$ for the set of all states reachable from M. The initial state of the system is represented by an *initial marking* M_0. We will write $(\mathscr{N}, M_0)$ for a Petri net with its initial marking M_0.

The set of all finite-length strings of the transitions in T is denoted by T^* and is called the *Kleene-closure* of T. As a result, members of T^* are created from concatenations of a finite number of elements of T. In particular, T^* contains the empty string ε, so that $t\varepsilon = \varepsilon t = t$ for all $t \in T$. Every subset of T^* is called a *language over the alphabet* T. Suppose that we have a sequence σ of $(\mathscr{N}, M_0)$, then the *Parikh vector* $\# : T^* \to \mathbb{N}^n$ is a map which assigns to every sequence σ a vector $\#(\sigma)$ in which each element represents the number of firings of each transition in σ. In other words, for $\#(\sigma) : T \to \mathbb{N}$, $\#(\sigma)(t)$ is the number of occurrence of $t \in T$ within the sequence σ. Sometimes, we also write $\#(t, \sigma)$ to represent the number of occurrences of t in σ.

The set of sequences of transitions resulting in reachable markings is called the *language* of the Petri net and is denoted by $L(\mathscr{N}, M_0)$, i.e., $L(\mathscr{N}, M_0) = \{\sigma \mid \exists M\ M_0 \xrightarrow{\sigma} M\}$. Suppose that a destination marking M is reachable from M_0 in a Petri net $\mathscr{N}$ through a sequence σ, we can then find M using the following *state equation*:

$$M = M_0 + A\mathbf{x} \geq \vec{\mathbf{0}} \tag{1}$$

where A is the incidence matrix of $\mathscr{N}$, and $\mathbf{x} \in \mathbb{N}^n$ is an n-dimensional column vector with $\mathbf{x} = (x_1, \ldots, x_n)$ and $x_i = \#(t_i, \sigma)$ for $t_i \in T$. Then, for any sequence σ of $\mathscr{N}$, there exists $\mathbf{x} = \#(\sigma)$ satisfying (1). The converse is not always true. In some cases, e.g. *acyclic* Petri nets, the converse holds too. Note that, from (1), we can derive a corresponding set of inequalities I in the form $-A\mathbf{x} \leq M_0$ equipped with non-negativity constraints on $\mathbf{x}$, i.e., $\mathbf{x} \geq \vec{\mathbf{0}}$.

Definition 1. *[15] Let $\nu = (\alpha_1, \ldots, \alpha_n)$ be a solution of the state equation for a Petri net $(\mathscr{N}, M_0)$ with a destination marking M. Then, the* firing count subnet *with respect to ν is the subnet $\mathscr{N}_\nu$ where each transition t_i in $\mathscr{N}_\nu$ is such that $\alpha_i > 0$ together with its input and output places and its connecting arcs. $M_{0\nu}$ and M_ν denote the restrictions of M_0 and M to places in $\mathscr{N}_\nu$.*

Finally, we note that whenever Petri nets are mentioned in this paper, we assume they are *pure*. A non-pure Petri net can be transformed to one that is pure by adding a dummy transition-place pair to open self-loops [14].

B. The Integer Fourier-Motzkin Elimination Method

The Fourier-Motzkin elimination (FME) method was originally proposed for solving a set of linear inequalities and also to establish if the set is solvable [9], [11]. In other words, given a matrix $A \in \mathbb{R}^{m \times n}$ and vector $\mathbf{b} \in \mathbb{R}^m$, FME tests if a set of inequalities $I := A\mathbf{x} \leq \mathbf{b}$, where the vector of variables $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$, has a solution. Then, if there exists a solution, FME will find it.

In sets of linear inequalities having integer-valued variables, we look for integer solutions. Such sets may have real solutions when integer solutions do not exist. When directly applying the FME method to eliminate integer-valued variables, difficulties can arise, which will be demonstrated as follows. Suppose that FME is applied to a set of inequalities I resulting in a reduced set of inequalities R. If R has no integer solution, then I has no an integer solution. In some cases, the set of inequalities R may have an integer solution but there does not exist a corresponding integer solution in I. To ensure that, for any integer solution in R, there exists an integer solution in I, the FME method has been extended. This extension, named the Integer FME (IFME) method, to cope with integer valued variables has been reported in [12] and [13]. In this paper, we have chosen the method presented in [13], which better meets our needs as it is somewhat simpler and more efficient. The following theorem captures the main result of the IFME method.

Theorem 1. *[13] Assume that the variables $x_n, \ldots, x_{k+1}$ have been eliminated in order by using the IFME method described above from a set of linear inequalities I. This results in the reduced set R. Then $\alpha_1, \ldots, \alpha_k$ is a solution of R iff there exist values $\alpha_{k+1}, \ldots, \alpha_n$ such that $\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n$ is a solution of I.*

III. Problem statement

In this section, we describe the problem of fault diagnosis in DES modelled by Petri nets, as outlined in [3]. Consider a Petri net $(\mathcal{N}, M_0)$ with a set of transitions $T = \{t_1, t_2, \ldots, t_n\}$. Suppose that T is partitioned into two sets: observable transitions T_o and unobservable transitions T_u. We further assume that faults are unobservable transitions, i.e., $T_f \subseteq T_u$, in which T_f is the set of transitions which are modelling occurrences of faults. The set T_u may have other transitions which model no fault, i.e., they model normal events.

Consider also the *projection* function $\pi : T \to T_o \cup \{\varepsilon\}$ that maps unobservable transitions to the empty string ε, i.e., $\pi(t) = \varepsilon$ for $t \in T_u$, while $\pi(t) = t$ for $t \in T_o$. The projection function π can be extended to the Kleene-closure of T by $\pi : T^* \to (T_o \cup \{\varepsilon\})^*$ where for each sequence of transitions σ and each transition t, $\pi(\sigma t) = \pi(\sigma)\pi(t)$. We assume $\pi(\varepsilon) = \varepsilon$ and that $\pi(t\varepsilon) = \pi(\varepsilon t) = \varepsilon$ for each $t \in T_u$. We denote by $\mathbf{s} = \pi(\sigma)$ the observed sequence corresponding to a given sequence $\sigma \in T^*$.

A system may have more than one type of fault. Thus, T_f is partitioned into $T_f^1, T_f^2, \ldots, T_f^r$ representing different types of fault. Since it is not required to uniquely identify occurrences of every fault of a given type, a firing of any transition $t \in T_f^i$ implies that a fault of type T_f^i has occurred. In Petri nets modelling partially observable DES, each observable transition is associated with an event (given as a label). We assume that, if a transition fires, the associated event is observed. In other words, in every execution of events, we can only observe a sequence of transitions from T_o.

A *diagnoser* uses such information (observations) to identify a diagnosis state to be one of the following : 1) a *Normal* state - when all sequences having the same have no fault transition from the set T_f; 2) a *Faulty* state, obtained when all sequences with the same observations have a fault transition with respect to T_f^i; and 3) an *Uncertain* state when we are not sure about the occurrence of faults. In this paper, we address the fault diagnosis problem in Petri nets under the assumption that every transition has a unique label and the system starts from a normal state.

IV. The IFME Method for Fault Diagnosis

This section presents the main results of the paper. We start by explaining how faults can be expressed as inequalities. Based on this, an extension of the diagnoser definition is given. We also prove our main results and apply our approach to a Petri net example.

A. Modelling Fault via Inequalities

In this paper, the proposed approach mainly relies on using inequalities. We use these in two ways. Firstly, the *state equation* constraints can be written as a set of inequalities, I. Secondly, a fault can also be written as an inequality.

Representation of a fault as an inequality: Suppose that transition $t_i \in T$ is a fault transition. Then t_i does not appear in a firing sequence σ if and only if $\mathbf{c} := \#(t_i, \sigma) \leq 0$ holds. Also, occurrence of t_i in σ can be trivially written as $\neg\mathbf{c} := \#(t_i, \sigma) > 0$, i.e., the negation of $\mathbf{c}$.

In addition, we can represent a family of faults as an inequality by extending the formulation above. Recall that each T_f^i, $i = 1, 2, \ldots, r$, is a fault type. We associate to each type T_f^i two inequalities $\neg\mathbf{c}_i := \sum_{t \in T_f^i} \#(t, \sigma) > 0$ and $\mathbf{c}_i := \sum_{t \in T_f^i} \#(t, \sigma) \leq 0$. Then, no fault of type T_f^i appearing in σ implies that $\mathbf{c}_i$ holds. In contrast, a fault of type T_f^i appears in σ implies that $\neg\mathbf{c}_i$ holds.

In what follows, we describe the definitions introduced in [8], in preparation for presenting the extended definition of the diagnoser below.

Definition 2. *Let $\mathbf{x} = (x_1, \ldots, x_n)$ be a set of variables. We suppose that the variables range over $\mathbb{N}$. A* valuation *ν for $\mathbf{x}$ is a function that associates a value in $\mathbb{N}$ to each variable x_i in $\mathbf{x}$.*

Remark 2: In light of Definition 2, given a sequence $\sigma \in T^*$, the Parikh vector $\#(\sigma)$ represents a valuation of $\mathbf{x}$. In other words, for each x_i of $\mathbf{x}$, $x_i = \#(t_i, \sigma)$, where $i = 1, 2, \ldots, n$.

Definition 3. *Suppose that $\mathbf{e}$ is an inequality of the form $a_1x_1 + \ldots + a_nx_n \leq b$ in the variables $\mathbf{x} = (x_1, \ldots, x_n), x_i \in \mathbb{N}$ and $a_1, \ldots, a_n, b \in \mathbb{Z}$. Consider a valuation ν as $\alpha_1, \ldots, \alpha_n$ assigned to $x_1, \ldots, x_n$ respectively. Then, we write $\nu \vDash \mathbf{e}$ to say that the valuation ν satisfies the inequality $\mathbf{e}$ if and only if $a_1\alpha_1 + \ldots + a_n\alpha_n \leq b$ holds.*

Definition 4. *Suppose that we have a set of inequalities $I = \{e_i \mid 1 \leq i \leq d\}$, where e_i has the form of $\mathbf{e}$ in Definition 3. Consider a valuation ν for the variables of the inequalities in I. Then, $\nu \vDash I$ if and only if $(\nu \vDash e_1) \wedge (\nu \vDash e_2) \wedge \ldots \wedge (\nu \vDash e_d)$.*

Using the new formulation of fault, described above, and the definition of the diagnoser presented in [3] which is itself an extension of the classic definition introduced in [1], we present the following definition.

Definition 5. *A* diagnoser *is a function $\Delta : T_o^* \times 2^{T_f} \to \{NoFault, Faulty, Uncertain\}$ that associates to each observed sequence $\mathbf{s}$ with respect to the fault type T_f^i, $i \in \{1, \ldots, r\}$, one of the following diagnosis states:*

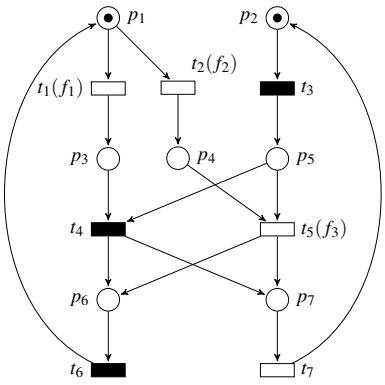

Fig. 1. A Petri net example

- $\Delta(\mathbf{s}, T_f^i) = NoFault$ *if* $\forall \sigma \in L(\mathcal{N}, M_0)$ *and* $\pi(\sigma) = \mathbf{s}$, $\#(\sigma) \models \mathbf{c}_i$. *This state implies that no fault from set* T_f^i *has occurred.*
- $\Delta(\mathbf{s}, T_f^i) = Faulty$ *if* $\forall \sigma \in L(\mathcal{N}, M_0)$ *and* $\pi(\sigma) = \mathbf{s}$, $\#(\sigma) \models \neg\mathbf{c}_i$. *Obtaining this state means a fault from set* T_f^i *has certainly occurred.*
- $\Delta(\mathbf{s}, T_f^i) = Uncertain$ *if there are two sequences* $\sigma_1, \sigma_2 \in L(\mathcal{N}, M_0)$ *such that* $\pi(\sigma_1) = \pi(\sigma_2) = \mathbf{s}$, $\#(\sigma_1) \models \mathbf{c}_i$ *and* $\#(\sigma_2) \models \neg\mathbf{c}_i$. *In this case, we are uncertain of the system behaviour.*

If $\Delta(\mathbf{s}, T_f^i) = NoFault$ for all $i = 1, \ldots, r$, then we are certain that no fault from any type has occurred during the observed sequence $\mathbf{s}$, i.e., the system is in a normal state.

Example 1. Consider the Petri net depicted in Fig. 1, where $P = \{p_1, \ldots, p_7\}$, $T = \{t_1, \ldots, t_7\}$ and $M_0 = [1100000]$. In the figure, observable transitions are depicted by solid rectangles, while empty rectangles represent unobservable transitions. Moreover, we model two types of faults, $T_f^1 = \{t_1\}$ and $T_f^2 = \{t_2, t_5\}$.

The inequalities $\mathbf{c}_1 := x_1 \leq 0$ and $\neg\mathbf{c}_1 := x_1 > 0$ are associated to T_f^1, while T_f^2 can be represented by the inequalities $\mathbf{c}_2 := x_2 + x_5 \leq 0$ and $\neg\mathbf{c}_2 := x_2 + x_5 > 0$. Suppose that the diagnoser observes no sequence ($\mathbf{s} = \varepsilon$), then $\Delta(\mathbf{s}, T_f^1) = \Delta(\mathbf{s}, T_f^2) =$ *Uncertain* because $\mathbf{s}$ might correspond to two other sequences, $\sigma_1 = t_1$ and $\sigma_2 = t_2$. In this case, $\mathbf{x}_1 = \#(\sigma_1) = (1,0,0,0,0,0,0)$ and $\mathbf{x}_2 = \#(\sigma_2) = (0,1,0,0,0,0,0)$. Then $\#(\sigma_1) \models \neg\mathbf{c}_1$, but $\#(\sigma_2) \models \mathbf{c}_1$. Also, $\#(\sigma_1) \models \mathbf{c}_2$ but $\#(\sigma_2) \models \neg\mathbf{c}_2$.

Assume now that $\mathbf{s} = t_3 t_4$. Then $\Delta(\mathbf{s}, T_f^1) = Faulty$, but $\Delta(\mathbf{s}, T_f^2) = NoFault$. The diagnoser estimates such a state because all sequences $\sigma \in L(\mathcal{N}, M_0)$ such that $\pi(\sigma) = t_3 t_4$ have a fault from type T_f^1, but no fault from the type T_f^2 appears in these sequences. In particular, there exist only two sequences $\sigma_1 = t_1 t_3 t_4 t_7$, $\sigma_2 = t_3 t_1 t_4 t_7$ with $\pi(\sigma_1) = \pi(\sigma_2) = t_3 t_4$. In this case, we have $\#(\sigma_1) = \#(\sigma_2) = (1,0,1,1,0,0,1)$. Then, $\#(\sigma_1), \#(\sigma_2) \models \neg\mathbf{c}_1$, but $\#(\sigma_1), \#(\sigma_2) \models \mathbf{c}_2$.

B. The Proposed Approach for Fault Diagnosis

In [8], the notion of using the IFME for fault diagnosis in DES modelled by Petri nets is introduced. Under the assumption that Petri nets are *acyclic* and have a single fault, it has been shown that the diagnoser can be expressed as two sets of inequalities. These sets are derived from the *state equation* of Petri nets augmented by $\mathbf{c}$ or $\neg\mathbf{c}$. In this paper, we relax the assumption to the case where the Petri nets under study have no cycle of unobservable transitions. In addition, we consider the case of multiple faults.

The IFME approach for fault diagnosis can be outlined as follows. Suppose that $(\mathcal{N}, M_0)$ is a Petri net with an initial marking M_0. Without any loss of generality, suppose that we have renamed the transitions of $\mathcal{N}$ such that the first k transitions are observable, i.e., $T_o = \{t_1, t_2, \ldots, t_k\}$. The remaining transitions are unobservable, i.e., $T_u = \{t_{k+1}, t_{k+2}, \ldots, t_n\}$. We further suppose that the set of fault transitions in $\mathcal{N}$ is $T_f \subseteq T_u$ and all faults are of the same type.

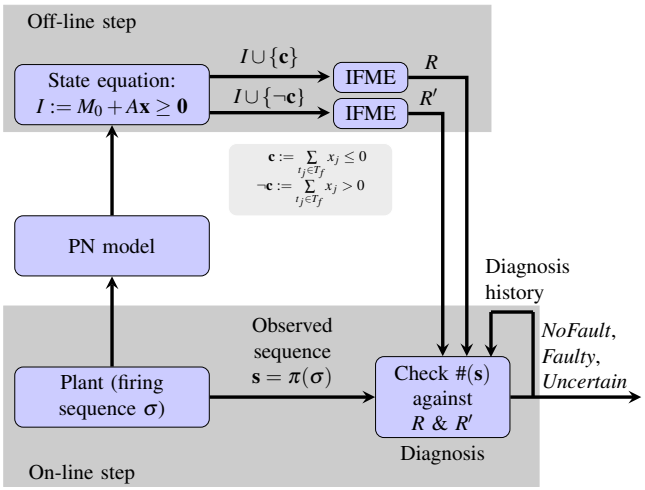

Fig. 2. Sketch of the proposed approach

We introduce variables $x_1, x_2, \ldots, x_n$ representing the number of firings of $t_1, t_2, \ldots, t_n$, respectively. Suppose that $M_0 + A\mathbf{x} \geq \vec{\mathbf{0}}$ represents the state equation constraint, where $\mathbf{x} = (x_1, x_2, \ldots, x_n)$. We further assume that $\mathbf{c}$ is the inequality $\sum_{t_j \in T_f} x_j \leq 0$ and $\neg\mathbf{c}$ is the negation of $\mathbf{c}$, i.e., the inequality $\sum_{t_j \in T_f} x_j > 0$. For each firing sequence σ of $(\mathcal{N}, M_0)$, if σ contains a fault from T_f, then $\mathbf{x} = \#(\sigma)$, the Parikh vector of σ, satisfies $\neg\mathbf{c}$. Conversely, for a firing sequence σ, if $\mathbf{x}$ satisfies $\mathbf{c}$, then σ has no fault transition.

The general idea of our approach to address the problem of fault diagnosis where cycles are permitted is illustrated in Fig. 2. The key difference between this and the scheme introduced in [8] is the addition of the concept of the diagnosis history, as shown in the figure. This becomes necessary to overcome the problem of not considering the order of firing transitions by state equation representation. Afterwards, the process of fault diagnosis can be divided into two steps:

- **Off-line step:** In this step, we start from the Petri net model to obtain a set of inequalities I created from the state equation and non-negativity constraints on $\mathbf{x}$. Then, two sets of inequalities $I \cup \{\mathbf{c}\}$ and $I \cup \{\neg\mathbf{c}\}$ are created. Applying the IFME method simultaneously to both $I \cup \{\mathbf{c}\}$ and $I \cup \{\neg\mathbf{c}\}$, two reduced sets, R and R', are obtained by eliminating every variable corresponding to a transition in the set T_u.
- **On-line step:** During this step, the reduced sets of inequalities R and R' along with the diagnosis history are used to compute the diagnosis state. In effect, the diagnosis history is only needed when the Parikh vector of the observed sequence $\mathbf{s}$ satisfies both R and R'.

To extend the idea of creating these reduced sets of inequalities to the case where there are multiple faults of different types, we produce a separate pair of sets of inequalities for each fault type. In particular, to create a set of inequalities for a given fault type, the transitions representing faults in the other fault types are considered as normal unobservable transitions. We say that a fault of type T_f^i, $i = 1, 2, \ldots, r$, occurs if and

only if at least one fault transition $t \in T_f^i$ fires.

Then, we use the reduced sets of inequalities to diagnose fault occurrence as follows. Inspired by Theorem 16 in [14], we present the following lemma which is necessary to prove Theorem 2 below.

Lemma 1. *Suppose that ν is an $n \times 1$ column vector and M is a reachable marking in a Petri net $\mathcal{N}$ such that $M' = M + A\nu \geq \vec{0}$. Considering that $\mathcal{N}_\nu$ (see Definition 1) is cycle-free, then there exists a sequence $\sigma \in T_\nu^*$ (T_ν is the set of transitions in $\mathcal{N}_\nu$) such that $M_\nu \xrightarrow{\sigma} M'_\nu$ and $\#(\sigma) = \nu$, where M_ν and M'_ν are restrictions of M and M' to places of $\mathcal{N}_\nu$. In addition, σ can fire under M resulting in M' such that $M \xrightarrow{\sigma} M'$.*

Proof. Following a similar proof of Theorem 16 in [14]. □

Definition 6. *Suppose that $\mathbf{s} = \omega t$ is a sequence of observable events, where $\omega \in T_o^*$ and $t \in T_o$, then the* most recent diagnosis state *of* $\mathbf{s}$ *is* $\Delta(\omega, T_f)$.

Note that the most recent diagnosis state of the empty string ε is *NoFault* as we assume that the system starts from a normal state.

Theorem 2. *Assume that $(\mathcal{N}, M_0)$ is a Petri net with no cycle of unobservable transition exists. Suppose that I is the set of inequalities $-A\mathbf{x} \leq M_0$ created from the state equation of $\mathcal{N}$. Assume also that $\mathbf{c}_i$ is the inequality $\sum_{t_j \in T_f^i} x_j \leq 0$ and $\neg\mathbf{c}_i := \sum_{t_j \in T_f^i} x_j > 0$ is its negation. For every $i \in \{1, \ldots, r\}$, suppose that the sets of inequalities R_i and R'_i are respectively produced from applying IFME to both $I \cup \{\mathbf{c}_i\}$ and $I \cup \{\neg\mathbf{c}_i\}$ to eliminate all variables corresponding to transitions in T_u. Then, for any given observed sequence $\mathbf{s} = \omega t, \omega \in T_o^*$ and $t \in T_o$ such that $M_0 \xrightarrow{\sigma} M$ and $\pi(\sigma) = \mathbf{s}$, $\Delta(\mathbf{s}, T_f^i)$ is determined as follows:*

$$\Delta(\mathbf{s}, T_f^i) = \begin{cases} \textit{NoFault} & \text{if } \#(\mathbf{s}) \not\models R'_i \\ \textit{Faulty} & \text{if } (\#(\mathbf{s}) \not\models R_i) \\ & \quad \vee((\#(\mathbf{s}) \models R_i) \wedge (\#(\mathbf{s}) \models R'_i) \\ & \quad \wedge(\Delta(\omega, T_f^i) = \textit{Faulty})) \\ \textit{Uncertain} & \text{if } (\#(\mathbf{s}) \models R_i) \wedge (\#(\mathbf{s}) \models R'_i) \\ & \quad \wedge((\Delta(\omega, T_f^i) = \textit{NoFault}) \\ & \quad \vee(\Delta(\omega, T_f^i) = \textit{Uncertain})) \end{cases}$$

Proof. This proof is presented for one fault type i. To obtain a complete proof we only need to repeat the proof to every fault type. In what follows, we assume that $\#(\mathbf{s}) = (\alpha_1, \ldots, \alpha_k)$.

Proof of $\Delta(\mathbf{s}, T_f^i) = \textit{NoFault}$: By contradiction, assume that $\#(\mathbf{s}) \not\models R'_i$, but the diagnosis state is not *NoFault*. If $\#(\mathbf{s}) \not\models R'_i$, then for every valuation $(\alpha_{k+1}, \ldots, \alpha_n)$ of $(x_{k+1}, \ldots, x_n)$ such that $\nu = (\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$, $\nu \not\models I \cup \{\neg\mathbf{c}_i\}$ by Theorem 1. As a result, $\forall\sigma' \in L(\mathcal{N}, M_0)$ such that $\pi(\sigma') = \mathbf{s}$, $\#(\sigma') \models \mathbf{c}_i$, i.e., $\sum_{t \in T_f} \#(t, \sigma') \leq 0$. Hence, the fault has not occurred during observing $\mathbf{s}$, i.e., the diagnosis state is *NoFault*. This contrasts the assumption.

Proof of $\Delta(\mathbf{s}, T_f^i) = \textit{Faulty}$: Here we have two cases to be proved.

Case 1 (if $\#(\mathbf{s}) \not\models R_i$ holds): This follows using the same argument as above, but replacing R_i with R'_i.

Case 2 (if $(\#(\mathbf{s}) \models R_i) \wedge (\#(\mathbf{s}) \models R'_i) \wedge (\Delta(\omega, T_f^i) = \textit{Faulty})$ holds): Since $\Delta(\omega, T_f^i) = \textit{Faulty}$ holds, i.e., the most recent diagnosis state is *Faulty*, then a fault has occurred during the observed sequence ω. Also, since the fault propagates to all states following the *Faulty* state, then the fault has occurred during $\mathbf{s} = \omega t$ too.

Proof of $\Delta(\mathbf{s}, T_f^i) = \textit{Uncertain}$: We first assume that $\mathbf{s} = \varepsilon$. Then there exists one possible case for the most recent diagnosis state, particularly *NoFault*, because we suppose that the system starts from a normal state. Now let us prove the result in the case where $\mathbf{s} = \varepsilon$. If $\#(\mathbf{s}) \models R_i$, then there exists a valuation $(\alpha_{k+1}, \ldots, \alpha_n)$ of $(x_{k+1}, \ldots, x_n)$ such that $\nu = (\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$ and $\nu \models I \cup \{\mathbf{c}_i\}$ by Theorem 1. If $\nu \models I \cup \{\mathbf{c}_i\}$, then $\nu \models I$, i.e., ν satisfies $M' = M_0 + A\nu \geq \vec{0}$. Since $\mathbf{s}$ has no observable transitions ($\mathbf{s} = \varepsilon$), then the subnet $\mathcal{N}_\nu$ has only unobservable transitions. Again, by the assumption of no cycles of unobservable transitions in $\mathcal{N}$, $\mathcal{N}_\nu$ is cycle free. As a result, there exists $\sigma' \in T_\nu^*$ such that $M_0 \xrightarrow{\sigma'} M'$ and $\#(\sigma') = \nu$ by Lemma 1. Hence, the sequence σ' has no fault. Likewise, we can prove that if $\#(\mathbf{s}) \models R'_i$, there exists another sequence having a fault. Since there are two sequences having the same $\mathbf{s}$ but one has a fault and the other has no, then we have an *Uncertain* state.

Now, assume that $\mathbf{s} = \omega t$, $t \in T_o$ and $\omega \in T_o^*$. Then there are two cases to be considered:

Case 1 (when the most recent diagnosis state is *NoFault* ($\Delta(\omega, T_f^i) = \textit{NoFault}$)): If $\#(\mathbf{s}) \models R_i$, then there exists a valuation $(\alpha_{k+1}, \ldots, \alpha_n)$ of $(x_{k+1}, \ldots, x_n)$ such that $\nu = (\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$ and $\nu \models I \cup \{\mathbf{c}_i\}$ by Theorem 1. If $\nu \models I \cup \{\mathbf{c}_i\}$, then $\nu \models I$, i.e., $M'' = M_0 + A\nu \geq \vec{0}$. Since no fault occurred during observing ω, and t is an observable transition, then we are certain that all sequences $\sigma' t$ such that $M_0 \xrightarrow{\sigma' t} M'$ and $\pi(\sigma') = \omega$ have no fault. Assuming $y = \nu - \#(\sigma' t)$, $y \in \mathbb{N}^n$, then $M'' = M' + Ay \geq \vec{0}$. Since the subnet $\mathcal{N}_y$ has only unobservable transitions, then $\mathcal{N}_y$ is cycle free. As a result, there exists $\sigma'' \in T_y^*$ such that $M' \xrightarrow{\sigma''} M''$ and $\#(\sigma'') = y$ by Lemma 1. Hence, the sequence $\sigma' t \sigma''$ with $\#(\sigma' t \sigma'') = \nu$ has no fault. Likewise, we can prove that if $\#(\mathbf{s}) \models R'_i$, there exists another sequence having a fault. Since there are two sequences having the same $\mathbf{s}$ but one has a fault and the other has no, then we have an *Uncertain* state.

Case 2 (when the most recent diagnosis state is *Uncertain* ($\Delta(\omega, T_f^i) = \textit{Uncertain}$)): If $\#(\mathbf{s}) \models R_i$, then there exists a valuation $(\alpha_{k+1}, \ldots, \alpha_n)$ of $(x_{k+1}, \ldots, x_n)$ such that $\nu = (\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$ and $\nu \models I \cup \{\mathbf{c}_i\}$ by Theorem 1. If $\nu \models I \cup \{\mathbf{c}_i\}$, then $\nu \models I$, i.e., $M'' = M_0 + A\nu \geq \vec{0}$. Since we have *Uncertain* state during observing ω, i.e., the most recent diagnosis state is *Uncertain*, and t is an observable transition, then we still have the same state for any sequence $\sigma' t$ such that $M_0 \xrightarrow{\sigma' t} M'$ and $\pi(\sigma') = \omega$. Assuming $y = \nu - \#(\sigma' t)$, $y \in \mathbb{N}^n$, then $M'' = M' + Ay \geq \vec{0}$. Since the subnet $\mathcal{N}_y$ has only unobservable transitions, then $\mathcal{N}_y$ is cycle free. As a result,

TABLE I
THE SETS OF INEQUALITIES RESULTING FROM APPLYING THE IFME METHOD IN EXAMPLE 2

R_1	R'_1	R_2	R'_2
$x_4 \leq 0$	$x_4 - x_6 \leq 1$	$x_4 - x_6 \leq 1$	$x_4 - x_6 \leq 1$
$x_4 - x_6 \leq 1$	$-x_3 + x_6 \leq 0$	$x_3 + x_6 \leq 0$	$-x_3 + x_6 \leq 0$
$-x_3 + x_6 \leq 0$	$-x_3 + x_4 \leq 0$	$-x_3 + x_4 \leq 0$	$-x_3 + x_4 \leq 0$
$-x_3 + x_4 \leq 0$	$x_3 - x_6 \leq 2$	$-x_4 + x_6 \leq 0$	$-x_3 + 2x_4 - x_6 \leq 0$
$x_3 - x_6 \leq 2$	$x_3 - x_4 - x_6 \leq 1$	$x_3 - x_4 \leq 1$	$2x_4 - 2x_6 \leq 1$
$x_3 - x_4 - x_6 \leq 2$	$x_3 - x_6 \leq 2$	$x_3 - x_6 \leq 2$	$x_3 - x_6 \leq 2$
$-x_4 - x_6 \leq 1$		$x_3 - x_4 - x_6 \leq 0$	$x_3 - x_4 - x_6 \leq 2$
			$-x_4 - x_6 \leq 1$

there exists $\sigma'' \in T_y^*$ such that $M' \xrightarrow{\sigma''} M''$ and $\#(\sigma'') = v$ by Lemma 1. Hence, the sequence $\sigma' t \sigma''$ with $\#(\sigma' t \sigma'') = v$ has no fault. Similarly, we can prove that if $\#(\mathbf{s}) \vDash R'_i$, there exists another sequence having a fault. Since there are two sequences having the same $\mathbf{s}$ but one has a fault and the other has no, then we have an *Uncertain* state.

□

Remark 3: a) the proofs of the states *NoFault* and *Faulty* in Theorem 2 are still valid for Petri nets which have cycle of unobservable transitions; b) it is not possible that $\#(\mathbf{s}) \nvDash R$ and $\#(\mathbf{s}) \nvDash R'$ simultaneously.

Example 2. Recall the Petri net of Fig. 1. Since we have two fault types, two pairs of sets of inequalities representing the diagnoser are created using the IFME method as shown in Table I. The pair (R_1, R'_1) expresses fault type T_f^1 and (R_2, R'_2) corresponds to T_f^2.

Suppose that the diagnoser observes no sequence ($\mathbf{s} = \varepsilon$), then $\Delta(\mathbf{s}, T_f^1) = \Delta(\mathbf{s}, T_f^2) = \textit{Uncertain}$ because $\#(\mathbf{s})$ satisfies R_1, R'_1, R_2 and R'_2 and the most recent diagnosis state is *NoFault* (see Theorem 2). In effect, the empty sequence ε might correspond to two other sequences, $\sigma_1 = t_1$ and $\sigma_2 = t_2$. In this case, for both fault types, there exist two sequences having the same observation, one of them has a fault but the other does not. Note that observing the sequence t_3 yields the same diagnosis state of the empty sequence ε. However, the most recent diagnosis state in this case is $\Delta(\varepsilon, T_f^1) = \Delta(\varepsilon, T_f^2) = \textit{Uncertain}$.

Assume now that the sequence $\mathbf{s} = t_3 t_4$ is observed, then $\Delta(\mathbf{s}, T_f^1) = \textit{Faulty}$, but $\Delta(\mathbf{s}, T_f^2) = \textit{NoFault}$. The diagnoser estimates such a state because $\#(\mathbf{s})$ satisfies R'_1 and R_2, but it does not satisfy R_1 and R'_2. In other words, all sequences $\sigma_1 = t_1 t_3 t_4 t_7$, $\sigma_2 = t_3 t_1 t_4 t_7$ with $\pi(\mathbf{s}) = t_3 t_4$ have a fault from type T_f^1, but no fault from the type T_f^2 appears in these sequences.

Finally, let us explore the case where the sequence $\mathbf{s} = t_3 t_6$ is observed. In this case, we have $\Delta(\mathbf{s}, T_f^1) = \textit{Uncertain}$ and $\Delta(\mathbf{s}, T_f^2) = \textit{Faulty}$. The set of sequences having $\pi(\mathbf{s}) = t_3 t_6$ is $\{t_3 t_2 t_5 t_6, t_2 t_3 t_5 t_6, t_3 t_2 t_5 t_6 t_1, t_2 t_3 t_5 t_6 t_1, t_3 t_2 t_5 t_6 t_2, t_2 t_3 t_5 t_6 t_2\}$. All of these sequences have a fault from type T_f^2 but only some of them have a fault from type T_f^1. Consequently, $\#(\mathbf{s})$ satisfies R_1, R'_1 and R'_2, but does not satisfy R_2. With regards to the fault type T_f^1, the most recent diagnosis state of the sequence $\mathbf{s} = t_3 t_6$ is $\Delta(t_3, T_f^1) = \textit{Uncertain}$. Using Theorem 2, we have $\Delta(\mathbf{s}, T_f^1) = \textit{Uncertain}$.

V. CONCLUSION

In this paper, a new approach is proposed to address the fault diagnosis problem in discrete event systems modelled by Petri nets. The systems under study are partially observable where faults are modelled as unobservable transitions. In this new approach, we present a different technique by which the diagnoser is represented as a pair of sets of inequalities in variables representing the number of firing observable transitions. This technique adopts the IFME method used to eliminate the variables corresponding to unobservable transitions and produce the sets of inequalities expressing the diagnoser. One set is used to ensure the normal state and the other is for the faulty state. The proposed approach has been applied to Petri net models where no cycle of unobservable transitions exists. More importantly, our approach can be applied to both bounded and unbounded Petri nets. The computational complexity of the proposed approach now relies on the number of unobservable transitions and not on the number of states in the system being analysed. Currently, we are working on an extension of our approach to labelled Petri nets.

REFERENCES

[1] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis, "Diagnosability of discrete-event systems," *IEEE Transactions on Automatic Control*, vol. 40, no. 9, pp. 1555–1575, 1995.

[2] S. Genc and S. Lafortune, "Distributed diagnosis of Place-Bordered Petri nets," *IEEE Transactions on Automatic Science and Enginnering*, vol. 4, no. 2, pp. 206–219, 2007.

[3] M. P. Cabasino, A. Giua, and C. Seatzu, "Fault detection for discrete event systems using petri nets with unobservable transitions," *Automatica*, vol. 46, no. 9, pp. 1531–1539, 2010.

[4] F. Basile, P. Chiacchiot, and G. D. Tommasi, "Sufficient conditions for diagnosability of petri nets," in *2008 9th International Workshop on Discrete Event Systems*, May 2008, pp. 370–375.

[5] M. Dotoli, M. P. Fanti, A. M. Mangini, and W. Ukovich, "On-line fault detection of discrete event systems by Petri nets and integer linear programming," *Automatica*, vol. 45, no. 11, pp. 2665–2672, 2009.

[6] G. Jiroveanu, R. K. Boel, and B. Bordbar, "On-line monitoring of large Petri net models under partial observation," *Discrete Event Dynamic Systems*, vol. 18, pp. 323–354, 2008.

[7] F. Basile, P. Chiacchio, and G. De Tommasi, "An efficient approach for online diagnosis of discrete event systems," *Automatic Control, IEEE Transactions on*, vol. 54, no. 4, pp. 748–759, 2009.

[8] A. Al-Ajeli and B. Bordbar, "Fourier-motzkin method for failure diagnosis in petri net models of discrete event systems," in *Proceedings of the 13th International Workshop on Discrete Event Systems*, Xi'an, China, 2016, pp. 165–170.

[9] H. W. Kuhn, "Solvability and consistency for linear equations and inequalities," *The American Mathematical Monthly*, vol. 63, no. 4, pp. 217–232, 1956.

[10] D. A. Kohler, "Projections of convex polyhedral sets." DTIC Document, Tech. Rep., 1967.

[11] R. Duffin, "On fourier's analysis of linear inequality systems," in *Pivoting and Extension*, ser. Mathematical Programming Studies, M. Balinski, Ed. Springer Berlin Heidelberg, 1974, vol. 1, pp. 71–95. [Online]. Available: http://dx.doi.org/10.1007/BFb0121242

[12] H. P. Williams, "Fourier-motzkin elimination extension to integer programming problems," *Journal of Combinatorial Theory, Series A*, vol. 21, no. 1, pp. 118–123, 1976.

[13] W. Pugh, "The omega test: a fast and practical integer programming algorithm for dependence analysis," in *Proceedings of the 1991 ACM/IEEE conference on Supercomputing*. ACM, 1991, pp. 4–13.

[14] T. Murata, "Petri nets: Properties, analysis and applications," *Proceedings of the IEEE*, vol. 77, no. 4, pp. 541–580, April 1989.

[15] K. Tsuji and T. Murata, "On reachability conditions for unrestricted petri nets," in *Circuits and Systems, 1993., ISCAS'93, 1993 IEEE International Symposium on*. IEEE, 1993, pp. 2713–2716.