DIAGNOSTICABILIDADE DE SISTEMAS HÍBRIDOS EMPREGANDO ANÁLISE DE ALCANÇABILIDADE

JÉSSICA S. VIEIRA[*], LILIAN K. CARVALHO[*], EDUARDO V. L. NUNES[*], ANTONIO E. C. DA CUNHA[†]

[*]*COPPE - Programa de Engenharia Elétrica*
Universidade Federal do Rio de Janeiro
Cidade Universitária, Ilha do Fundão, 21.945-970
Rio de Janeiro, RJ, Brasil

[†]*Programa de Pós-Graduação em Engenharia de Defesa (PGED)*
Instituto Militar de Engenharia (IME)
Praça General Tibúrcio, 80, Praia Vermelha, 22.290-270, Rio de Janeiro, RJ, Brasil

Emails: jessica.vieira@poli.ufrj.br, lilian.carvalho@poli.ufrj.br, eduardo@coep.ufrj.br, carrilho@ime.eb.br

Abstract— This paper addresses a first proposal of diagnosability of Hybrid Systems (HS) using reachability analysis, a technique broadly applied in verification of properties in HS. To this end, a new definition of diagnosability that combines the diagnosability of Discrete Event Systems (DES) with the reachability analysis to compare the continuous behavior is presented. Furthermore, a case study to carry out diagnosability analyses of HS inspired by a classical DES example is deployed to show the advantage of performing the diagnosability analysis of the states associated with continuous-time dynamics of the hybrid system to make the fault diagnosable.

Keywords— Hybrid systems, Reachability analysis, Diagnosability, Discrete event systems.

Resumo— Este artigo apresenta uma primeira proposta da diagnosticabilidade de Sistemas Híbridos (SHs) usando a análise de alcançabilidade, uma técnica amplamente empregada na verificação de propriedades em SHs. Para tanto, apresenta-se uma nova definição de diagnosticabilidade que combina a diagnosticabilidade de sistemas a eventos discretos (SEDs) com a análise de alcançabilidade para comparação dos comportamentos contínuos. Além disso, apresenta-se um estudo de caso da análise da diagnosticabilidade de falhas de SHs inspirado num exemplo clássico de diagnóstico de SEDs para mostrar a vantagem de se realizar a análise da alcançabilidade dos estados associados à dinâmica a tempo contínuo do modelo híbrido com vistas a tornar diagnosticável uma falha.

Palavras-chave— Sistemas híbridos, Análise de alcançabilidade, Diagnosticabilidade, Sistemas a eventos discretos.

1 Introdução

A evolução tecnológica vem trazendo grandes avanços na indústria culminando com a indústria 4.0. Essa nova revolução industrial se baseia em sistemas ciberfísicos operando em tempo real, descentralizados e utilizando o conceito de internet das coisas. Para atender a essa nova indústria, os sistemas devem funcionar sem interrupção e caso o sistema apresente alguma falha, esse problema deve ser solucionado de forma eficiente sem trazer grandes prejuízos. Para tanto, é necessário que o sistema de diagnose de falhas consiga diagnosticar a falha a tempo de não trazer danos tanto à produção quanto às instalações.

A diagnose de falhas consiste em determinar se o sistema se encontra em seu comportamento normal ou se alguma falha ocorreu. Uma das abordagens para o problema da diagnose de falhas é a partir do conhecimento do modelo do sistema e, nesse contexto, destacam-se os trabalhos que usam os chamados modelos a eventos discretos (Sampath et al., 1995; Zaytoon e Lafortune, 2013). Contudo, a evolução dos sistemas a eventos discretos (SEDs) se dá pela ocorrência assíncrona de eventos e nenhuma informação sobre a evolução dinâmica do sistema é utilizada enquanto o sistema permanece em um determinado estado. Sistemas Híbridos (SHs), por outro lado, são sistemas que possuem ambas as dinâmicas, contínua e a eventos discretos, que interagem entre si durante sua evolução (Henzinger, 2000; Raskin, 2005). Muitos SEDs representam uma abstração de SHs, e dependendo do nível dessa abstração, muitas informações podem ser perdidas.

A diagnose de falha em SHs ainda é uma área incipiente com poucos trabalhos publicados. Uma abordagem encontrada na literatura é a detecção de falhas em tempo finito utilizando a invalidação de modelos para sistemas chaveados afins (Harirchi e Ozay, 2015; Harirchi et al., 2016). Nesse contexto, obtêm-se vários modelos a partir da observação entrada-saída do sistema. Esses trabalhos são limitados a sistemas contínuos chaveados sem dinâmica a eventos discretos. Outros trabalhos consideram a diagnose de falhas em SHs como uma extensão da diagnose de falha de sistemas a eventos discretos adicionando eventos através da discretização da análise das dinâmicas contínuas do sistema (Bayoudh e Travé-Massuyès, 2014; Diene et al., 2015). Mais recentemente, (Diene et al., 2017) apresenta uma nova definição de diagnosticabilidade para sistemas híbridos, assim como um método de verificação baseado no autômato verificador e na distinção dos modos baseados nos modelos de estados contínuos através da análise de resíduos.

Dentre as diversas técnicas empregadas para SHs, a *análise de alcançabilidade* destaca-se como uma das

mais relevantes e com direta aplicação na verificação de propriedades (*model checking*) de SHs (Alur et al., 1995; Maler, 2013; Le Guernic, 2009). Ferramentas computacionais bastante eficientes, como SpaceEx (Goran et al., 2011), estão disponíveis para a análise de alcançabilidade de subclasses de SHs.

Neste trabalho, apresenta-se uma primeira proposta de emprego da análise de alcançabilidade à diagnosticabilidade de falhas em SHs. Uma nova definição de diagnosticabilidade é apresentada, que combina a diagnosticabilidade de SEDs proposta por Sampath et al. (1995) com a análise de alcançabilidade para comparação dos comportamentos contínuos. A análise de alcançabilidade é empregada para distinguir os diferentes comportamentos contínuos subjacentes aos comportamentos discretos, permitindo assim, a diagnose da falha quando essa não era possível considerando apenas o modelo a eventos discretos.

Esse trabalho organiza-se da seguinte forma. Após serem apresentados conceitos e notações preliminares na seção 2, apresenta-se na seção 3 um texto introdutório sobre SHs e técnicas associadas, com ênfase na análise de alcançabilidade. Em seguida, na seção 4 apresenta-se nossa proposta para o diagnóstico de falhas de SHs baseada na análise de alcançabilidade e, na seção 5, apresenta-se um estudo de caso baseado num exemplo em (Cassandras e Lafortune, 2009). Por fim, na seção 6 apresentam-se comentários sobre a abordagem apresentada.

2 Preliminares

Nessa seção são apresentados conceitos preliminares e notações relativos à teoria de linguagens e autômatos empregados nas abordagens de Sistemas a Eventos Discretos e de Sistemas Híbridos (Cassandras e Lafortune, 2009).

Um alfabeto é um conjunto finito de símbolos Σ, normalmente associado a um conjunto de eventos físicos. Dado um alfabeto Σ, Σ^* denota o conjunto de todos os traços de comprimento finito formados por justaposição de símbolos em Σ, incluindo o traço vazio ε. A concatenação de dois traços $u, v \in \Sigma^*$ é escrita como uv. Um traço $s \in \Sigma^*$ é dito ser prefixo de $v \in \Sigma^*$, escrito $s \leq v$, se existir $u \in \Sigma^*$ tal que $su = v$. Para o traço $u \in \Sigma^*$, $\|u\|$ denota o seu comprimento em número de eventos. Para um traço $u \in \Sigma^*$ e um sub-alfabeto $\Sigma_f \subseteq \Sigma$ a notação $\Sigma_f \notin u$ representa que não há ocorrência dos elementos de Σ_f em u e a notação $\Psi(\Sigma_f) \subseteq \Sigma^*$ indica todos os traços terminadas por símbolos de Σ_f, ou seja $\Psi(\Sigma_f) = \{s\sigma_f \in L : \sigma_f \in \Sigma_f\}$.

Uma linguagem é qualquer subconjunto de Σ^*. O fecho prefixo de uma linguagem $L \subseteq \Sigma^*$ é $\overline{L} = \{u \in \Sigma^* : (\exists v \in L) u \leq v\}$. Uma linguagem L é dita ser prefixo fechada quando $L = \overline{L}$. Para uma linguagem $L \subseteq \Sigma^*$ e um traço $u \in L$, a pós-linguagem em L após u é definida por $L/u = \{v \in \Sigma^* : uv \in L\}$.

Definimos um *autômato não determinístico* por uma quádrupla $A = (\Sigma, Q, E, Q_0)$ em que Σ é o alfabeto, Q é um conjunto de estados, $E \subseteq Q \times \Sigma \times Q$ é uma relação de transição e $Q_0 \subseteq Q$ é um conjunto de estados iniciais. Para uma transição $e = (q, \sigma, p) \in E$, escrevemos $q \xrightarrow{\sigma}_A p$. O autômato A é dito ser determinístico quando $q \xrightarrow{\sigma}_A p_1$ e $q \xrightarrow{\sigma}_A p_2$ implicam $p_1 = p_2$ e $|Q_0| \leq 1$.

A relação de transição do autômato é estendida para traços em Σ^* como a seguir: $q \xrightarrow{\varepsilon}_A q$, para $q \in Q$; e $q \xrightarrow{u\sigma}_A p$ se $q \xrightarrow{u}_A r$ e $r \xrightarrow{\sigma}_A p$, para $q, p, r \in Q$, $\sigma \in \Sigma$ e $u \in \Sigma^*$. Escreve-se $q \xrightarrow{s}_A$ se existir $p \in Q$ tal que $q \xrightarrow{\sigma}_A p$. A notação se estende para conjuntos $Q_1, Q_2 \subseteq Q$ como a seguir: $Q_1 \xrightarrow{\sigma}_A Q_2$ se houver $p \in Q_1$ e $q \in Q_2$ tais que $p \xrightarrow{\sigma}_A q$. A *linguagem gerada* pelo autômato A é então definida por $L(A) = \{u \in \Sigma^* : Q_0 \xrightarrow{u}_A\}$. A linguagem gerada por um autômato é prefixo-fechada (Cassandras e Lafortune, 2009).

O conjunto de eventos Σ é particionado em subconjuntos de eventos observáveis (Σ_o) e não-observáveis (Σ_{uo}), isto é, $\Sigma = \Sigma_o \dot{\cup} \Sigma_{uo}$. Dados os alfabetos Σ e $\Sigma_o \subseteq \Sigma$, a projeção $P : \Sigma^* \to \Sigma_o^*$ é definida recursivamente por: $P(\varepsilon) = \varepsilon$; $P(\sigma) = \sigma$, se $\sigma \in \Sigma_o$, e $P(\sigma) = \varepsilon$, caso contrário; e $P(u\sigma) = P(u)P(\sigma)$, para $u \in \Sigma^*$ e $\sigma \in \Sigma$. A imagem inversa de uma projeção $P^{-1} : \Sigma_o^* \to 2^{\Sigma^*}$ é definida para $v \in \Sigma_o^*$ como $P^{-1}(v) = \{u \in \Sigma^* : P(u) = v\}$. Tanto a operação de projeção, quanto a sua imagem inversa podem ser estendidas à linguagens aplicando-se as mesmas a todos traços nelas contidas (Cassandras e Lafortune, 2009).

Por fim, para um autômato $A = (\Sigma, Q, E, Q_0)$ e o conjunto de eventos não observáveis $\Sigma_{uo} \subseteq \Sigma$, o alcance não observável de um estado $q \in Q$, denotado $UR(q)$, é definido como $UR(q) = \{p \in Q : (\exists u \in \Sigma_{uo}^*)\ q \xrightarrow{u}_A p\}$. O alcance não observável é definido para um conjunto de estados $P \in 2^Q$ como $UR(P) = \bigcup_{p \in P} UR(p)$.

3 Sistemas Híbridos

Nesta seção são apresentados resumidamente conceitos sobre *sistemas híbridos* (SHs) necessários para o desenvolvimento do trabalho.

Dentre os diversos formalismos para descrição de SHs, como os *sistemas chaveados* (Harirchi e Ozay, 2015), os *sistemas condição-evento* (Chutinan, 1999) ou os *sistemas de transição etiquetados* (Henzinger, 2000), o *autômato híbrido* (Henzinger, 2000; Raskin, 2005; Van Der Schaft e Schumacher, 2000) destaca-se como um dos mais relevantes, chegando a se confundir com a definição de um sistema híbrido em alguns trabalhos.

Definição 1 *Um autômato híbrido (AH) é definido por uma décupla:*

$$H \quad = \quad (\Sigma, Q, E, Q_0, X, f, I, G, R, X_0)$$

em que:

- Σ *é um conjunto de símbolos;*

- *Q é um conjunto de estados discretos;*
- *$E \subseteq Q \times \Sigma \times Q$ é uma relação de transição;*
- *$Q_0 \subseteq Q$ é o conjunto de estados discretos iniciais;*
- *$X \subseteq \mathbb{R}^n$ é um espaço de estados contínuo, com $n \in \mathbb{N}$;*
- *$f : Q \times X \to X$ é um campo vetorial;*
- *$I : Q \to 2^X$ é um invariante;*
- *$G : E \to 2^X$ é um guarda;*
- *$R : E \times X \to X$ é uma função de reinicialização; e*
- *$X_0 \subseteq X$ é o conjunto de estados contínuos iniciais.*

Um AH é construído sobre a estrutura de um autômato a que são adicionados predicados relativos à dinâmica contínua. O estado de um AH é definido pelo par $(q, x) \in Q \times X$, em que q é o estado discreto, também denominado modo ou local, e x é o estado contínuo. Os símbolos em Σ são associados a eventos e os disparos das transições correspondem à ocorrência dos eventos a elas associados. Para o local $q \in Q$, o campo vetorial define que a primeira derivada do estado contínuo se comporta como $\dot{x} = f(q, x)$, e o invariante determina uma condição de validade do estado contínuo na forma $x \in I(q)$. Para a transição $e \in E$, o guarda define uma condição para habilitação do disparo da transição a partir do estado contínuo na forma $x \in G(e)$, e a reinicialização define o valor do estado contínuo no disparo da transição conforme $x' := R(e, x)$. Para expressarmos que um evento pode ocorrer independentemente da condição no estado contínuo faremos $G(e) = X$.

Condições adicionais sobre os elementos do AH neste trabalho são:

- A relação de transição do AH é determinista.
- Os campos vetoriais são funções globalmente Lipschitz contínuas para garantir a unicidade da solução das equações diferenciais que definem as dinâmicas contínuas em cada local (Tripakis e Dang, 2009).
- O invariante, o guarda e a reinicialização são funções lineares sobre as componentes do estado.

A dinâmica contínua $\dot{x} = f(q, x)$ está na forma de um sistema autônomo no intuito de expressar o comportamento de um sistema em malha fechada com um controlador, podendo o controlador ser dependente do local q.

Uma *solução* para um AH é um par de sinais contínuos à direita $x : [0, \infty) \to X$ e $q : [0, \infty) \to Q$ tais que (Alur et al., 1995):

- $x(t)$ é diferenciável por partes e $q(t)$ é contínuo por partes;
- Em qualquer intervalo (t_1, t_2) no qual $q(t)$ seja constante e $x(t)$ seja contínuo define-se para todo $t \in [t_1, t_2)$ por:

$$x(t) \quad = \quad \phi(q(t_1), x(t_1), t)$$

  em que $\phi(q, x(t_0), t)$ é a solução para $\dot{x} = f(q, x)$ para $t \geq t_0$ e com condição inicial $x(t_0)$; e
- Nos demais instantes $t \geq 0$, $(q(t), x(t))$ é tal que existe $e = (q_1, \sigma, q_2)$ com $q(t^-) = q_1$, $q(t) = q_2$, $x(t^-) \in G(e)$ e $x(t) := R(e, x(t^-))$.

Define-se o *autômato tempo-abstraído* (Alur et al., 2000) do autômato híbrido H por:

$$T_H \quad = \quad (Q \times X, \Sigma_{T_H}, E_{T_H}, Q_0 \times X_0)$$

em que:

- $\Sigma_{T_H} = \Sigma \cup \{\tau\}$, com $\tau \notin \Sigma$; e
- $E_{T_H} \subseteq (Q \times X) \times \Sigma_{T_H} \times (Q \times X)$ definido por:
  - *Evolução discreta*: $(q_1, x_1) \xrightarrow{\sigma}_{T_H} (q_2, x_2)$ sse existe $e = (q_1, \sigma, q_2) \in E$ tal que $x_1 \in G(e)$ e $x_2 := R(e, x_1)$.
  - *Evolução contínua*: $(q_1, x_1) \xrightarrow{\tau}_{T_H} (q_2, x_2)$ sse $q_1 = q_2$ e existirem $\delta \geq 0$ e $x : [0, \delta] \to X$ tais que $x(0) = x_1$, $x(\delta) = x_2$, $\forall t \in [0, \delta]$ $x(t) \in I(q_1)$ e $\forall t \in (0, \delta)$ $\dot{x}(t) = f(q_1, x(t))$.

É possível então definirem-se duas linguagens em Σ^* a partir de um AH:

- A linguagem gerada pelo autômato que forma a estrutura do AH, $L(H) \subseteq \Sigma^*$; e
- A projeção em Σ^* da linguagem gerada pelo autômato tempo-abstraído T_H, $P_\Sigma(L(T_H)) \subseteq \Sigma^*$ em que $P_\Sigma : \Sigma^*_{T_H} \to \Sigma^*$.

Observe que $P_\Sigma(L(T_H)) \subseteq L(H)$ pois as soluções nem sempre vão esgotar todas as possibilidades de transição previstas em H.

O autômato tempo-abstraído T_H possui espaço de estados infinito e denso, tornando-se inviável seu emprego em operações computacionais, como a verificação de propriedades (Chutinan e Krogh, 2001). A prática é a obtenção de *sistemas de transição quociente* de estados finitos que sejam *bissimulações* de T_H, cuja existência e construção é demonstrada possível apenas para subclasses específicas de AH, como os autômatos temporizados e os autômatos retangulares inicializados (Alur et al., 2000). Por outro lado, existem trabalhos que buscam obter sistemas de transição quociente aproximados que ainda assim sirvam para a verificação de propriedades de um dado autômato híbrido (Chutinan e Krogh, 2001).

Seja o conjunto $Q_i \times X_i \subseteq Q \times X$, denota-se por $\mathcal{R}_H(Q_i, X_i)$ os *estados alcançáveis* ou *região alcançável* a partir de $Q_i \times X_i$ em H (Alur et al., 1995),

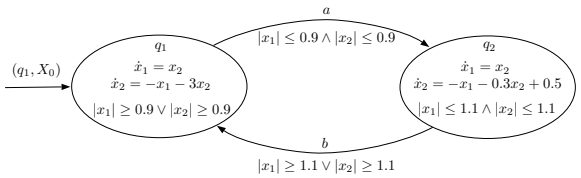


Figura 1: Autômato híbrido.

o conjunto formado pelos pares $(q_f, x_f) \in Q \times X$ para os quais exista uma solução $(q(t), x(t))$ para H em que:

- $(q(0), x(0)) \in Q_i \times X_i$; e
- Exista $t_f \geq 0$ para o qual $(q(t_f), x(t_f)) = (q_f, t_f)$.

O conjunto $Q_i \times X_i$ é dito ser um conjunto invariante quando $\mathcal{R}_H(Q_i, X_i) = Q_i \times X_i$.

A região alcançável $\mathcal{R}_H(Q_i, X_i)$ é calculada por um algoritmo interativo que obtém sucessivamente os conjuntos estados sucessores de um certo conjunto de estados por transições discretas e pela evolução contínua (Alur et al., 1995). Ferramentas computacionais calculam $\mathcal{R}_H(Q_i, X_i)$ empregando estados simbólicos (q, Y) em que $q \in Q$ e $Y \subseteq X$ é um conjunto contínuo representado por uma entidade geométrica, seja um poliedro, um elipsoide, um zonotopo, ou uma função suporte, entre outras (Le Guernic, 2009; Goran et al., 2011; Maler, 2013). Em geral, trabalha-se com uma aproximação conservativa $\tilde{\mathcal{R}}_H(Q_i, X_i)$ de uma região alcançável $\mathcal{R}_H(Q_i, X_i)$, no sentido de que os cálculos garantem que $\tilde{\mathcal{R}}_H(Q_i, X_i) \supseteq \mathcal{R}_H(Q_i, X_i)$ (Maler, 2013). A verificação de propriedades de sistemas híbridos emprega a *análise de alcançabilidade* para comparar uma dada região alcançável a partir de um conjunto de estados iniciais, $\mathcal{R}_H(Q_i, X_i)$, com um conjunto $F \subseteq Q \times X$ que caracteriza uma propriedade desejada (Maler, 2013).

Exemplo 1 *Considere o autômato híbrido da figura 1. São identificados os seguintes elementos: locais* $Q = \{q_1, q_2\}$*; eventos* $\Sigma = \{a, b\}$*; transições* $q_1 \xrightarrow{a}_H q_2$ *e* $q_2 \xrightarrow{b}_H q_1$*; estados contínuos na forma de um vetor* $x = [x_1\ x_2]^T$*. A dinâmica contínua é* $\dot{x}_1 = x_2$ *e* $\dot{x}_2 = -x_1 - 3x_2$ *em* q_1 *e* $\dot{x}_1 = x_2$ *e* $\dot{x}_2 = -x_1 - 0.3x_2 + 0.5$ *em* q_2*. Os invariantes são* $|x_1| >= 0.9 \vee |x_2| >= 0.9$ *em* q_1*, o exterior de um quadrado de lado* 1.8 *centrado na origem de* $x_1 \times x_2$*, e* $|x_1| <= 1.1 \wedge |x_2| <= 1.1$ *em* q_2*, o interior de um quadrado de lado* 2.2 *também centrado na origem de* $x_1 \times x_2$*. Para a transição etiquetada por* a *a condição de guarda é que o estado atinja o perímetro do quadrado de lado* 1.8*, enquanto que, para a transição etiquetada por* b*, a condição de guarda corresponde ao perímetro do quadrado de lado* 2.2*. Quando se omite a condição de reinicialização de uma transição significa que a mesma corresponde à identidade, que é o caso das transições deste exemplo.*

As figuras 2 e 3 mostram as soluções e as trajetórias de estados do AH para condições iniciais $(q_1, [2\ 0]^T)$*, linha contínua, e* $(q_1, [-2\ 0]^T)$*, linha traço-ponto. As simulações foram realizadas empregando o* toolbox Stateflow *da ferramenta* Matlab *(Mathworks, 2018). As figuras também mostram os limites dos quadrados de lado* 1.8*, pontilhado, e* 2.2*, tracejado, que limitam os guardas das transições etiquetadas por* a *e* b *respectivamente. Observe que, enquanto a linguagem gerada pela estrutura discreta do autômato híbrido* $L(H)$ *seja* $\overline{(ab)}^*$*, as linguagens de fato são* a *para a primeira condição inicial e* $ababa$ *para a segunda.*

Por fim, a figura 4 mostra a região alcançável para a condição inicial $(q_1, [[1.9, 2.1]\ 0]^T)$*. O gráfico foi obtido da ferramenta* SpaceEx *(Goran et al., 2011). Para o caso em questão, observa-se que a região alcançável é aproximada pelas ditas funções suporte (Le Guernic, 2009).*

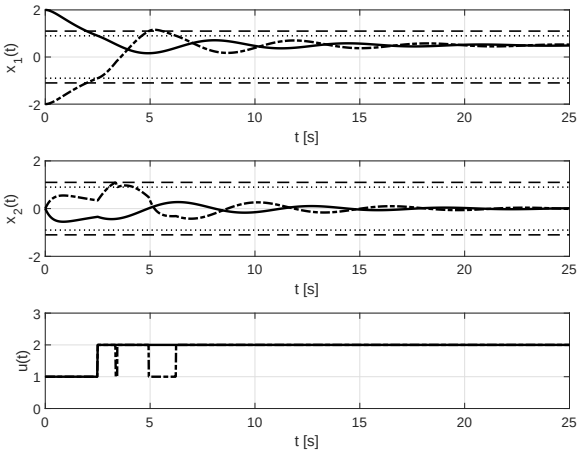


Figura 2: Exemplo de sinais temporais solução para o autômato híbrido.

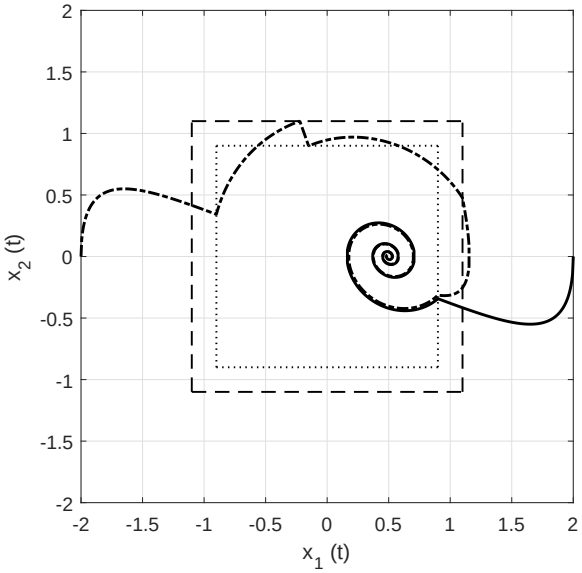


Figura 3: Exemplos de trajetórias de estados do autômato híbrido.

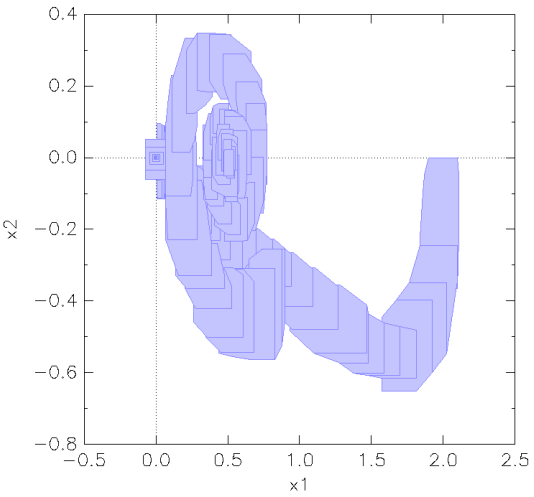


Figura 4: Exemplo de região alcançável para o autômato híbrido.

4 Diagnosticabilidade em Sistemas Híbridos

Seja Σ_f o conjunto de falhas do sistema, $\Sigma_f = \{\sigma_{f_1}, \sigma_{f_2}, \ldots, \sigma_{f_n}\}$. Considera-se que a falha seja um evento não observável, ou seja, $\Sigma_f \subseteq \Sigma_{uo}$. Caso a falha seja observável, a sua identificação será trivial.

A diagnosticabilidade de um sistema é a capacidade de se identificar a ocorrência de uma falha por intermédio da observação do comportamento do sistema após um tempo finito ou uma ocorrência finita de eventos. A diagnose de falhas de sistemas híbridos é um campo em aberto e podemos identificar que a abordagem comum é a combinação da diagnose puramente discreta de $L(H)$ com a distinção das dinâmicas contínuas para cada local (Bayoudh e Travé-Massuyès, 2014; Diene et al., 2017). Entretanto, esses trabalhos procuram obter informações discretas a partir da dinâmica contínua utilizando a abordagem de diagnose a SEDs.

Neste trabalho, faremos uma proposta preliminar de um novo conceito de diagnosticabilidade para os sistemas híbridos combinando a diagnose discreta com a distinção das dinâmicas contínuas para cada modo empregando análise de alcançabilidade que é uma ferramenta adequada aos SHs. Sem perda de generalidade, consideramos o sistema com apenas uma falha σ_f.

Seja $\chi_0 \subseteq X$ um conjunto de condições iniciais. Além disso, será considerada a alcançabilidade dentro de um mesmo local, considerando que o mesmo não possua transições possíveis. Supõe-se que todos os traços que não contém a falha são chamados de traços normais s_N e, equivalentemente, todos os traços que contém a falha são chamados de traços de falha, s_F. Todos os locais para os quais $q_0 \xrightarrow{s_N}_H q_N$ são chamados de locais normais e os locais $q_0 \xrightarrow{s_F}_H q_F$ são chamados de locais de falha.

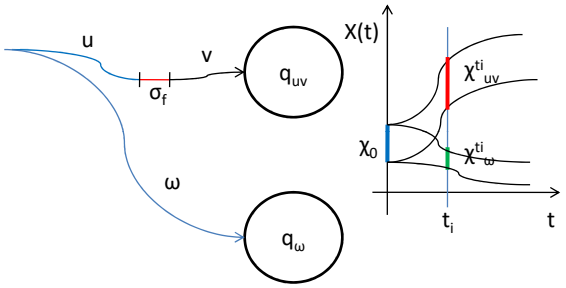


Figura 5: Ilustração da definição de diagnosticabilidade de sistemas híbrido.

Definição 2 *[Diagnosticabilidade] Seja L a linguagem gerada pelo autômato híbrido H. O sistema híbrido modelado por H é diagnosticável com relação projeção P, conjunto de falhas Σ_f, condição inicial $\chi_0 \subseteq X$ se as condições $D_D \vee D_C$ forem satisfeitas, em que*

$$
\begin{aligned}
D_D :&(\exists n \in \mathbb{N})(\forall u \in \Psi(\Sigma_f))(\forall v \in L/u)(\|v\| \geq n) \\
&\Rightarrow (\nexists \omega \in L)[(P(uv) = P(\omega)) \wedge (\Sigma_f \notin \omega)] \\
D_C :&(\exists t_i \in \mathbb{R}^+)(\forall u \in \Psi(\Sigma_f)) \\
&(\exists v \in L/u \wedge v \in \Psi(\Sigma_o)) \\
&(P(uv) = P(\omega) \wedge \Sigma_f \notin \omega) \Rightarrow \\
&\mathcal{R}_H(\mathcal{Q}_\omega, \chi_\omega^{t_i}) \cap \mathcal{R}_H(\mathcal{Q}_{uv}, \chi_{uv}^{t_i}) = \emptyset
\end{aligned}
$$

sendo que $\mathcal{Q}_s = UR(q_0 \xrightarrow{s}_H)$ e $\chi_s^{t_i} = \phi(\mathcal{Q}_s, \chi_0, t_i)$.

A definição 2 sugere que o sistema pode ser diagnosticado puramente de forma discreta ou com base no comportamento contínuo do sistema híbrido adotando-se a abordagem por alcançabilidade. A condição D_D proposta em (Sampath et al., 1995) expressa que deve existir um traço de comprimento arbitrariamente longo após a ocorrência da falha que não se confunde com nenhum traço normal do sistema.

A figura 5 ilustra a condição D_C. Essa condição exprime que, quando as projeções do traço de falha uv e de um traço normal ω se confundam ($P(uv) = P(\omega)$), deve existir pelo menos um local de falha que tenha seu comportamento contínuo diferente de um local normal. Na figura 5, o local de falha q_{uv} e local normal q_ω tem evolução contínua diferente com a mesma condição inicial χ_0 a partir no instante t_i. Essa diferença é traduzida no conjuntos alcançáveis $\mathcal{R}_H(q_\omega, \chi_\omega^{t_i})$ e $\mathcal{R}_H(q_{uv}, \chi_{uv}^{t_i})$ com condições iniciais $\chi_\omega^{t_i}$ e $\chi_{uv}^{t_i}$ que possuem uma interseção vazia. Note que alcance não observável $\mathcal{Q}_s = UR(q_0 \xrightarrow{s}_H)$ na condição D_C representa o conjunto de todos os locais $\mathcal{Q}$, após a ocorrência de s, que são alcançáveis por eventos não observáveis e $\chi_s^{t_i} = \phi(\mathcal{Q}_s, \chi_0, t_i)$ é conjunto de estados contínuo para a solução $\dot{x} = f(q, x)$ no intervalo (t_0, t_i) com condição inicial χ_0 para todo $q \in \mathcal{Q}_s$. Vale ressaltar que, implícita na condição D_C, está a necessidade do sistema permanecer nos locais onde essa condição está sendo verificada até que

a condição $\mathcal{R}_H(\mathcal{Q}_\omega, \chi_\omega^{t_i}) \cap \mathcal{R}_H(\mathcal{Q}_{uv}, \chi_{uv}^{t_i}) = \emptyset$ seja satisfeita. Caso um novo evento observável ocorra, as condições D_D e D_C devem ser novamente verificadas.

5 Exemplo

Nessa seção trataremos de um sistema híbrido composto por uma válvula, uma bomba e um controlador (Cassandras e Lafortune, 2009). A vazão da válvula está sujeita a existência de pressão fornecida pela bomba. Por simplicidade, representamos o comportamento concorrente do autômato híbrido $H = (\Sigma, Q, E, Q_0, X, f, I, G, R, X_0)$ sujeito a ação do controlador conforme destacado em azul na figura 6. Esse AH representa o comportamento normal do sistema, no qual podemos observar o conjunto de eventos $\Sigma_o = \{ov, cv, SaP, SoP\}$, em que ov consiste no comando de abrir a válvula, cv é o comando de fechar a válvula e SaP e SoP são os comandos de ligar e desligar a bomba, respectivamente; os locais $Q = \{1, 2, 3, 4\}$; o estado contínuo é f, a vazão; o estado inicial $(Q_0, X_0) = (1, 0)$. A dinâmica contínua nos locais $1, 2$ e 4 é $\dot{f} = -9f$ e no local 3 é $\dot{f} = -9f + 25$. O invariante é $0 \leq f \leq 25/9$ para todos os locais. O local 1 consiste na bomba desligada e a válvula fechada, ao ocorrer o evento ov ele transiciona para o local 2, que consiste na válvula aberta e bomba desligada. Na ocorrência de SaP, o autômato vai para o local 3, em que a válvula está aberta e a bomba ligada. Analogamente ao ocorrer SoP, a bomba é desligada e o autômato encontra-se no local 4. O ciclo se fecha após o comando cv de fechamento da válvula, retornando ao local 1.

Considere que esse sistema esteja sujeito às seguintes falhas associadas a eventos: válvula emperra totalmente fechada sc, válvula emperra totalmente aberta so_{100} e válvula emperra em 50% de sua abertura total so_{50}, *i.e.*, conjunto de eventos de falha $\Sigma_f = \{sc, so_{100}, so_{50}\}$. Por hipótese, as falhas são eventos não observáveis $\Sigma_f \subseteq \Sigma_{uo}$ podendo ocorrer a qualquer momento. Portanto o conjunto de eventos é $\Sigma = \Sigma_o \cup \Sigma_f$. A figura 6 representa o comportamento completo do sistema sujeito ao conjunto de falhas Σ_f, em que os locais e transições em azul representam o comportamento normal do sistema. Analisando o traço de falha em que ocorre o evento de falha sc para um possível traço do ciclo de falha $uv = \{scovSaPSoPcv\}^*$ e o traço do ciclo normal $\omega = \{ovSaPSoPcv\}^*$, observa-se que a projeção da linguagem $P : \Sigma^* \to \Sigma_o^*$ dos traços de falha e normal são iguais $P(uv) = \{ovSaPSoPcv\}^* = P(\omega)$. Por inspeção, verifica-se que todos os ciclos de falha têm a mesma projeção do ciclo normal. Portanto, pela definição 2, o sistema híbrido modelado por H não atende a condição D_D. Para solucionar esse problema (Cassandras e Lafortune, 2009) propõem o uso do mapa de sensores. Neste artigo, iremos analisar a condição de diagnosticabilidade D_C que emprega a análise de alcançabilidade.

A figura 7 representa os gráficos de alcançabilidade referentes a cada local do AH, considerando-se que a alcançabilidade é realizada sujeita às mesmas condições iniciais $\chi_0 : 0 \leq f \leq 25/9$ em cada local e o mesmo não possui transições. O tempo é limitado em 2 segundos visto que todas as trajetórias convergem para um valor constante dentro desse período de tempo. Resumidamente a figura 7-(a) representa as regiões alcançáveis para os locais $1, 2, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14$ e 16. A figura 7-(b) representa as regiões alcançáveis para os locais 3 e 11 e a figura 7-(c) o local 15.

Nota-se que desde o primeiro momento o evento de falha pode ter ocorrido, sendo assim, pela definição 2 um traço de falha terminado em sequência de falha $u = sc$ e sua possível continuação $v_1 = ov$ possuem a mesma projeção que um traço normal ω_1, $P(uv_1) = ov = P(\omega_1)$. Devemos, então, encontrar ao menos uma região alcançável dos locais de falha que não possua interseção com a região alcançável dos locais normais a partir de um tempo $t \geq t_i$. Os locais referentes à esses traços são $1 \overset{uv_1}{\to}_H 6$ e $1 \overset{\omega_1}{\to}_H 2$. A análise é baseada na figura 7-(a) levando em consideração as regiões alcançáveis desses locais, comportamentos de falha sc e normal, respectivamente. Observa-se que $\nexists t_i \in \mathbb{R}^+$ que garanta a não interseção das regiões alcançáveis.

Prosseguimos, assim, com a continuação $v_2 = ovSaP$, cuja projeção $P(uv_2) = ovSaP$ é a mesma que a projeção do traço normal $\omega_2 = ovSaP$, $P(\omega_2) = ovSaP$. Os locais referentes a esses traços são $1 \overset{uv_2}{\to}_H 7$ e $1 \overset{\omega_2}{\to}_H 3$. Por meio dos gráficos nas figuras 7-(a) e (b) verificamos que $\exists t_i \in \mathbb{R}^+$ em que as regiões alcançáveis não possuem interseção. Por inspeção, por exemplo, $t_i = 0.2$ já satisfaz a condição D_C. Obtemos o mesmo resultado do mapa de sensores.

Para o caso da falha so_{100}, o mapa de sensores não é capaz de diferenciar os comportamentos normal e de falha. Pela definição 2 também não é possível diagnosticar essa falha, pois as regiões alcançáveis do comportamento normal e de falha sempre serão as mesmas recaindo nas figuras 7-(a) e (b).

Diferente do caso abordado em (Cassandras e Lafortune, 2009), foi introduzida uma nova falha, so_{50} que pelo mapa de sensores também não seria distinguível do comportamento normal do sistema. Analisando pela definição 2, seja um traço de falha terminado em sequência de falha $u = so_{50}$ e sua possível continuação $v_1 = ov$, as projeções $P(uv_1) = ov = P(\omega_1)$, em que $\omega_1 = ov$. Os locais referentes a esses traços são $1 \overset{uv_1}{\to}_H 14$ e $1 \overset{\omega_1}{\to}_H 2$. Observa-se que $\nexists t_i \in \mathbb{R}^+$ que garanta a não interseção das regiões alcançáveis. Para outra continuação $v_2 = ovSaP$, cuja projeção $P(u_v 2) = ovSaP$ é a mesma que a projeção do traço normal $\omega_2 = ovSaP$, $P(\omega_2) = ovSaP$ seus referentes locais são $1 \overset{uv_2}{\to}_H 15$ e $1 \overset{\omega_2}{\to}_H 3$ representados pelas figuras 3-(c) e (b), respectivamente. Por inspeção, $t_i = 0.2$ já satisfaz a condição D_C. Assim, pelo emprego da análise de alcançabilidade podemos diagnosticar a falha so_{50}.

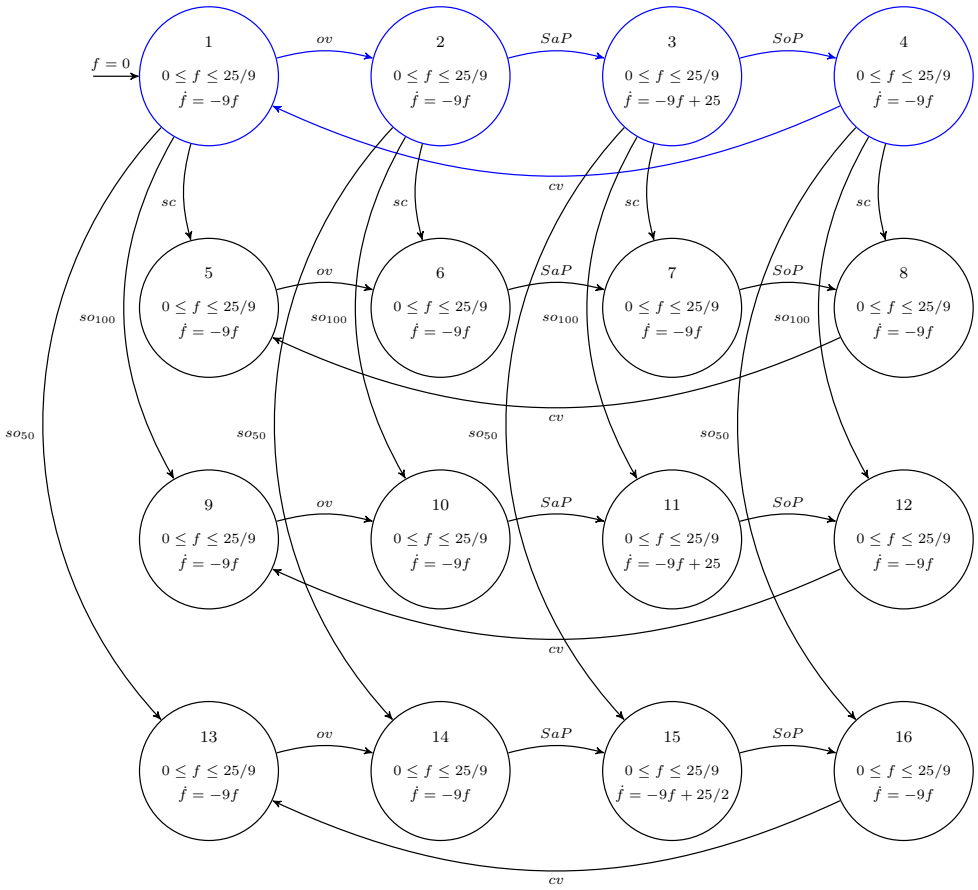
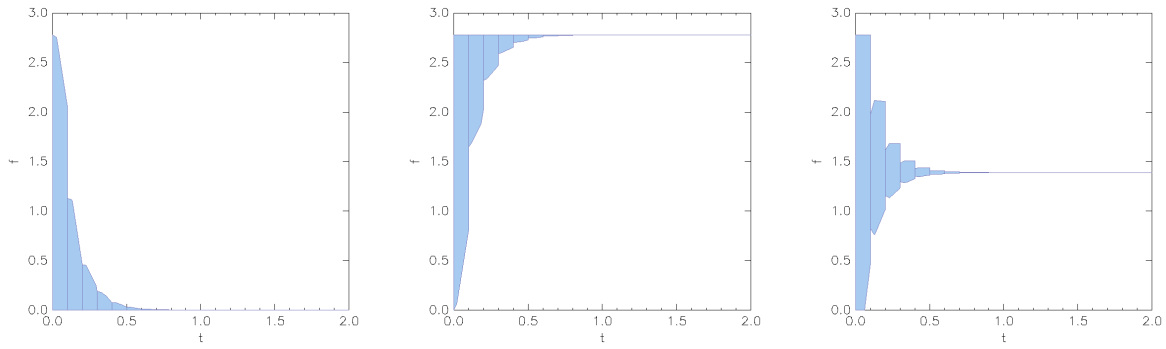


Figura 6: Autômato híbrido representando seu comportamento de falha.



(a) (b) (c)

Figura 7: Gráfico de alcançabilidade referente aos locais do AH sujeitos às mesmas condições iniciais $\chi_0 = 0 \leq f \leq 25/9$. A subfigura (a) se refere ao comportamento dos locais $1, 2, 4-10, 12-14$ e 16. A subfigura (b) se refere ao comportamento dos locais 3 e 11 e a subfigura (c) ao comportamento do local 15.

6 Conclusões

Neste trabalho é proposta uma nova definição de diagnosticabilidade de SHs empregando-se a análise da alcançabilidade combinada à diagnosticabilidade de SEDs. Para isso, o sistema é representado na forma de um autômato híbrido, sendo a análise da diagnosticabilidade feita utilizando o modelo a evento discreto juntamente com a análise de alcançabilidade dos estados do modelo a tempo contínuo. Como perspectiva de trabalho futuro, prevê-se o aprofundamento do emprego da análise de alcançabilidade do sistema híbrido como um todo para verificação da diagnosticabilidade.

Agradecimentos

Este trabalho foi parcialmente financiado pela CAPES.

Referências

Alur, R., Courcoubetis, C., Halbwachs, N., Henzinger, T. A., Ho, P.-H., Nicollin, X., Olivero, A., Sifakis, J. e Yovine, S. (1995). The algorithmic analysis of hybrid systems, *Theoretical computer science* **138**(1): 3–34.

Alur, R., Henzinger, T. A., Lafferriere, G. e Pappas, G. J. (2000). Discrete abstractions of hybrid systems, *Proceedings of the IEEE* **88**(7): 971–984.

Bayoudh, M. e Travé-Massuyès, L. (2014). Diagnosability analysis of hybrid systems cast in a discrete-event framework, *Discrete Event Dynamic Systems* **24**(3): 309–338.

Cassandras, C. G. e Lafortune, S. (2009). *Introduction to discrete event systems*, Springer Science & Business Media.

Chutinan, A. (1999). Hybrid system verification using discrete model approximations, *Ph. D. dissertation, Department of Electrical and Computer Engineering, Carnegie Mellon University* .

Chutinan, A. e Krogh, B. H. (2001). Verification of infinite-state dynamic systems using approximate quotient transition systems, *IEEE Transactions on automatic control* **46**(9): 1401–1410.

Diene, O., Moreira, M. V., Alvarez, V. R. e Silva, E. R. (2015). Computational methods for diagnosability verification of hybrid systems, *Control Applications (CCA), 2015 IEEE Conference on*, IEEE, pp. 382–387.

Diene, O., Moreira, M. V., Silva, E. A., Alvarez, V. R. e Nascimento, C. F. (2017). Diagnosability of hybrid systems, *IEEE Transactions on Control Systems Technology* .

Goran, F., Le Guernic, C., Donzé, A., Cotton, S., Ray, R., Lebeltel, O., Ripado, R., Girard, A., Dang, T. e Maler, O. (2011). Spaceex: Scalable verification of hybrid systems, *Computer Aided Verification. CAV*, Vol. 6806 of *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, pp. 379–395.

Harirchi, F., Luo, Z. e Ozay, N. (2016). Model (in) validation and fault detection for systems with polynomial state-space models, *American Control Conference (ACC), 2016*, IEEE, pp. 1017–1023.

Harirchi, F. e Ozay, N. (2015). Model invalidation for switched affine systems with applications to fault and anomaly detection, *IFAC-PapersOnLine* **48**(27): 260–266.

Henzinger, T. A. (2000). The theory of hybrid automata, *Verification of Digital and Hybrid Systems*, number 170 in *NATO ASI Series (Series F: Computer and Systems Sciences)*, Springer-Berlin-Heidelberg, pp. 265–292.

Le Guernic, C. (2009). *Reachability analysis of hybrid systems with linear continuous dynamics*, Computer science, Université Joseph-Fourier - Grenoble I.

Maler, O. (2013). Algorithmic verification of continuous and hybrid systems, *Int. Workshop on Verification of Infnite-State System (Infnity)*.

Mathworks (2018). Stateflow: Model and simulate decision logic using state machines and flow charts, https://www.mathworks.com/products/stateflow.html.

Raskin, J.-F. (2005). An introduction to hybrid automata, *Handbook of Networked and Embedded Control Systems*, Springer, pp. 491–517.

Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K. e Teneketzis, D. (1995). Diagnosability of discrete-event systems, *IEEE Transactions on automatic control* **40**(9): 1555–1575.

Tripakis, S. e Dang, T. (2009). Modeling, verification and testing using timed and hybrid automata, *Model-Based Design for Embedded Systems* pp. 383–436.

Van Der Schaft, A. J. e Schumacher, J. M. (2000). *An introduction to hybrid dynamical systems*, Vol. 251, Springer London.

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