Diagnostic de motifs de comportements dans les systèmes temporels

Yannick Pencolé[1], **Audine Subias**[1,2]
[1]LAAS-CNRS, Toulouse, France
[2]INSA de Toulouse, France

MSR-17 15-17th November 2017

De quoi s'agit-il ?

- Diagnostic de faute dans SED :
  - On se donne le modèle du système (automate, réseau de Petri,...)
  - Ce modèle contient des événements fautifs $f_1, \ldots, f_n$ non observables
  - Le système est partiellement observable
- Une littérature très riche sur le sujet (diagnostic, analyse de diagnosticabilité)
- Une extension du problème aux motifs de supervision [T.Jéron 2006] (approche basée automate)
  - Généralisation + Séparation du modèle des comportements du système et des objectifs de diagnostic (définis par le motif)

=> Problèmes de diagnostic et de diagnosticabilité des motifs modélisés par réseaux de Petri

Le système

Definition: Modèle du système temporel

Le système temporel de langage $\mathscr{L}$ est un RdPTEPrA $\Theta = \langle P, T, A, \succ, \ell, \Sigma, I_s, Q, M_0 \rangle$ tel que $\mathscr{L} = \mathscr{L}(\Theta)$.

1. le réseau est sauf
2. la borne inférieure de chaque intervalle temporel statique est strictement positive
3. l'ensemble des marquages accepteurs est l'ensemble des marquages accessibles.

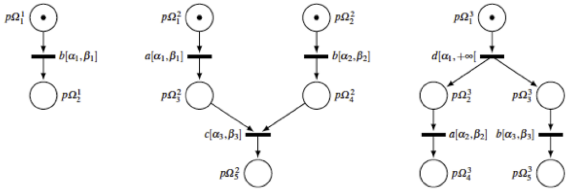
Le motif

Definition: Motif temporel

Un motif sur un ensemble d'événements $\Sigma_{\mathscr{R}}$ est un langage temporel $\mathscr{R} \subseteq \mathscr{T}(\Sigma_{\mathscr{R}}) = (\mathbb{R}^+ \times (\Sigma \cup \lambda))^+$ tel que si $\rho \in \mathscr{R}$ alors seules des continuations de ρ de la forme $\rho\delta\lambda, \delta \in \mathbb{R}^+$ sont dans $\mathscr{R}$.

- Motif : *l'événement a arrive après b*
- $\mathscr{R}$ défini par $\{\delta_0 b \delta_1 a \delta_2 \lambda, \delta_0, \delta_1, \delta_2 \in \mathbb{R}^+, \delta_1 > 0\}$,
- Représentation en intension

Exemple de motifs



$Q_{\Omega_1} = \{\{p_{\Omega^1_2}\}\}$
$Q_{\Omega_2} = \{\{p_{\Omega^2_5}\}\}$
$Q_{\Omega_3} = \{\{p_{\Omega^3_4}, p_{\Omega^3_5}\}\}$

- $M_0 \notin Q_\Omega$, le motif ne contient pas la séquence 0λ ;
- tout événement du motif n'est pas observable dans le système ;
- tout marquage accepteur est bloquant (définition d'un motif temporel)

Diagnostic de motifs : formulation du problème

Mettre en place une fonction de diagnostic qui prend en entrée une séquence d'observations et qui en retour renvoie dans un délai borné un des trois résultats suivants :

1. *Le comportement décrit par le motif s'est produit pendant l'évolution du système.*
2. *Le comportement décrit par le motif ne s'est pas produit pendant l'évolution du système .*
3. *Il est possible que le comportement décrit par le motif se soit produit pendant l'évolution du système.*

LAAS CNRS

Concordance (*Matching*) d'un motif

Definition: Matching

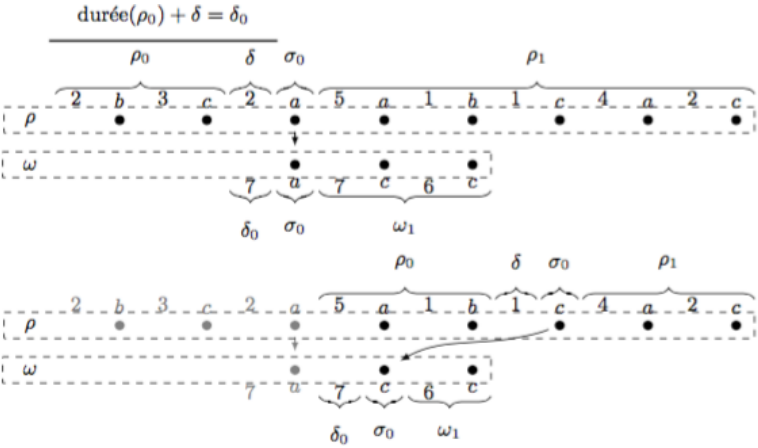
Une séquence $\rho \in \mathscr{T}(\Sigma)$ est en concordance avec une autre séquence $\omega \in \mathscr{T}(\Sigma)$, noté $\rho \supseteq \omega$, si :

- $\omega = \delta\lambda$, avec : $\delta \in \mathbb{R}^+$, et duree$(\rho) \geq \delta$; ou
- $\omega = \delta_0\sigma_0\omega_1$, telle que : $\delta_0 \in \mathbb{R}^+$, $\sigma_0 \in \Sigma$, $\omega_1 \in \mathscr{T}(\Sigma)$ et il existe deux séquences $\rho_0 \in \mathscr{T}(\Sigma), \rho_1 \in \mathscr{T}(\Sigma)$ et une durée $\delta \in \mathbb{R}^+$ telles que :
  1. $\rho = \rho_0\delta\sigma_0\rho_1$;
  2. $\delta_0 = \text{duree}(\rho_0) + \delta$;
  3. $\rho_1 \supseteq \omega_1$.

Definition: $\mathscr{R}$-concordance (Matching d'un motif)

Soit $\mathscr{R}$ un motif de comportement. Une séquence $\rho \in \mathscr{T}(\Sigma)$ est $\mathscr{R}$-concordante s'il existe une séquence $\omega \in \mathscr{R}$ telle que $\rho \supseteq \omega$, c.-à -d. ρ matche ω.

Matching



durée(ρ_0) + δ = δ_0
ρ_0
δ
σ_0
ρ_1
2 b 3 c 2 a 5 a 1 b 1 c 4 a 2 c
ρ
ω
7 a 7 c 6 c
δ_0
σ_0
ω_1
ρ_0
δ
σ_0
ρ_1
2 b 3 c 2 a 5 a 1 b 1 c 4 a 2 c
ρ
ω
7 a 7 c 6 c
δ_0
σ_0
ω_1

Diagnostic de motif

Pour un motif $\mathscr{R}$ donné il s'agit de définir une fonction $\mathscr{R}$-diagnostiqueur

Definition: $\mathscr{R}$-diagnostiqueur

Soit $\mathscr{L}$ le langage temporel du système sur l'ensemble d'événements $\Sigma = \Sigma_u \cup \Sigma_o$, un $\mathscr{R}$-diagnostiqueur est une fonction

$$\Delta_{\mathscr{R}} : \mathscr{T}(\Sigma_o) \to \{\mathscr{R}-\mathit{certain}, \mathscr{R}-\mathit{sain}, \mathscr{R}-\mathit{ambigu}\}$$

telle que :

- $\Delta_{\mathscr{R}}(\sigma) = \mathscr{R}-\mathit{certain}$ si pour toute séquence $\rho \in \mathscr{L}$ qui est cohérente avec σ (i.e.$P^t_{\Sigma_o}(\rho) = \sigma$), ρ est $\mathscr{R}$-concordante ;
- $\Delta_{\mathscr{R}}(\sigma) = \mathscr{R}-\mathit{sain}$ si pour toute séquence $\rho \in \mathscr{L}$ qui est cohérente avec σ, ρ n'est pas $\mathscr{R}$-concordante ;
- $\Delta_{\mathscr{R}}(\sigma) = \mathscr{R}-\mathit{ambigu}$ dans tout autre cas.

Diagnostic d'un ensemble de motifs

Considérons maintenant un ensemble de motifs, $\mathscr{R}_1, \ldots, \mathscr{R}_n$,

Definition: Diagnoser

$\Delta : \mathscr{T}(\Sigma_o) \rightarrow \prod_{i=1}^{n} \{\mathscr{R}_i - certain, \mathscr{R}_i - sain, \mathscr{R}_i - ambigu\}$ tel que $\Delta(\sigma) = (\Delta_{\mathscr{R}_1}(\sigma), \ldots, \Delta_{\mathscr{R}_n}(\sigma))$.

Représentation du matching (système-motif)(1)

- Combinaison : $\Theta_\Omega = \Theta \ltimes \Omega$.
- Le motif ne peut évoluer sans le système, le système peut évoluer seul
- $Q = \{q_\Omega \cup q_\Theta : (q_\Omega, q_\Theta) \in Q_\Omega \times Q_\Theta\}$

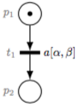
Soit Θ le RdPEPrA d'un système et Ω celui du pattern :

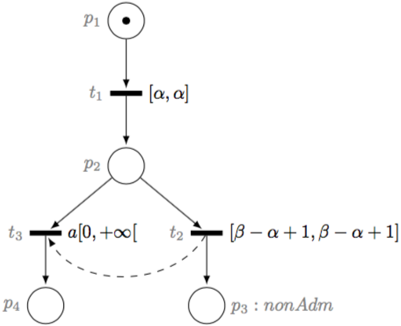
$$\mathscr{L}(\Theta \ltimes \Omega) = \{\rho \in \mathscr{L}(\Theta) : \rho \Supset \Omega\}.$$

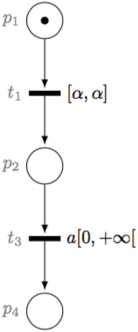
Toute execution du système Θ conduit à un marquage dans Θ_Ω. Toute exécution de Θ qui est concordante (matche) avec le motif Ω conduit à un marquage accepteur pour Ω

Représentation du matching (système-motif)(2)

Au préalable : décomposition temporelle de chaque transition du réseau initial à synchroniser (utilisation des priorités)







LAAS CNRS

Représentation du matching (système-motif)(3)

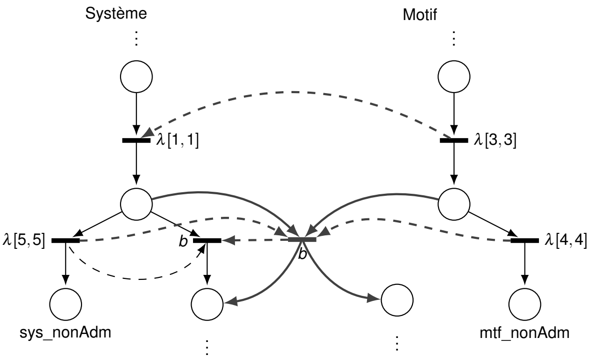


FIGURE: combinaison asymétrique d'une transition $b[1,4]$ d'un système avec une transition $b[3,6]$ d'un motif.

Combinaison du systèmes-motif et des observations

1. Observations : sequence temporelle σ.
2. modélisation de la séquence par un réseau de Petri *Obs* avec une place finale p_{obs}.
3. Décomposition temporelle des transitions de *Obs* ainsi que des transitions de $\Theta \ltimes \Omega$ dont les étiquettes sont présentes dans *Obs*.
4. Synchonisation : $\Theta_\Omega || Obs$

Toute exécution de Θ qui génère σ est une exécution de $\Theta_\Omega || Obs$ qui mène à marquage M tel que $M(p_{obs}) = 1$.

Diagnostic par model checking

- Soit M un marquage de $\Theta_\Omega \parallel Obs$
- $M_{|\Omega}$ la restriction de M à Ω
- $M_{|O}$ la restriction de M à O

Deux questions posées :

1. est-il toujours vrai ($\Box$) que si le système produit Obs ($sys\_nonAdm = 0 \wedge p_{Obs} = 1$) alors ($\Rightarrow$) il est concordant avec le motif ($M_{|\Omega} \in Q_\Omega$) :

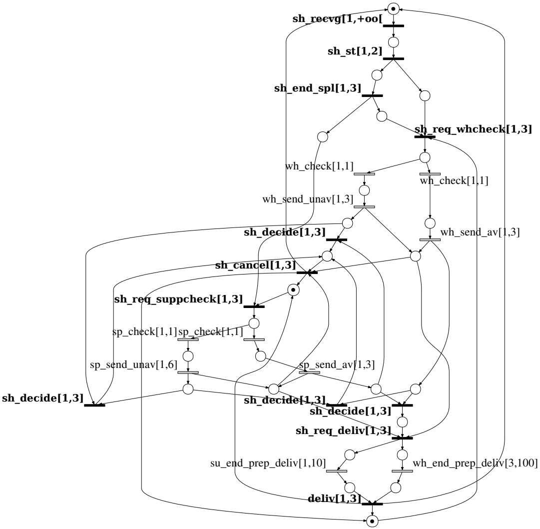
$$\varphi_{CERTAIN} \equiv \Box((sys\_nonAdm = 0 \wedge p_{Obs} = 1) \Rightarrow M_{|\Omega} \in Q_\Omega)$$

2. est-il est toujours vrai ($\Box$) que si le système produit Obs ($sys\_nonAdm = 0 \wedge p_{Obs} = 1$) alors ($\Rightarrow$) il n'est pas concordant avec le motif ($M_{|\Omega} \notin Q_\Omega$) :

$$\varphi_{SAIN} \equiv \Box((sys\_nonAdm = 0 \wedge p_{Obs} = 1) \Rightarrow M_{|\Omega} \notin Q_\Omega)$$

Application au diagnostic d’un food shop

- Magasin en ligne de produits alimentaires : focus sur les activités pour la gestion d’un client
- Modèle = comportement vu par la boutique
- Evénements observables (en gras) sont ceux de la boutique



Application au diagnostic d'un food shop

Motif1 : simple occurrence d'un événement

- le fournisseur répond à la boutique que les produits ne sont pas disponibles
- motif $\mathscr{R}_1$: occurrence de *sp_send_unav*
- séquence d'observations $\sigma_1 = \mathbf{50}\mathit{sh\_recvg}\ \mathbf{1}\mathit{sh\_st}\ \mathbf{1}\mathit{sh\_end\_spl}\ \mathbf{1}\mathit{sh\_req\_whcheck}\ \mathbf{1}\mathit{sh\_req\_suppcheck}\ \mathbf{3}\mathit{sh\_decide}\ \mathbf{2}\mathit{sh\_req\_deliv}\ \mathbf{10}\mathit{deliv}$:

- $[]((sys_n onAdm = 0 / \ p9 = 1) => (pp1 = 1))$: False
- $[]((sys_n onAdm = 0 / \ p9 = 1) => -(pp1 = 1))$: True $(\Delta_{\mathscr{R}_1}(\sigma_1) = \mathscr{R}_1 - sain\ )$
- *sh_req_deliv* : tous les produits sont effectivement disponibles(car vont être livrés)

Application au diagnostic d'un food shop

Motif1 : simple occurrence d'un événement

- motif $\mathscr{R}_1$: occurrence de *sp_send_unav*
- $\sigma_2 = \mathbf{50}\mathit{sh\_recvg}\ \mathbf{1}\mathit{sh\_st}\ \mathbf{1}\mathit{sh\_end\_spl}\ \mathbf{1}\mathit{sh\_req\_whcheck}\ \mathbf{1}\mathit{sh\_req\_suppcheck}\ \mathbf{7}\mathit{sh\_decide}\ \mathbf{2}\mathit{sh\_cancel}$.
- Réponses négatives aux deux questions : $\Delta_{\mathscr{R}_1}(\sigma_2) = \mathscr{R}_1 - \mathit{ambigu}$
- Pas possible de savoir si la décision de non-livraison vient du fournisseur (occurrence du motif) ou seulement de l'entrepôt (non-occurrence du motif).
- $\sigma_3 = \mathbf{50}\mathit{sh\_recvg}\ \mathbf{1}\mathit{sh\_st}\ \mathbf{1}\mathit{sh\_end\_spl}\ \mathbf{1}\mathit{sh\_req\_whcheck}\ \mathbf{1}\mathit{sh\_req\_suppcheck}\ \mathbf{8}\mathit{sh\_decide}\ \mathbf{2}\mathit{sh\_cancel}$.
- le temps de traitement par le fournisseur en cas de non disponibilité est parfois plus long ($\mathit{sp\_send\_unav}[1,6]$ et ($\mathit{sp\_send\_av}[1,3]$)) ; $\Delta_{\mathscr{R}_1}(\sigma_3) = \mathscr{R}_1 - \mathit{certain}$

LAAS CNRS

Application au diagnostic d'un food shop

Motif2 : séquence d'évenements

- retours clients : dans le cas où l'entrepôt envoie une disponibilité des produits et réalise la préparation des produits, cette préparation se ferait avec un délai trop grand (de 70 à 200 utps)
- motif $\mathscr{R}_2$: $wh\_send\_av[0,+\infty[\rightarrow wh\_end\_prep[70,200]$:
- séquence d'observations $\sigma_4 =$ **50**sh_recvg **1**sh_st **1**sh_end_spl **1**$sh\_req\_whcheck$ **1**$sh\_req\_suppcheck$ **3**sh_decide **2**sh_req_deliv **50**$deliv$.
- $\Delta_{\mathscr{R}_2}(\sigma_4) = \mathscr{R}_2 - sain$
- la date de livraison étant à 50 après la requête, le motif ne peut effectivement pas avoir lieu.
- modification de σ_4 (50 -> 80) : $\Delta_{\mathscr{R}_2}(\sigma_4) = \mathscr{R}_2 - certain$

Conclusion/Perspectives

- Une proposition pour le diagnostic de motifs temporels
- Un cadre de modélisation des motifs
- Une formulation du problème de diagnostic en un problème de model-checking

- Extension de l'expressivité des patterns
- Diagnosticabilité