

DIAGNOSE ONLINE EM SISTEMAS A EVENTOS DISCRETOS MODELADOS POR REDES DE PETRI ACÍCLICAS ROTULADAS

PEDRO R R PAIVA*, LILIAN KAWAKAMI CARVALHO*, JOÃO CARLOS BASILIO*

**Universidade Federal do Rio de Janeiro, COPPE, Programa de Engenharia Elétrica
Rio de Janeiro, RJ, Brasil*

Emails: pedrorrpaiva@gmail.com, lilian@dee.ufrj.br, basilio@dee.ufrj.br

Abstract— We discuss in this paper a new method for fault diagnosis in discrete event systems (DES) modeled by acyclic labeled Petri nets, in which different transitions can be labeled by the same event. The proposed online diagnoser makes its decision about the occurrence of failure by storing the sequence of observed events and verifying, after each occurrence of an observable event, whether three sets of inequalities are satisfied: two sets represent the normal behavior of the system, while the third one defines the faulty behavior of the system. The online diagnostic method proposed in this work has the advantage over those previously proposed because they are based only on the verification of sets of inequalities requiring no knowledge of the automaton theory, being self-contained within the formalism of the Petri net.

Keywords— Discrete event systems, Petri net, Fault diagnosis.

Resumo— Abordamos neste artigo um novo método para diagnose de falhas em sistemas a eventos discretos (SED) modelados por redes de Petri acíclicas rotuladas nas quais diferentes transições podem ser rotuladas por um mesmo evento. O diagnosticador online proposto toma sua decisão quanto à ocorrência de uma falha armazenando a sequência de eventos observados e verificando, após cada ocorrência de evento observável, se três conjuntos de desigualdades são satisfeitos: dois conjuntos representam o comportamento normal do sistema, enquanto o terceiro define o comportamento após a falha do sistema. O método de diagnose online proposto neste trabalho tem a vantagem sobre os anteriormente propostos por se basearem apenas na verificação de conjuntos de desigualdades não requerendo nenhum conhecimento da teoria do autômato, sendo auto-contido dentro do formalismo da rede de Petri.

Palavras-chave— Sistemas a eventos discretos, Rede de Petri, Diagnose de falhas.

1 Introdução

A diagnose de falhas em sistemas a eventos discretos tem sido uma área de pesquisa muito ativa nas últimas décadas (ver Zaytoon and Lafortune (2013) que apresentam uma revisão bastante completa da literatura sobre o assunto). Esta área de estudo busca encontrar formas eficientes e confiáveis de detectar ocorrências de falhas e seu isolamento. Uma falha é definida como qualquer desvio de um sistema do seu comportamento normal ou desejado. A atividade de pesquisa nessa área foi impulsionada pelas necessidades de diversos campos de aplicação, tais como: controle de processos, sistemas de controle, transporte, redes de comunicação, engenharia de software e outros. A necessidade de procedimentos eficazes para detectar ocorrências de falhas é bastante evidente se considerarmos suas consequências e impactos nessas áreas.

A diagnose de falhas é o processo de detecção de uma anormalidade no comportamento do sistema. Uma falha ou anormalidade é definida como qualquer desvio de um sistema de seu comportamento normal ou desejado e são inevitáveis nos ambientes industriais atuais. A diagnose de falha consiste em verificar o comportamento do sistema após cada ocorrência de evento observável e emitir um veredito como "normal" ou "com falha" ou "incerteza".

Trabalhos iniciais nesta área usando autômatos podem ser encontrados na literatura (Zaytoon and Lafortune (2013) e referências). A aplicação de um autômato, embora apropriado para modelar um sistema, traz problemas de complexidade para a diagnose em grandes sistemas, limitando sua utilização a peque-

nos sistemas. Para lidar com o problema da explosão de estados, as redes de Petri têm sido cada vez mais utilizadas para descrever um SED, uma vez que este tipo de modelagem oferece vantagens significativas devido à sua representação gráfica e matemática (Murata, 1989). Além disso, o conceito de estados (marcações) e ações (transições) reduz a complexidade computacional envolvida na resolução de um problema de diagnose.

A diagnose de falhas utilizando redes de Petri pode ser dividido em duas abordagens diferentes (Zaytoon and Lafortune (2013)): a primeira é através da análise de acessibilidade da marcação de locais observáveis (Hadjicostis and Verghese, 2002; Lefebvre and Delherm, 2007; Miyagi and Riascos, 2006; Ramírez-Treviño et al., 2007); A outra abordagem é baseada no conjunto de transições observáveis (Basile et al., 2009; Benveniste et al., 2003; Cabasino et al., 2011; Dotoli et al., 2009; Genc and Lafortune, 2007; Manyari-Rivera et al., 2007). Nossa metodologia se encaixa na segunda abordagem.

Dotoli et al. (2009) e Basile et al. (2009) consideram o problema da diagnose através da modelagem das falhas como transições não observáveis e propõe um diagnóstico online que observa sequências de eventos observáveis e emite uma decisão sobre a ocorrência de falha com base na solução de um problema de programação linear inteira. Ambos os artigos supõem que duas transições diferentes não podem ser rotuladas pelo mesmo evento.

Cabasino et al. (2014) abordam o problema da diagnose de falhas para redes de Petri ilimitadas e propõe um método de verificação inspirado no diagnosti-

gador que é um autômato de estados finitos propostos por Sampath et al. (1995) e fornece condições necessárias e suficientes para diagnosticabilidade. Jiroveanu and Boel (2010) obtiveram um resultado semelhante de forma independente. Manyari-Rivera et al. (2007) propõem um autômato diagnosticador online para SED modelado por redes de Petri ilimitadas. Al-Ajeli and Bordbar (2016) propõem um diagnosticador online para diagnose de falhas em redes de Petri acíclicas não rotuladas baseado na equação de estado.

Neste artigo, abordamos o problema da diagnose online inspirado no trabalho de Al-Ajeli and Bordbar (2016). Neste sentido, consideramos redes de Petri acíclicas rotuladas, nas quais, transições diferentes podem ser rotuladas pelo mesmo evento (observável, não observável e falha) e é proposto um novo diagnosticador online que toma sua decisão quanto à ocorrência da falha verificando, após cada ocorrência de evento observável, se três conjuntos de desigualdades são satisfeitos: dois conjuntos representam o comportamento normal do sistema, enquanto o terceiro representa o comportamento após a falha do sistema. O método proposto tem a vantagem sobre os anteriormente propostos por se basearem apenas na verificação de conjuntos de desigualdades não requerendo nenhum conhecimento da teoria do autômato, sendo auto-contido dentro do formalismo da rede de Petri.

Este artigo está organizado da seguinte forma. Na seção 2, apresentamos conceitos preliminares sobre redes de Petri e diagnosticabilidade de SED. Na seção 3, obtemos conjuntos de desigualdades a partir da equação de estado associada à rede de Petri. Na seção 4, propomos condições necessárias e suficientes para a diagnose online que se baseia nos conjuntos de desigualdades desenvolvidos na seção anterior. Finalmente, na seção 5, apresentamos as conclusões.

2 Noções Preliminares

2.1 Rede de Petri

Uma rede de Petri é uma 4-tupla $\mathcal{N} = (P, T, F, W)$ onde $P = \{p_1, \dots, p_m\}$ é um conjunto finito de lugares, $T = \{t_1, t_2, \dots, t_n\}$ é um conjunto finito de transições, $F \subseteq (P \times T) \cup (T \times P)$ é um conjunto de arcos e $W : F \rightarrow \{1, 2, 3, \dots\}$ é uma função de ponderação. Um estado de uma rede de Petri é representado pela função de marcação $M : P \rightarrow \mathbb{N}^m$ que captura o número de fichas em cada lugar; (\mathcal{N}, M_0) denota uma rede de Petri com marcação inicial M_0 . Se uma marcação M é acessível a partir de M_0 através de uma seqüência de transições $\sigma = t_1 \dots t_k$, denotada como $M_0 \xrightarrow{\sigma} M$, então existe um vetor x tal que a seguinte equação de estado é satisfeita:

$$M = M_0 + Ax, \quad (1)$$

em que $A = [a_{ij}] \in \mathbb{Z}^{m \times n}$ é a matriz de incidência, cujo elemento $a_{ij} = W(j, i) - W(i, j)$, com $W(j, i)$ (resp. $W(i, j)$) sendo o peso do arco da transição j (resp. lugar i) para o lugar i (resp. transição j) e $x = [x_1 \dots x_n]^T \in \mathbb{N}^n$ é o vetor de contagem de disparos,

em que x_i representa a quantidade de ocorrências da transição $t_i \in T$ na seqüência σ .

Uma rede de Petri que não tem circuitos dirigidos é chamada acíclica. É bem conhecido que, para as redes de Petri acíclicas, a equação de estado (1) não tem soluções espúrias (Murata, 1989).

Uma rede de Petri marcada com marcação inicial é definida como $\mathcal{N} = (P, T, F, W, E, \ell, M_0)$ em que (P, T, F, W) é uma rede de Petri, E é um conjunto de eventos, $\ell : T \rightarrow E$ é uma função de rotulagem de transição e M_0 é a marcação inicial. A função de rotulagem pode ser estendida para seqüências de modo que $\ell : T^* \rightarrow E^*$. A linguagem gerada pela rede de Petri \mathcal{N} é $\mathcal{L}(\mathcal{N}) = \{\ell(\sigma) \in E^* : (\exists M \in \mathbb{N}^m)[M_0 \xrightarrow{\sigma} M]\}$, em que M denota o estado acessível a partir de M_0 através da Equação (1).

Considerando $E = E_o \cup E_{uo}$ uma partição de E , em que E_o e E_{uo} são os conjuntos de eventos observáveis e não observáveis, respectivamente e definindo T_o e T_{uo} como os conjuntos de transições observáveis e não observáveis, respectivamente, i.e., $T_o = \{t \in T : (\exists e \in E_o)[\ell(t) = e]\}$ e $T_{uo} = \{t \in T : (\exists e \in E_{uo})[\ell(t) = e]\}$. Duas ou mais transições $t_1, t_2, \dots, t_n \in T$ são chamadas indistinguíveis se eles compartilham o mesmo rótulo, ou seja, $\ell(t_1) = \ell(t_2) = \dots = \ell(t_n) = e \in E$. Uma operação de linguagem importante é a projeção natural $P_o : E^* \rightarrow (E_o \cup \{\varepsilon\})^*$, que transforma seqüências não observáveis na seqüência vazia ε , i.e., $P_o(e) = \{\varepsilon\}$ para $e \in E_{uo}$, e $P_o(e) = e$, para $e \in E_o$, e $P_o(se) = P_o(s)P_o(e)$, $s \in E^*$ e $e \in E$.

2.2 Diagnosticabilidade

Seja $E_f \subseteq E_{uo}$ o conjunto de eventos de falha e consideramos, por uma questão de simplicidade, que há apenas um evento de falha, i.e., $E_f = \{f\}$. Seja $\Psi(E_f) = \{s \in \mathcal{L} : (\exists u \in (E \setminus f)^*)[s = uf]\}$ o conjunto de todas as seqüências finitas de L que terminam com o evento de falha f . Então, a linguagem \mathcal{L} é dita ser diagnosticável se a ocorrência de f puder ser detectada dentro de um número finito de eventos após sua ocorrência usando apenas seqüências formadas com eventos observáveis. Formalmente, a diagnosticabilidade da linguagem é definida como segue (Sampath et al., 1995).

Definição 1 Uma linguagem \mathcal{L} prefixo-fechada e viva é diagnosticável com relação à projeção P_o e $E_f = \{f\}$ se a seguinte relação for verdadeira:

$$(\exists n \in \mathbb{N})(\forall s \in \Psi(E_f))(\forall t \in \mathcal{L}/s)(\|t\| \geq n \Rightarrow D),$$

em que a condição de diagnosticabilidade D é

$$(\nexists \omega \in \mathcal{L})[(P_o(st) = P_o(\omega)) \wedge (f \notin \omega)] \quad (2)$$

Exemplo 1 Considere a rede de Petri rotulada $\mathcal{N} = (P, T, F, W, E, \ell, M_0)$ mostrada na Figura 1, em que $P = \{p_1, p_2, p_3, p_4, p_5\}$, $T = \{t_1, t_2, t_3, t_4, t_5, t_6\}$, $F = \{(p_1, t_1), (t_1, p_2), (p_2, t_2), (t_2, p_3), (p_3, t_3), (t_3, p_4),$

$(p_4, t_4), (p_1, t_5), (t_5, p_5), (p_5, t_6)\}$, $W(i, j) = 1, \forall (i, j) \in F, E = \{a, b, c, f\}, M_0 = [10000]^T$. A função de rotulação de transição ℓ é definida como: $\ell(t_1) = c, \ell(t_2) = \ell(t_6) = b, \ell(t_4) = \ell(t_5) = a$ e $\ell(t_3) = f$. Consideremos $E_o = \{a, b\}$ e $E_f = \{f\}$ como o conjunto de eventos observáveis e o conjunto de eventos de falha, respectivamente. Transições associadas a eventos observáveis são representadas por retângulos sólidos, enquanto retângulos vazios representam transições associadas a eventos não observáveis. Essas transições serão tratadas ao longo do texto como transições observáveis e não observáveis, respectivamente.

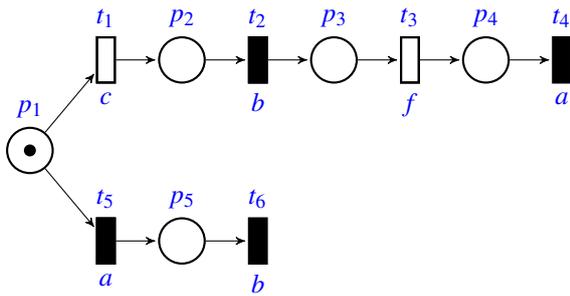


Figura 1: rede de Petri acíclica rotulada (\mathcal{N}, M_0)

A equação de estado para a rede de Petri da Figura 1 é dada por:

$$M = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} -1 & 0 & 0 & 0 & -1 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix}$$

Observe que as transições t_2 e t_6 são indistinguíveis porque estão rotuladas pelo evento b e as transições t_4 e t_5 também são indistinguíveis, já que estão rotuladas pelo evento a .

No exemplo, a ocorrência das seqüências de eventos $s_1 = cb$ ou $s_2 = cbf$ produz a seqüência b de eventos observáveis, portanto não podemos ter certeza se a falha ocorreu ou não. A ocorrência da seqüência de eventos $s_3 = ab$, por outro lado, produz a seqüência ab de eventos observáveis e, neste caso, temos certeza de que a falha não ocorreu porque não existe outra seqüência de eventos que contenha a falha com a mesma seqüência de eventos observáveis, assim estamos, neste caso, certos de que o sistema está em seu comportamento normal. A ocorrência de seqüência de eventos $s_4 = cbfa$ produz a seqüência ba de eventos observáveis e, neste caso, temos a certeza de que a falha ocorreu porque não existe outra seqüência de eventos que não contenha a falha e tenha a mesma seqüência de eventos observáveis.

2.3 Eliminação de variáveis em um sistema de desigualdades

A eliminação da n th variável em um sistema de desigualdades $-Ax \leq b$ em que $A \in \mathbb{Z}^{m \times n}$, $b \in \mathbb{N}^m$ e $x = (x_1, x_2, \dots, x_n) \in \mathbb{N}^n$ pode ser executado como proposto por (Duffin, 1974; Dantzig, 1972; Williams, 1976). Podemos obter todos os elementos na última coluna de $-A$ como $0, +1$ ou -1 multiplicando cada desigualdade por um escalar positivo e então, o conjunto de desigualdades pode ser reescrito como se segue,

$$\begin{aligned} a'_i x' &\leq b_i, i = 1, \dots, m_1 \\ a'_j x' - x_n &\leq b_j, j = m_1 + 1, \dots, m_2 \\ a'_k x' + x_n &\leq b_k, k = m_2 + 1, \dots, m \end{aligned} \quad (3)$$

em que $x' = (x_1, x_2, \dots, x_{n-1}) \in \mathbb{N}^{n-1}$. Assumimos que $L = \max(a'_j x' - b_j, j = m_1 + 1, \dots, m_2)$ e $U = \min(b_k - a'_k x', k = m_2 + 1, \dots, m)$. Desde que as duas últimas linhas na Equação 3 são equivalentes a $L \leq x_n \leq U$, então a variável x_n pode ser eliminada obtendo as desigualdades como se segue.

$$\begin{aligned} a'_i x' &\leq b_i, i = 1, \dots, m_1 \\ a'_j x' - b_j &\leq b_k - a'_k x', j = m_1 + 1, \dots, m_2, \\ k &= m_2 + 1, \dots, m \end{aligned} \quad (4)$$

Repetindo este processo, podemos sucessivamente eliminar as variáveis indesejadas.

3 Um modelo matemático para diagnose online

Nesta seção, apresentamos uma técnica matemática que será útil para a diagnose online em sistemas a eventos discretos parcialmente observados (SED) modelados por redes de Petri acíclicas rotuladas. No modelo proposto aqui, permitimos a existência de transições indistinguíveis (incluindo transições rotuladas pelo evento de falha).

O método começa com a equação de estado da rede de Petri dada pela Equação (1). Uma vez que cada marcação M de um estado acessível é não-negativa, *i.e.*, $M \geq 0$, a Equação (1) pode ser reescrita como:

$$M_0 + Ax \geq 0 \Rightarrow -Ax \leq M_0 \quad (5)$$

em que teremos um conjunto de desigualdades nas componentes x_i do vetor de contagem de disparos x . Denotaremos S como o conjunto formado por essas desigualdades e as desigualdades $-x_i \leq 0$ porque o número de disparos de uma certa transição não pode ser negativo.

A ocorrência ou não de uma transição rotulada por uma falha (ou transição de falha, para abreviar) pode ser escrita na forma de desigualdades, como se segue. Suponha que t_i é uma transição de falha e x_i a variável que representa o número de disparos de t_i numa seqüência de disparos σ . Então, a desigualdade $c := x_i \leq 0$, é satisfeita se σ não contém t_i . Da mesma forma, a negação dessa desigualdade, *i.e.*, $c' := x_i > 0$ é satisfeita se σ contém t_i .

Agora, considerando $T_f = \{t \in T : \ell(t) = f\}$ como o conjunto de transições de falha e $|\cdot|$ indicando a cardinalidade de um conjunto, então, quando $|T_f| > 1$, podemos definir as desigualdades c e c' como se segue:

$$c := \sum_{x_i: t_i \in T_f} x_i \leq 0 \quad \wedge \quad c' := \sum_{x_i: t_i \in T_f} x_i > 0 \quad (6)$$

Adicionando as desigualdades c e c' ao conjunto S separadamente, produzimos dois novos conjuntos de desigualdades denominados de $S \oplus c$ e $S \oplus c'$. Se nenhuma falha ocorrer em uma seqüência de eventos s , todas as desigualdades em $S \oplus c$ serão satisfeitas, mas não aquelas em $S \oplus c'$. Por outro lado, se uma falha ocorrer em uma seqüência s , todas as desigualdades em $S \oplus c'$ serão satisfeitas, mas não aquelas em $S \oplus c$.

Consideremos agora que estamos interessados apenas nas seqüências de eventos que poderão ter um evento de falha no futuro e nas seqüências que possuem pelo menos um evento de falha. Podemos, então, adicionar um conjunto de desigualdades chamado c_f a $S \oplus c$ e $S \oplus c'$ que será composto de $x_i \leq 0$ para toda transição i que não pertence às seqüências de interesse. Produzimos, então, dois novos conjuntos de desigualdades $S \oplus c \oplus c_f$ e $S \oplus c' \oplus c_f$. Se nenhuma falha ocorrer em uma seqüência de eventos s que poderá ter um evento de falha no futuro, então, todas as desigualdades em $S \oplus c \oplus c_f$ serão satisfeitas, mas não aquelas em $S \oplus c' \oplus c_f$. Por outro lado, se um evento de falha ocorrer em uma seqüência s , então, todas as desigualdades em $S \oplus c' \oplus c_f$ serão satisfeitas, mas não aquelas em $S \oplus c \oplus c_f$.

Consideremos agora que estamos interessados nas seqüências de eventos que não têm um evento de falha, excluindo as seqüências que poderão ter um evento de falha no futuro. Desta forma, podemos adicionar um conjunto de desigualdades chamado c_n a $S \oplus c$ que será composto de $x_i \leq 0$ para toda transição i que não pertence às seqüências de interesse. Produzimos um novo conjunto de desigualdades denominado $S \oplus c \oplus c_n$. Se houver uma seqüência de eventos s que não tenha e que não possa ter, no futuro, um evento de falha, então, todas as desigualdades em $S \oplus c \oplus c_n$ serão satisfeitas caso contrário haverá pelo menos uma desigualdade não satisfeita.

Consideremos agora as transições indistinguíveis associadas aos eventos observáveis. Sendo $T_e = \{t \in T_o : \ell(t) = e\}$ o conjunto de transições observáveis rotuladas pelo evento e . Se $|T_e| = 1$, então para x_i tal que $t_i \in T_e$, substituímos $x_i = y_e$. Por outro lado, se $|T_e| > 1$, então adicionamos as seguintes restrições aos conjuntos $S \oplus c \oplus c_f$, $S \oplus c' \oplus c_f$ e $S \oplus c \oplus c_n$.

$$y_e = \sum_{x_i: t_i \in T_e} x_i, \quad y_e \geq 0. \quad (7)$$

Como $S \oplus c \oplus c_f$, $S \oplus c' \oplus c_f$ e $S \oplus c \oplus c_n$ são formados por desigualdades, devemos transformar a igualdade da Equação (7) em duas desigualdades, da seguinte forma:

$$\sum_{x_i: t_i \in T_e} x_i \geq y_e \quad \wedge \quad \sum_{x_i: t_i \in T_e} x_i \leq y_e. \quad (8)$$

Como estamos trabalhando com sistemas a eventos discretos parcialmente observados, a quantidade de ocorrências de eventos não observáveis não é conhecida em uma seqüência s , sendo conhecida, apenas, a quantidade de ocorrências dos eventos observáveis. Podemos então aplicar um método de eliminação de variáveis nos conjuntos $S \oplus c \oplus c_f$, $S \oplus c' \oplus c_f$ e $S \oplus c \oplus c_n$ para eliminar todas as variáveis x , deixando apenas as variáveis y_e . Os conjuntos resultantes de desigualdades serão denotados como AF , PF e SF , respectivamente.

A formação dos sistemas de desigualdades AF , PF e SF está resumido no Algoritmo 1 e a equivalência entre o modelo descrito pela Equação 1 e os sistemas de desigualdades AF , PF e SF é garantido pelo seguinte resultado.

Teorema 1 (Duffin, 1974) *Suponha que as variáveis $x_{k+1}, x_{k+2}, \dots, x_n$ foram eliminadas aplicando um método de eliminação de variáveis a partir de um conjunto de desigualdades lineares \mathcal{A} com variáveis x_1, \dots, x_n resultando no conjunto reduzido \mathcal{B} com as variáveis x_1, \dots, x_k . Então $\alpha_1, \dots, \alpha_k$ é uma solução de \mathcal{B} , se e somente se, existem valores $\alpha_{k+1}, \dots, \alpha_n$, tal que $\alpha_1, \dots, \alpha_k, \alpha_{k+1}, \dots, \alpha_n$ é uma solução de \mathcal{A} .*

Algoritmo 1 Algoritmo para determinar AF , PF e SF

Entrada:

- $\mathcal{N} = (P, T, F, W, E, \ell, M_0)$: Modelo rede Petri rotulada
- T_o, T_{uo}, T_f : Conjuntos de transições observáveis, não observáveis e de falhas respectivamente

Saída: AF , PF e SF : Conjunto de desigualdades com variáveis que quantificam as ocorrências dos eventos observáveis

1: Determinar a equação de estado da rede de Petri \mathcal{N} ,

$$M = M_0 + Ax$$

2: Formar o conjunto S das desigualdades $-Ax \leq M_0$ e $x_i \leq 0$

3: Determinar $T_f = \{t \in T : \ell(t) = f\}$ e então, as restrições c e c' que modela a ocorrência de falhas.

$$c := \sum_{x_i: t_i \in T_f} x_i \leq 0 \quad \wedge \quad c' := \sum_{x_i: t_i \in T_f} x_i > 0$$

4: Formar os conjuntos $S \oplus c$ e $S \oplus c'$

5: Determinar o conjunto c_f composto das desigualdades $x_i \leq 0$ relacionadas às transições i que não estão contidas nas seqüências de eventos que possam ter, no futuro, um evento de falha e nas seqüências que possuem pelo menos um evento de falha.

- 6: Formar os conjuntos $S \oplus c \oplus c_f$ e $S \oplus c' \oplus c_f$
- 7: Determinar o conjunto c_n composto das desigualdades $x_i \leq 0$ relacionadas às transições i que não estão contidas nas seqüências de eventos que não tenham um evento de falha excluindo as seqüências que poderão ter, no futuro, um evento de falha.
- 8: Formar o conjunto $S \oplus c \oplus c_n$
- 9: Para todo $e \in E$, determinar $T_e = \{t \in T_o : \ell(t) = e\}$

- Se $|T_e| = 1$, estabeleça $x_i = y_e$
- Se $|T_e| > 1$, adicione as seguintes desigualdades aos conjuntos $S \oplus c \oplus c_f$, $S \oplus c' \oplus c_f$ e $S \oplus c \oplus c_n$

$$\sum_{x_i: t_i \in T_e} x_i \geq y_e \wedge \sum_{x_i: t_i \in T_e} x_i \leq y_e.$$

- 10: Determinar os conjuntos AF , PF e SF através da aplicação de um método de eliminação de variáveis aos conjuntos $S \oplus c \oplus c_f$, $S \oplus c' \oplus c_f$ e $S \oplus c \oplus c_n$, eliminando todas as variáveis x e deixando somente as variáveis y_e .

Exemplo 2 A rede de Petri mostrada na Figura 1 será usada para ilustrar a aplicação do modelo matemático proposto baseado em conjuntos de desigualdades. As restrições c e c' serão $x_3 \leq 0$ e $x_3 > 0$ respectivamente. O conjunto de restrições c_f será composto de $x_5 \leq 0$ e $x_6 \leq 0$. O conjunto de restrições c_n será composto de $x_1 \leq 0$, $x_2 \leq 0$, $x_3 \leq 0$ e $x_4 \leq 0$. Consideremos agora as transições indistinguíveis associadas aos eventos observáveis na Figura 1, vemos que $T_a = \{t_4, t_5\}$ e $T_b = \{t_2, t_6\}$. Portanto, uma vez que $|T_a| = 2$ e $|T_b| = 2$, devemos adicionar as seguintes desigualdades aos conjuntos $S \oplus c$ e $S \oplus c'$:

$$x_4 + x_5 \geq y_a \wedge x_4 + x_5 \leq y_a.$$

e

$$x_2 + x_6 \geq y_b \wedge x_2 + x_6 \leq y_b.$$

A Tabela 1 mostra o conjunto de desigualdades que representa $S \oplus c \oplus c_f$, $S \oplus c' \oplus c_f$ e $S \oplus c \oplus c_n$ com a inclusão das restrições necessárias para a mudança de variáveis

Eliminando todas as variáveis x , deixando apenas as variáveis y_e nos conjuntos $S \oplus c \oplus c_f$, $S \oplus c' \oplus c_f$ e $S \oplus c \oplus c_n$, obtemos os conjuntos reduzidos AF , PF e SF descritos na Tabela 2.

4 Diagnose online

Vamos agora introduzir um novo diagnosticador online para redes de Petri acíclicas rotuladas. Seja s a seqüência de eventos e $s_o = P_o(s)$ a seqüência correspondente de eventos observáveis. A diagnose que propomos tem três estados: (i) N , se tivermos certeza que o evento de falha não ocorreu; (ii) F , se tivermos certeza de que ocorreu um evento de falha e (iii) FN , se houver dúvida da ocorrência de um evento de falha.

Vamos assumir que $E_o = \{e_1, e_2, \dots, e_p\}$. Portanto, associado a cada seqüência $s \in \mathcal{L}(\mathcal{N}, M_0)$ existe um vetor $v(s_o) = [y_{e_1} y_{e_2} \dots y_{e_p}]^T$, em que $s_o = P_o(s)$ e y_{e_i} é a quantidade de ocorrências de e_i em s_o . O vetor $v(s_o)$ será referido como a valoração de s_o . O diagnosticador D será um mapeamento $D : \mathcal{L}(\mathcal{N}, M_0) \rightarrow \{N, F, FN\}$ definido da seguinte maneira:

$$D = \begin{cases} N, & \begin{array}{l} \text{(i) se } v(s_o) \not\models PF \text{ ou,} \\ \text{(ii) se } v(s_o) \not\models AF \wedge v(s_o) \models PF \wedge v(s_o) \models SF \\ \text{e na diagnose anterior ocorreu } D = N \end{array} \\ F, & \begin{array}{l} \text{(i) se } v(s_o) \not\models AF \wedge v(s_o) \models PF \wedge v(s_o) \not\models SF \text{ ou} \\ \text{(ii) se } v(s_o) \not\models AF \wedge v(s_o) \models PF \wedge v(s_o) \models SF \\ \text{e na diagnose anterior ocorreu:} \\ D = F \text{ ou } D = FN \wedge v(s'_o) \not\models SF \end{array} \\ FN, & \begin{array}{l} \text{(i) se } v(s_o) \models AF \wedge v(s_o) \models PF \text{ ou} \\ \text{(ii) se } v(s_o) \not\models AF \wedge v(s_o) \models PF \wedge v(s_o) \models SF \\ \text{e na diagnose anterior ocorreu:} \\ D = FN \wedge v(s'_o) \models SF \end{array} \end{cases}$$

em que s'_o representa a seqüência de eventos anterior a s_o . Os resultados mostram que a diagnose proposta é realmente capaz de diagnosticar qualquer ocorrência de falha em redes de Petri acíclicas rotuladas.

Prova: A prova é uma aplicação direta do Teorema 1, da seguinte forma:

1. $D = N$

(i) se $v(s_o) \not\models PF$, então, de acordo com Teorema 1, $v(s) \not\models S \oplus c' \oplus c_f$ implicando em que $f \notin s$.

(ii) se $v(s_o) \not\models AF$ e $v(s_o) \models PF$, então, de acordo com Teorema 1, $v(s) \not\models S \oplus c \oplus c_f$ e $v(s) \models S \oplus c' \oplus c_f$ e assim $f \in s$, mas por outro lado, como $v(s_o) \models SF$, então, de acordo com Teorema 1, $v(s) \models S \oplus c \oplus c_n$ e assim $f \notin s$. Desta forma, temos uma incerteza, mas recorrendo a diagnose anterior, caso tenha sido $D = N$ e como o evento de falha é não observável, não é possível termos $D = F$ imediatamente após $D = N$ sem termos antes $D = FN$ implicando em que $f \notin s$.

2. $D = F$

(i) se $v(s_o) \not\models SF$, então, de acordo com Teorema 1, $v(s) \not\models S \oplus c \oplus c_n$ e temos certeza que a seqüência s tem ou poderá ter no futuro um evento de falha, por outro lado como $v(s_o) \not\models AF$ e $v(s_o) \models PF$, então, de acordo com Teorema 1, $v(s) \not\models S \oplus c \oplus c_f$ e $v(s) \models S \oplus c' \oplus c_f$ implicando em que $f \in s$.

(ii) se $v(s_o) \not\models AF$, $v(s_o) \models PF$ e $v(s_o) \models SF$, então como visto no caso (ii) para $D = N$, temos uma incerteza, mas recorrendo a diagnose anterior, caso tenha sido $D = F$ não temos dúvida de que $f \in s$. Caso tenha sido $D = FN$ e a seqüência observada anterior tivesse nos dado o resultado $v(s'_o) \not\models SF$, então, de acordo com Teorema 1, já possuíamos a certeza que a seqüência s poderia ter no futuro um evento de falha mas não a certeza sobre a ocorrência do evento de falha, que é desfeita com o resultado atual $v(s_o) \not\models AF$ e $v(s_o) \models PF$ implicando em que $f \in s$.

Tabela 1: Conjunto de desigualdades do exemplo da Figura 1

conjunto $S \oplus c \oplus c_f$	conjunto $S \oplus c' \oplus c_f$	conjunto $S \oplus c \oplus c_n$
conjunto S	conjunto S	conjunto S
$x_1 + x_5 \leq 1$	$x_1 + x_5 \leq 1$	$x_1 + x_5 \leq 1$
$-x_1 + x_2 \leq 0$	$-x_1 + x_2 \leq 0$	$-x_1 + x_2 \leq 0$
$-x_2 + x_3 \leq 0$	$-x_2 + x_3 \leq 0$	$-x_2 + x_3 \leq 0$
$-x_3 + x_4 \leq 0$	$-x_3 + x_4 \leq 0$	$-x_3 + x_4 \leq 0$
$-x_5 + x_6 \leq 0$	$-x_5 + x_6 \leq 0$	$-x_5 + x_6 \leq 0$
$-x_i \leq 0$	$-x_i \leq 0$	$-x_i \leq 0$
$i \in \{1, \dots, 6\}$	$i \in \{1, \dots, 6\}$	$i \in \{1, \dots, 6\}$
restrição c	restrição c'	restrição c
$x_3 \leq 0$	$-x_3 \leq -1$	$x_3 \leq 0$
restrições c_f	restrições c'_f	restrições c_n
$x_j \leq 0$	$x_j \leq 0$	$x_k \leq 0$
$j \in \{5, 6\}$	$j \in \{5, 6\}$	$k \in \{1, \dots, 4\}$
restrições para mudança de variáveis	restrições para mudança de variáveis	restrições para mudança de variáveis
$x_4 + x_5 - y_a \leq 0$	$x_4 + x_5 - y_a \leq 0$	$x_4 + x_5 - y_a \leq 0$
$y_a - x_4 - x_5 \leq 0$	$y_a - x_4 - x_5 \leq 0$	$y_a - x_4 - x_5 \leq 0$
$-y_a \leq 0$	$-y_a \leq 0$	$-y_a \leq 0$
$x_2 + x_6 - y_b \leq 0$	$x_2 + x_6 - y_b \leq 0$	$x_2 + x_6 - y_b \leq 0$
$y_b - x_2 - x_6 \leq 0$	$y_b - x_2 - x_6 \leq 0$	$y_b - x_2 - x_6 \leq 0$
$-y_b \leq 0$	$-y_b \leq 0$	$-y_b \leq 0$

Tabela 2: Conjunto de de desigualdades AF , PF e SF do exemplo da Figura 1

conjunto AF	conjunto PF	conjunto SF
$y_a \leq 0$	$y_a \leq 1$	$y_a \leq 1$
$y_b \leq 1$	$y_b \leq 1$	$y_b \leq 1$
$-y_a \leq 0$	$-y_a \leq 0$	$-y_a \leq 0$
$-y_b \leq 0$	$-y_b \leq -1$	$-y_b \leq 0$
$y_a + y_b \leq 1$	$y_a - y_b \leq 0$	$y_a + y_b \leq 2$
$y_a - y_b \leq 0$	$-y_a + y_b \leq 1$	$y_a - y_b \leq 1$
$-y_a + y_b \leq 1$		$-y_a + y_b \leq 0$

3. $D = FN$

(i) se $v(s_o) \models AF$ e $v(s_o) \models PF$, então, de acordo com Teorema 1, $v(s) \not\models S \oplus c \oplus c_f$ e $v(s) \not\models S \oplus c' \oplus c_f$ e o resultado nos mostra que a sequência s tem ou poderá ter no futuro um evento de falha. Desta forma, temos uma incerteza e não é possível recorrer a diagnose anterior para termos certeza com relação a ocorrência ou não de uma falha.

(ii) se $v(s_o) \not\models AF$, $v(s_o) \models PF$ e $v(s_o) \models SF$, então como visto no caso (ii) para $D = N$, temos uma incerteza, que se mantém no caso da diagnose anterior tenha sido $D = FN$ e a sequência observada anterior tivesse nos dado o resultado $v(s'_o) \models SF$, então, de acordo com Teorema 1, o resultado anterior teria nos dado que a sequência s poderia não ter no futuro um evento de falha ou que ela já tivesse um evento de falha, que é mantida com o resultado atual $v(s_o) \models SF$.

Exemplo 3 Vamos agora ilustrar a aplicação da diagnose proposta neste trabalho na rede de Petri mostrada na Figura 1. Vemos que a ocorrência da sequência de eventos $s_1 = cb$ ou $s_2 = cbf$ produz a mesma sequência $s_o = b$ de eventos observáveis, o que implica em $y_a = 0$ e $y_b = 1$. Usando esses valores na Tabela 2, observamos que os conjuntos AF e PF são satisfeitos e que SF não é satisfeito, o que nos leva a $D(s_o) = FN$. Assim, o diagnosticador não está certo de que a falha ocorreu.

A ocorrência da sequência $s_3 = a$ produz a sequência $s_o = a$ de eventos observáveis que implica em $y_a = 1$ e $y_b = 0$. Usando esses valores na Tabela 2, observamos que os conjuntos AF e PF não são satisfeitos e que SF é satisfeito, o que nos leva a $D(s_o) = N$. Assim, o diagnosticador está certo de que a falha não ocorreu.

A ocorrência da sequência $s_4 = cbfa$ produz a sequência $s_o = ba$ de eventos observáveis que implica em $y_a = 1$ e $y_b = 1$. Usando esses valores na Tabela 2, observamos que os conjuntos PF e SF são satisfeitos e que AF não é satisfeito, o que nos leva a $D(s_o) = F$ porque na diagnose anterior para a sequência cbf obtivemos os conjuntos AF e PF sendo satisfeitos e SF não sendo satisfeito. Assim, o diagnosticador está certo de que a falha ocorreu.

A Tabela 3 mostra todas as sequências de eventos que podem ocorrer no SED em análise e a diagnose na respectiva sequência de eventos observáveis.

Tabela 3: Diagnose do exemplo da Figura 1

s	$s_o = P_o(s)$	$v(s_o) \models AF$	$v(s_o) \models PF$	$v(s_o) \models SF$	$D(s_o)$
ε	ε	sim	não	sim	N
c	ε	sim	não	sim	N
cb	b	sim	sim	não	FN
cbf	b	sim	sim	não	FN
$cbfa$	ba	não	sim	sim	F
a	a	não	não	sim	N
ab	ab	não	sim	sim	N

5 Conclusão

Neste trabalho, propomos uma novo diagnosticador online para sistemas a eventos discretos modelados por redes de Petri acíclicas rotuladas. A diagnose de falha baseia-se na verificação de conjuntos de desigualdades nas variáveis que representam a quantidade de ocorrências dos eventos observáveis e nos fornece o status do comportamento do sistema: normal, com falha e incerto. Um trabalho que está sendo realizado é estender a abordagem aqui proposta para outros tipos de redes de Petri.

Referências

- Al-Ajeli, A. and Bordbar, B. (2016). Fourier-Motzkin method for failure diagnosis in Petri net models of discrete event systems, *13th International Workshop on Discrete Event Systems*, Xi'an, China, pp. 165–170.
- Basile, F., Chiacchio, P. and De Tommasi, G. (2009). An efficient approach for online diagnosis of discrete event systems, *IEEE Trans. on Automatic Control* **54**(4): 748–759.
- Benveniste, A., Fabre, E., Haar, S. and Jard, C. (2003). Diagnosis of asynchronous discrete-event systems: a net unfolding approach, *IEEE Trans. on Automatic Control* **48**(5): 714–727.
- Cabasino, M. P., Giua, A., Pocci, M. and Seatzu, C. (2011). Discrete event diagnosis using labeled Petri nets. An application to manufacturing systems, *Control Engineering Practice* **19**(9): 989–1001.
- Cabasino, M. P., Giua, A. and Seatzu, C. (2014). Diagnosability of discrete-event systems using labeled Petri nets, *IEEE Trans. on Automation Science and Engineering* **11**(1): 144–153.
- Dantzig, G. B. (1972). Fourier-Motzkin elimination and its dual, *Technical report*, DTIC Document.
- Dotoli, M., Fanti, M. P., Mangini, A. M. and Ukovich, W. (2009). On-line fault detection in discrete event systems by Petri nets and integer linear programming, *Automatica* **45**(11): 2665–2672.
- Duffin, R. (1974). On Fourier’s analysis of linear inequality systems, *Pivoting and Extension*, Springer, pp. 71–95.
- Genc, S. and Lafortune, S. (2007). Distributed diagnosis of place-bordered Petri nets, *IEEE Trans. on Automation Science and Engineering* **4**(2): 206–219.
- Hadjicostis, C. N. and Verghese, G. C. (2002). Fault-tolerant computation in groups and semigroups: applications to automata, dynamic systems and Petri nets, *Journal of the Franklin Institute* **339**(4): 387–430.
- Jiroveanu, G. and Boel, R. K. (2010). The diagnosability of Petri net models using minimal explanations, *IEEE Trans. on Automatic Control* **55**(7): 1663–1668.
- Lefebvre, D. and Delherm, C. (2007). Diagnosis of DES with Petri net models, *IEEE Trans. on Automation Science and Engineering* **4**(1): 114–118.
- Manyari-Rivera, M., Basilio, J. C. and Bhaya, A. (2007). Integrated fault diagnosis based on Petri net models, *Proc. of the 16th IEEE International Conference on Control Applications*, Singapore, pp. 958–963.
- Miyagi, P. and Riascos, L. (2006). Modeling and analysis of fault-tolerant systems for machining operations based on Petri nets, *Control Engineering Practice* **14**(4): 397–408.
- Murata, T. (1989). Petri nets - properties, analysis and applications, *Proc. of the IEEE* **77**(4): 541–580.
- Ramírez-Treviño, A., Ruiz-Beltrán, E., Rivera-Rangel, I. and Lopez-Mellado, E. (2007). Online fault diagnosis of discrete event systems. a Petri net-based approach, *IEEE Trans. on Automation Science and Engineering* **4**(1): 31–39.
- Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K. and Teneketzis, D. (1995). Diagnosability of discrete-event systems, *IEEE Trans. on Automatic Control* **40**: 1555–1575.
- Williams, H. P. (1976). Fourier-Motzkin elimination extension to integer programming problems, *Journal of combinatorial theory, series A* **21**(1): 118–123.
- Zaytoon, J. and Lafortune, S. (2013). Overview of fault diagnosis methods for discrete event systems, *Annual Reviews in Control* **37**(2): 308–320.