Analyse de diagnosticabilité de motifs dans les systèmes à événements discrets.

Yannick Pencolé

Équipe DISCO, CNRS-LAAS, Univ. Toulouse, FRANCE

26 avril 2017

LAAS CNRS

Introduction

- Analyse de diagnosticabilité : étude de la capacité à diagnostiquer un système en fonction des observations données
- De nombreux travaux sur le sujet, spécialement dans le cas des SED. En général
  - On se donne le modèle d'un SED (automates, réseau de Petri,...)
  - Ce modèle est un modèle contenant des événements fautifs $f_1, \ldots, f_n$.
  - Le SED est partiellement observable et produit des événements observables $o_1, \ldots, o_m$.
  - Le problème : trouver une méthode pour analyser le SED afin de garantir, a priori, que lorsque le SED sera en opération, si un événement f a lieu, un diagnostiqueur pourra le déterminer avec certitude en un temps fini.

Motivations

- Géneraliser le problème à des comportements plus complexes que de simples événements de faute
- Mieux séparer le modèle du système de l'objectif du diagnostic (motif)
- Mettre en œuvre une méthode générique et automatique
- Formalise utilisé : les réseaux de Petri à priorité
- Mise en œuvre à l'aide d'une technique de vérification de modèle (*Model Checking*)

LAAS CNRS

Réseau de Petri (RP)

Definition (RP)

Un Réseau de Petri est un triplet $N = \langle P, T, A \rangle$ tel que :

- P est un ensemble fini de nœuds (places) ;
- T est un ensemble fini de nœuds (transitions) et $P \cap T = \varnothing$;

LAAS CNRS

Réseau de Petri étiqueté (RPE)

Definition (RP)

Un Réseau de Petri étiqueté est un quintuplet $N = \langle P, T, A, \succ, \ell \rangle$ tel que :

- P est un ensemble fini de nœuds (places) ;
- T est un ensemble fini de nœuds (transitions) et $P \cap T = \varnothing$;
- $A \subseteq (P \times T) \cup (T \times P)$ est une relation binaire qui représente les arcs entre places et transitions ;
- Σ est un ensemble fini d'étiquettes (événements) ;
- $\ell : T \to \Sigma$ est la fonction d'étiquetage.

On parle aussi de réseau de Petri interprété.

LAAS CNRS

Réseau de Petri étiqueté et à priorité (RPEP)

Definition (RPE)

Un Réseau de Petri étiqueté et à priorité est un sextuplet $N = \langle P, T, A, \succ, \ell, \Sigma \rangle$ tel que :

- P est un ensemble fini de nœuds (places) ;
- T est un ensemble fini de nœuds (transitions) et $P \cap T = \varnothing$;
- $A \subseteq (P \times T) \cup (T \times P)$ est une relation binaire qui représente les arcs entre places et transitions ;
- La relation de priorité $\succ \subseteq T^2$ est une relation binaire qui est :
  - transitive ($t_1 \succ t_2 \wedge t_2 \succ t_3 \Longrightarrow t_1 \succ t_3$) ;
  - non-réflexive ($\forall t \in T, t \not\succ t$) ;
  - non-symétrique ($\forall t_1, t_2 \in T, t_1 \succ t_2 \Longrightarrow t_2 \not\succ t_1$) ;
- Σ est un ensemble fini d'étiquettes (événements) ;
- $\ell : T \to \Sigma$ est la fonction d'étiquetage.

LAAS CNRS

Réseau de Petri étiqueté et à priorité de type L (RPEPL)

Definition (RPEP)

Un Réseau de Petri étiqueté et à priorité de type L est un septuplet $N = \langle P, T, A, \succ, \ell, \Sigma, Q \rangle$ tel que :

- P est un ensemble fini de nœuds (places) ;
- T est un ensemble fini de nœuds (transitions) et $P \cap T = \varnothing$;
- $A \subseteq (P \times T) \cup (T \times P)$ est une relation binaire qui représente les arcs entre places et transitions ;
- La relation de priorité $\succ \subseteq T^2$ est une relation binaire qui est :
  - transitive ($t_1 \succ t_2 \wedge t_2 \succ t_3 \Longrightarrow t_1 \succ t_3$) ;
  - non-réflexive ($\forall t \in T, t \not\succ t$) ;
  - non-symétrique ($\forall t_1, t_2 \in T, t_1 \succ t_2 \Longrightarrow t_2 \not\succ t_1$) ;
- Σ est un ensemble fini d'étiquettes (événements) ;
- $\ell : T \to \Sigma$ est la fonction d'étiquetage.

'ensemble de marquage accepteur.

LAAS CNRS

Modèle d'un système

Definition

Le modèle d'système est un RPEPL $\Theta = \langle P, T, A, \succ, \ell, \Sigma_o \cup \Sigma_u, Q, M_0 \rangle$ tel que :

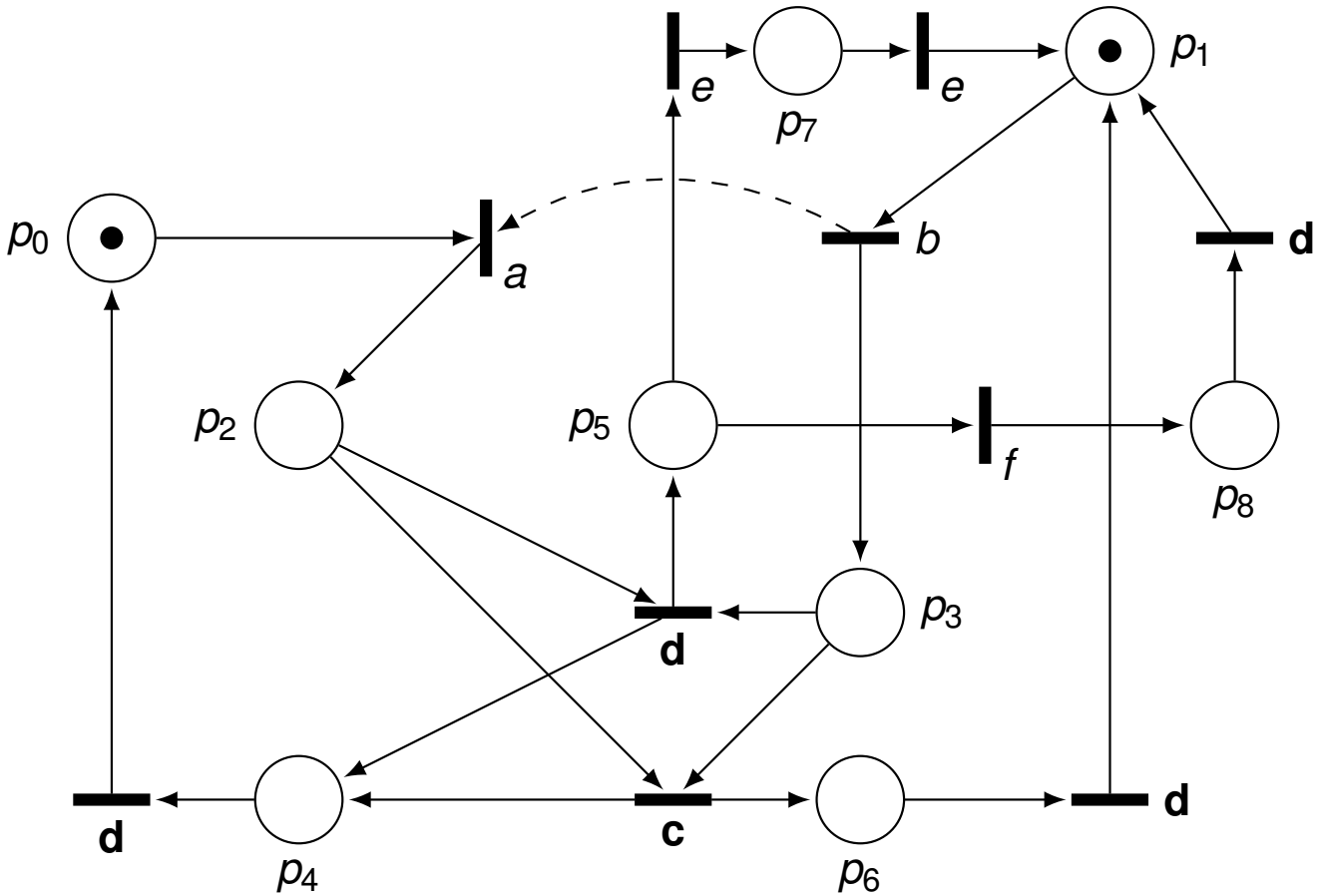
- Σ_o ensemble d'événements observables ;
- Σ_u ensemble d'événements non-observables ;
- Q est l'ensemble des marquages accessibles $R(\Theta, M_0)$;
- le RP est borné ($\exists n \in \mathbb{N}^+ : \forall M \in R(\Theta, M_0), \forall p \in P, M(p) \leq n$).

2 autres hypothèses (classiques) :

1. Pas de deadlock
2. Pas de cycle d'événements non-observables.
3. $\Rightarrow$ toute séquence non-observable est finie et suivie d'un observable

LAAS CNRS

Exemple



Modèle d'un motif

Definition (Motif)

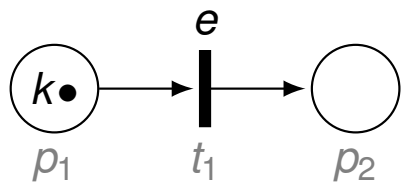
Un motif Ω est un RPEPL

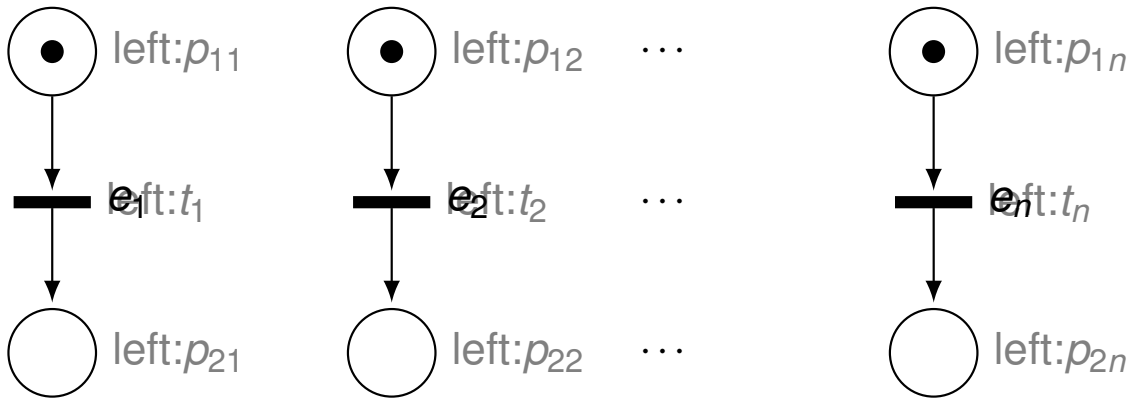
$$\Omega = \langle P, T, A, \succ, \ell, \Sigma, Q, M_0 \rangle$$

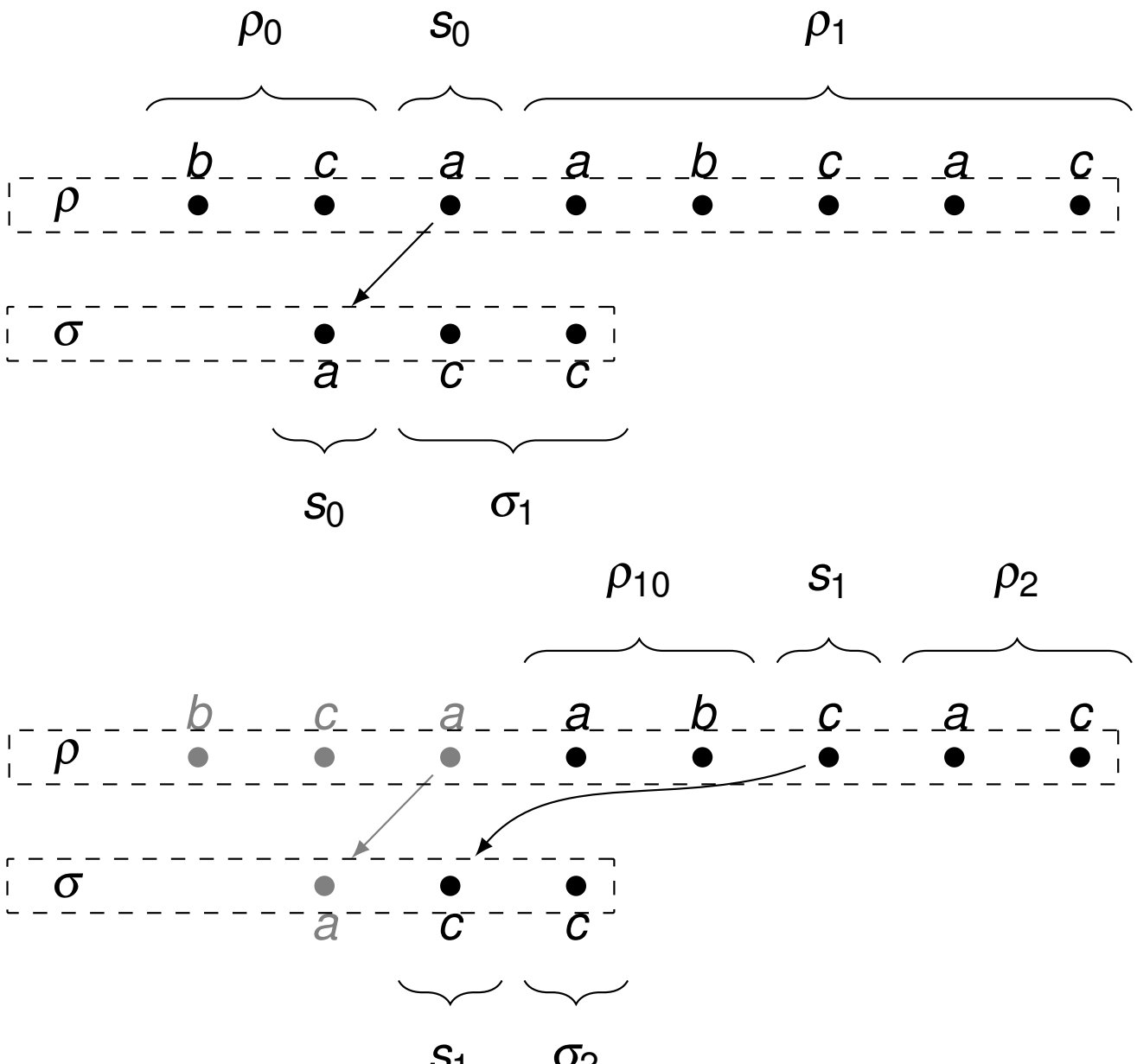
tel que

1. (initialisation) $M_0 \notin Q$ (le mot vide nést pas dans le langage $\mathscr{L}(\Omega)$) ;
2. (bien-formé) de tout marquage accessible M de $R(\Omega, M_0)$ on peut accéder à un marquage accepteur $M' \in Q$;
3. (déterminisme événementiel) de tout marquage accessible M de $R(\Omega, M_0)$, il n'y a pas d'événement $e \in \Sigma$ qui étiquette plus dúne transition ;
4. (stabilité) $\forall M \in Q, \forall M' : (\exists t \in T, M \xrightarrow{t} M') \Rightarrow M' \in Q$;
5. (pas de priorité) $\succ = \varnothing$.

LAAS CNRS


e
k
p1
t1
p2


left:p_{11}
left:t_1
left:p_{21}
left:p_{12}
left:t_2
left:p_{22}
left:p_{1n}
left:t_n
left:p_{2n}


ρ_0
s_0
ρ_1
b c a a b c a c
ρ
σ
a c c
s_0
σ_1
ρ_{10}
s_1
ρ_2
b c a a b c a c
ρ
σ
a c c
s_1
σ_2

Théorème

Soit Θ le RdPLP d'un système sur un alphabet Σ et Ω le RdPLP d'un motif :

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

LAAS CNRS

Théorème

$\mathscr{L}(N_1 \| N_2) = \{\rho \in (\Sigma_1 \cup \Sigma_2)^* : \mathscr{P}_{\Sigma_1 \cup \Sigma_2 \to \Sigma_1}(\rho) \in \mathscr{L}(N_1) \wedge \mathscr{P}_{\Sigma_1 \cup \Sigma_2 \to \Sigma_2}(\rho) \in \mathscr{L}(N_2)\}$.

Théorème

$$\mathscr{L}(\Gamma) = \{\rho \in \Sigma_\Gamma^*, \exists \rho_1, \rho_2 \in \mathscr{L}(\Theta), \rho_1 \ni \Omega \wedge \rho_2 \not\ni \Omega, \mathscr{P}_{\Sigma \to \Sigma_o}(\rho_1) = \mathscr{P}_{\Sigma \to \Sigma_o}(\rho_2) \wedge \rho_1 = \mathscr{P}_{\Sigma_\Gamma \to \Sigma}(\rho) \wedge \rho_2 = \mathscr{R}_{\Sigma' \to \Sigma}(\mathscr{P}_{\Sigma_\Gamma \to \Sigma'}(\rho))\}.$$

LAAS CNRS

Théorème

Un motif Ω est diagnosticable dans un système Θ ssi dans son produit jumelé Γ on ne peut pas tirer de cycles ambigus.

Vérification de modèle : principe

- Représentation d'un système à nombre fini d'états S par une structure de Kripke : M
- Propriété à verifier : formule de logique temporelle φ (LTL,CTL,etc)
- Vérification :

$$\{s \in S : M, s \models \varphi\},$$

  - Déterminer l'ensemble des états s de la structure de Kripke M qui vérifie la propriété φ
- En pratique, un vérificateur répond :
  - VRAI si φ est vérifié (φ est vrai pour au moins un état s), sinon,
  - FAUX + un contre-exemple (une exécution du système où φ n'est pas vérifiée)

LAAS CNRS

Vérification de modèle : structure de Kripke

Definition (Structure de Kripke Classique)

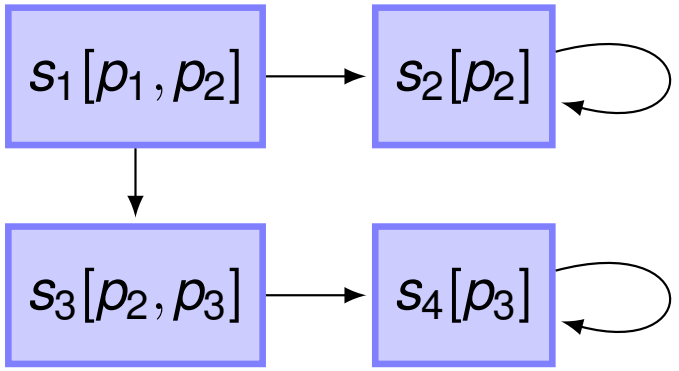
Une structure de Kripke sur un ensemble de propositions atomiques P est une machine à nombre fini d'états $M = (S, S_0, R, L)$ telle que :

1. S est un ensemble fini d'états ;
2. $S_0 \subseteq S$ est l'ensemble des états initiaux ;
3. $R \subseteq S \times S$ est une relation de transition totale, pour tout état $s \in S$, il existe au moins un état $s' \in S$ tel que $R(s, s')$ soit vraie ;
4. $L : S \to 2^P$ est une fonction qui étiquette chaque état avec l'ensemble des propositions atomiques qui sont vraies dans cet état.

LAAS CNRS

Exemples de vérification

Propositions $P = \{p_1, p_2, p_3\}$ Etat initial s_1



Exemple

Formules φ (logique temporelle linéaire)

- $\bigcirc p_2$: dans tout chemin, tout état successeur de s_1 a-t-il la propriété p_2 ? VRAI.
- $\Diamond p_3$: dans tout chemin existe-il un état avec la propriété p_3 ? FAUX. Contre-exemple : $s_1 \to s_2 \to s_2 \ldots$.
- $\Box p_2$: dans tout chemin tout état a-t-il la propriété p_2 ? FAUX. Contre-exemple : $s_1 \to s_3 \to s_4$ et $M, s_4 \not\models p_2$.
- $\Box(p_1 \Rightarrow \Diamond p_2)$: dans tout chemin tout état a-t-il la propriété $p_1 \Rightarrow \Diamond p_2$? VRAI.

LAAS CNRS

Vérificateur de réseau de Petri : TINA

- Transforme des réseaux de Petri (temporels) en structures de Kripke enrichis
- Logique utilisée : SE-LTL (*State/Event Linear Temporal Logic*).

$$
\begin{array}{rcl}
\varphi & ::= & cst \mid r \mid \neg\varphi \mid \varphi \vee \varphi \mid\mid \varphi \wedge \varphi \mid \bigcirc \varphi \mid \Box\varphi \mid \Diamond\varphi \mid \varphi \mathbf{U} \varphi \\
r & ::= & e \mid e \triangle e \\
e & ::= & p \mid a \mid c \mid e \triangledown e \\
cst & ::= & \mathbf{dead} \mid \mathbf{div} \mid \mathbf{sub}
\end{array}
$$

- Propositions : propriétés sur des places p ou des transitions a du réseau ($p_1 \leq 3$, $p_1 + p_4 > p_5$, $a \leq 2$, etc).
- **dead** deadlock, **div** divergence temporelle, **sub** état partiellement connu.

LAAS CNRS

Vérification de la diagnosticabilité avec TINA

- Objectif : trouver la question φ à poser à TINA sur le réseau Γ.
- On doit vérifier : pas de cycles de marquages ambigus
- Autrement dit, à partir d'un marquage ambigu après un nombre fini de transitions :
  - on aboutit à un deadlock ;
  - on aboutit à un marquage non-ambigu.
- D'où la question posée :

$$\varphi_{\text{DIAG}} = \forall\Box((M \in Q_\Gamma) \Rightarrow (\Diamond(M' \notin Q_\Gamma \vee \textbf{dead})))$$

Pour tout chemin $\forall$, pour tout état du chemin $\Box$, s'il contient un marquage ambigu ($M \in Q_\Gamma$) alors cet état sera suivi dans le futur $\Diamond$ soit d'un état non ambigu ($M' \notin Q_\Gamma$), soit d'un deadlock **dead**.

LAAS CNRS

Résumé de la méthode

1. Calcul du produit jumelé $\Gamma = \Theta_{\Omega} || \Theta'_{\overline{\Omega}'}$.
2. Synthèse de φ_{DIAG} issue de Γ.
3. Appel de TINA pour le calcul de la structure de Kripke enrichie $K(\Gamma)$ de Γ (commande `sift`),
4. Appel de TINA pour la vérification de φ_{DIAG} sur $K(\Gamma)$ (commande `selt`).

LAAS CNRS

Complexité algorithmique (au pire)

- p_Ω, t_Ω : nombre de places/transitions de Ω
- p_Θ, t_Θ : nombre de places/transitions de Θ
- Produit jumelé Γ :
  - $2 \times (p_\Omega + p_\Theta)$ places (linéaire)
  - $(t_\Theta + t_\Omega \times t_\Theta)^2$ transitions (quadratique)
- La synthèse de φ_{DIAG} : $O((k+1)^{|p_\Omega|})$ si Ω est k-borné.
- Synthèse de la structure de Kripke (enumérative) :
  - spatial $O((k+1)^{2(p_\Omega+p_\Theta)})$,
  - temporel $2^{O(|\varphi|)}.O((k+1)^{2(p_\Omega+p_\Theta)})$
- Verification sur la structure de φ_{DIAG} : $2^{O(|\varphi|)}.O((k+1)^{2(p_\Omega+p_\Theta)})$

En pratique, TINA optimise la représentation de la structure (ensembles persistents) pour éviter les énumérations.

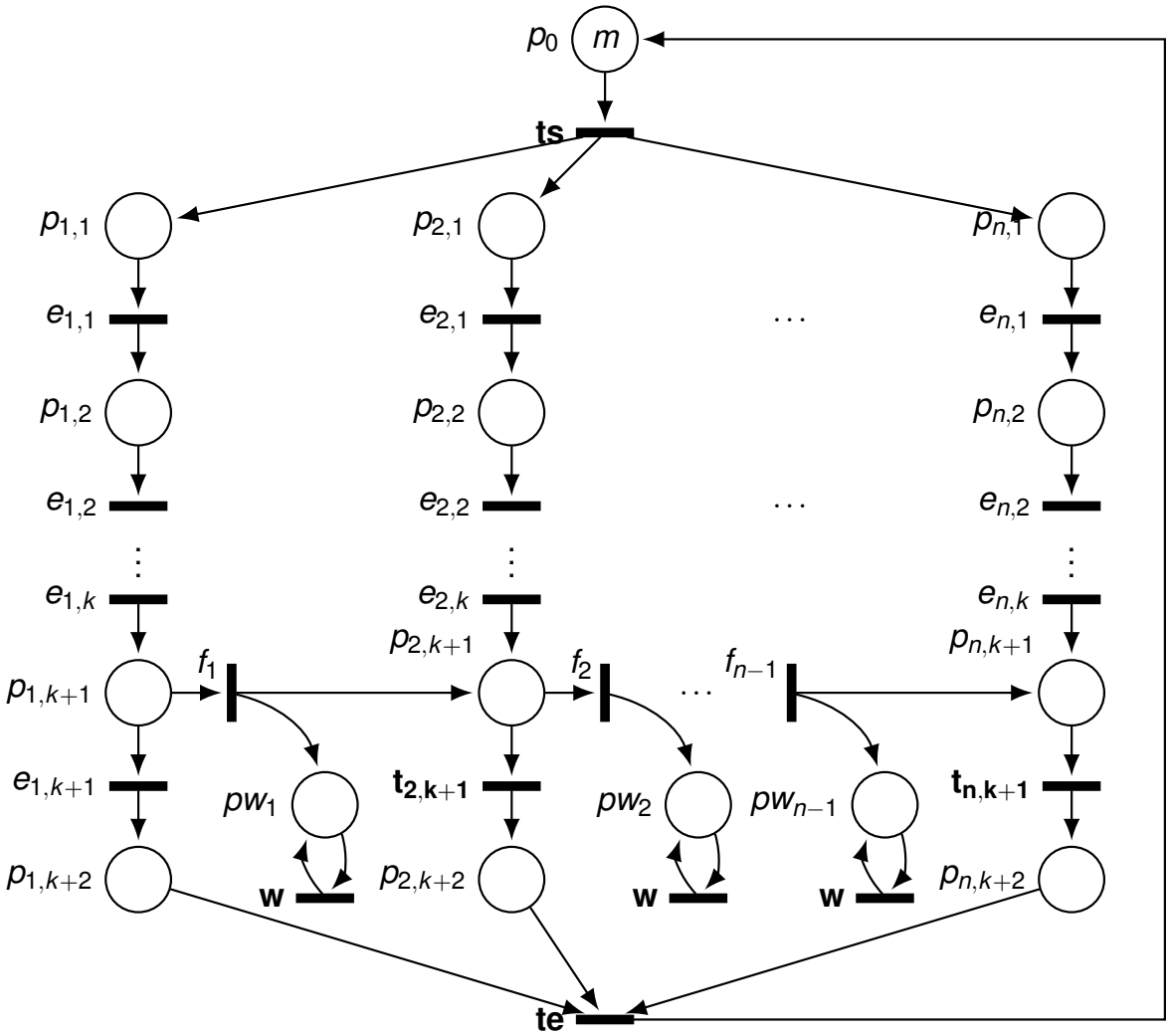
LAAS CNRS

Quelques résultats expérimentaux

Deux études de cas

1. Benchmark WODES [Guia] sur des lignes de production
   - Réseau de Petri classique
   - Objectifs :
     - retrouver les résultats de travaux précédents [Liu] pour validation sur des fautes
     - recherche de nouveaux motifs
2. Système de transport de produits
   - Réseau de Petri à priorité
   - Objectifs :
     - exploiter les priorités du modèle
     - expliciter des motifs plus complexes.

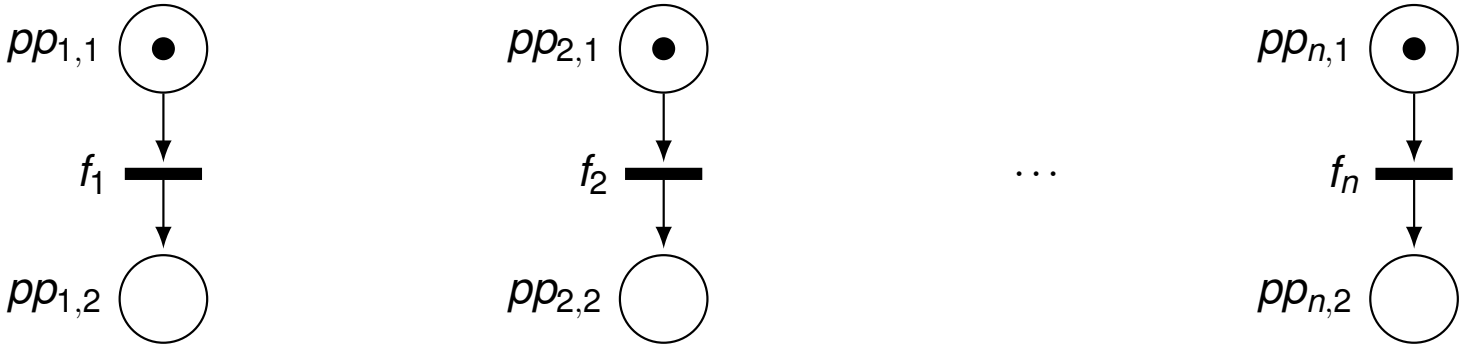
Lignes de production



- n lignes de production de taille $k+1$
- m ressources
- $\mathbf{t_s}, \mathbf{t_e}, \mathbf{t_{i,k+1}}, \mathbf{w}$ observables
- f_i : événements fautifs (déroutage)

Motif de classe fautive simple

- Dans les résultats de [Liu], tout événement de faute f_i appartient à la même classe de faute
- Détectabilité d'un comportement anormal
- Motif associé



- $Q_\Omega = \{M : \exists i \in \{1,\ldots,n\}, M(pp_{i,2}) = 1\}$.
- Pour la configuration $m = 1, n = 3, k = 1$,
  $\varphi_{DIAG3} =$

$$\forall\Box(((pp_{1,2} \geq 1 \vee pp_{2,2} \geq 1) \wedge (\overline{pp_{1,2}} = 0 \wedge \overline{pp_{2,2}} = 0)) \Rightarrow (\Diamond(\overline{pp_{1,2}} \geq 1 \vee \overline{pp_{2,2}} \geq 1 \vee \mathbf{dead})))$$

LAAS CNRS

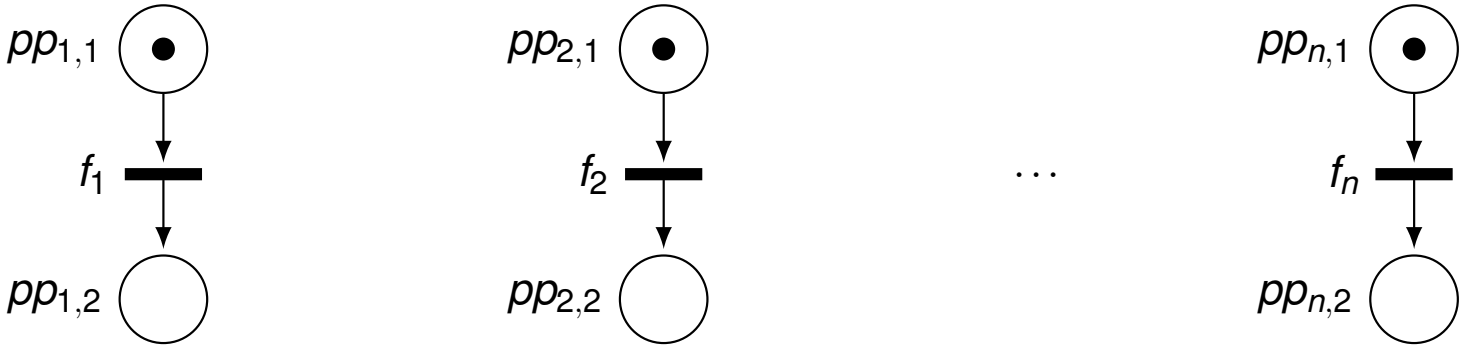
Résultats : classe de faute simple

1	2	3	4	5	6	7	8	9
m	n	k	$nS(\Theta)$	$nT(\Theta)$	$nS(K(\Gamma_3))$	$nT(K(\Gamma_3))$	t. (s)	Res.
1	2	1	15	27	91	237	0.004	Oui
1	2	2	24	45	276	815	0.004	Oui
1	2	3	35	67	659	2085	0.004	Oui
1	2	4	48	93	1348	4455	0.012	Oui
1	3	1	80	250	1434	6640	0.020	Oui
1	3	2	159	512	7071	35087	0.092	Oui
1	3	3	274	892	24550	126348	0.280	Oui
1	3	4	431	1408	68391	360235	0.752	Oui
1	4	1	495	2286	28703	222808	0.44	Oui
1	4	2	1200	5670	225792	1787416	3.864	Oui
1	4	3	2415	11486	1123695	8922268	21.276	Oui
1	4	4	4320	20550	4207640	33358840	76.076	Oui
1	5	1	3295	20382	659323	8108532	18.136	Oui
1	5	2	9691	61187	8234185	99990516	218.668	Oui
2	2	1	96	278	2140	8926	0.016	Non
2	2	2	237	746	17405	85966	0.144	Non
2	3	1	1484	7006	232508	1756465	3.136	Non
2	3	2	5949	30612	5645449	48717944	82.756	Non
2	4	1	28203	190144	35331057	444379980	1393.796	Non
3	2	1	377	1371	21171	110757	0.196	Non
3	3	1	12048	69302	8118900	76016894	166.492	Non

LAAS CNRS

Motif de fautes multiples

- L'occurrence des n fautes est-elle diagnosticable
- Motif associé (seuls les marquages de Q changent)



- $Q_\Omega = \{M : \forall i \in \{1,\ldots,n\}, M(pp_{i,2}) = 1\}$.
- Pour la configuration $m = 1, n = 3, k = 1$,

$$\forall\Box(((pp_{1,2} \geq 1 \wedge pp_{2,2} \geq 1) \wedge (\overline{pp_{1,2}} = 0 \vee \overline{pp_{2,2}} = 0)) \Rightarrow (\Diamond((\overline{pp_{1,2}} \geq 1 \wedge \overline{pp_{2,2}} \geq 1) \vee \mathbf{dead}))).$$

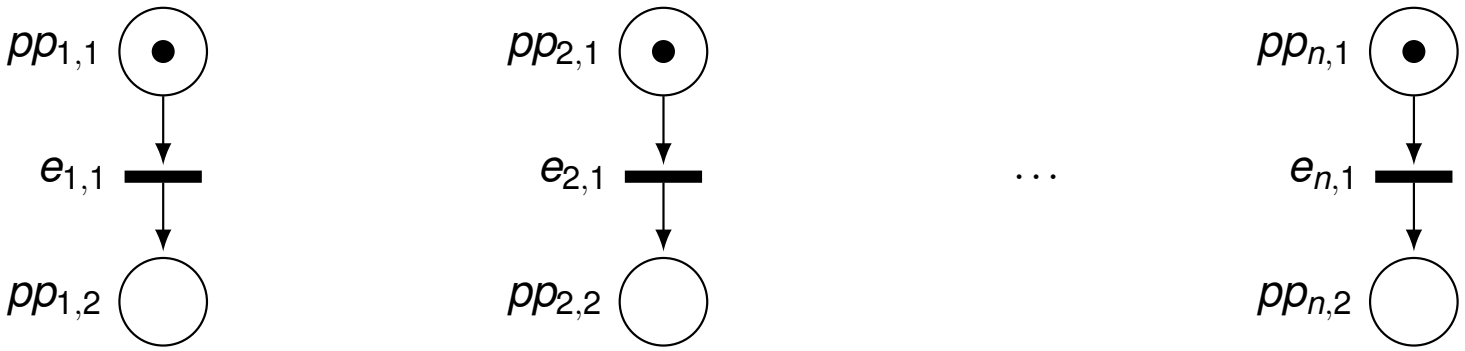
LAAS CNRS

Motif de fautes multiples : résultats

1	2	3	4	5	6	7
m	*n*	*k*	t. (s)	Res. (simple)	t. (s)	Res. (multiple)
1	2	1	0.004	Yes	0.004	Yes
1	2	2	0.004	Yes	0.004	Yes
1	2	3	0.004	Yes	0.004	Yes
1	2	4	0.012	Yes	0.008	Yes
1	3	1	0.020	Yes	0.008	No
1	3	2	0.092	Yes	0.048	No
1	3	3	0.280	Yes	0.164	No
1	3	4	0.752	Yes	0.476	No
1	4	1	0.44	Yes	0.312	No
1	4	2	3.864	Yes	2.552	No
1	4	3	21.276	Yes	13.172	No
1	4	4	76.076	Yes	48.336	No
1	5	1	18.136	Yes	11.956	No
1	5	2	218.668	Yes	150.468	No
2	2	1	0.016	No	0.016	No
2	2	2	0.144	No	0.148	No
2	3	1	3.136	No	2.964	No
2	3	2	82.756	No	87.816	No
2	4	1	1393.796	No	1031.936	No
3	2	1	0.196	No	0.196	No
3	3	1	166.492	No	154.576	No

LAAS CNRS

Motif : un événement sur n



$$Q_\Omega = \{M : \exists i \in \{1, \ldots, n\}, M(pp_{i,2}) = 1\}$$

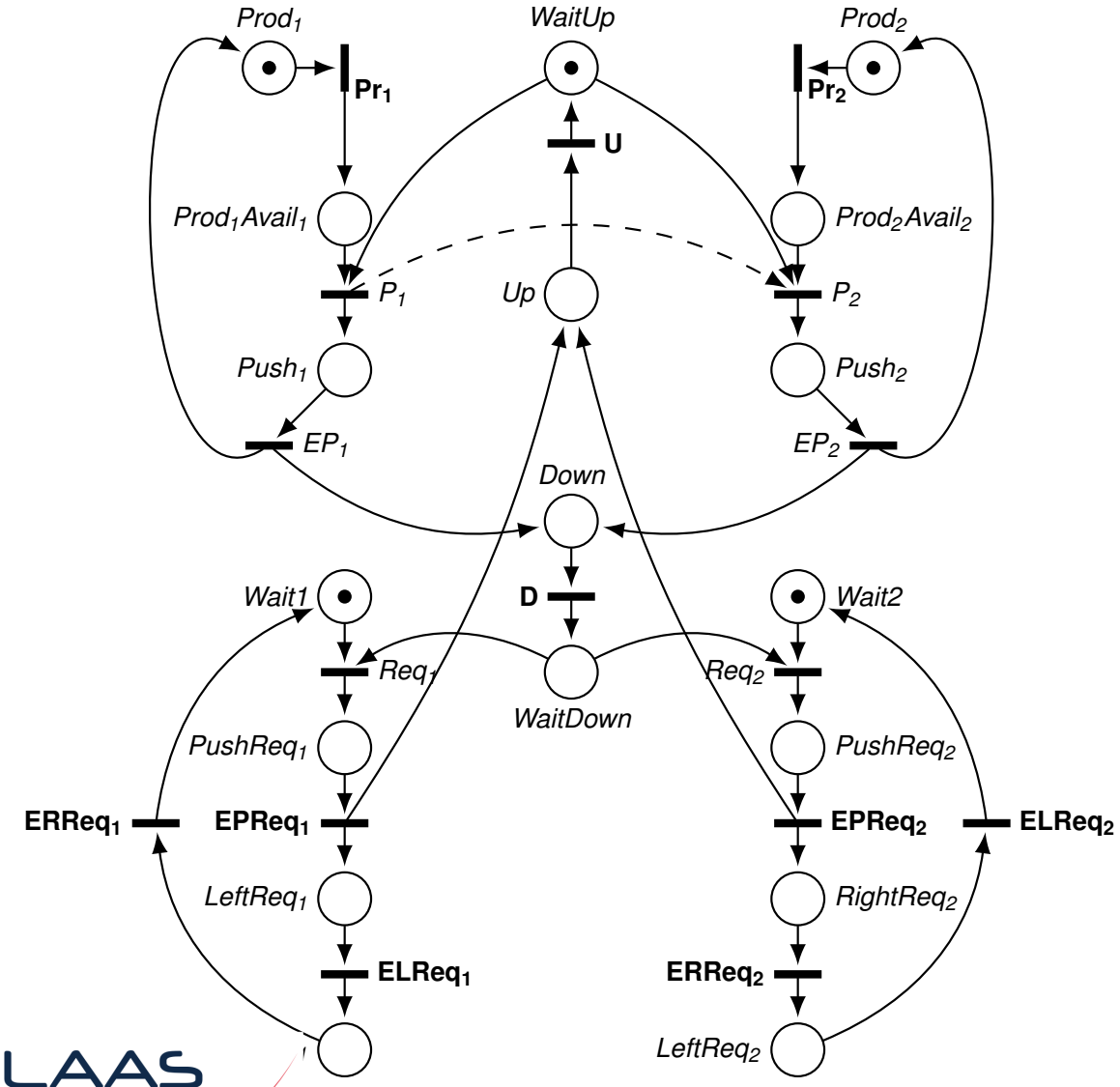
Motif : un événement sur n

m	n	k	$nS(K(\Gamma_5))$	$nT(K(\Gamma_5))$	Temps(s)	Résultat
1	2	1	129	339	0.004	Oui
1	2	2	371	1105	0.004	Oui
1	2	3	853	2719	0.004	Oui
1	2	4	1695	5637	0.008	Oui
1	3	1	2430	11289	0.02	Oui
1	3	2	11238	55858	0.104	Oui
1	3	3	37142	191409	0.376	Oui
1	3	4	99486	524706	1.032	Oui
1	4	1	52901	410215	0.796	Oui
1	4	2	393198	3103031	6.834	Oui
1	4	3	1865237	14754887	31.576	Oui
1	4	4	6708482	52988035	116.572	Oui
1	5	1	1265621	15542016	32.364	Oui
1	5	2	15124090	182988624	683.392	Oui
2	2	1	2470	10156	0.02	Oui
2	2	2	18950	92732	0.2	Oui
2	3	1	311440	2320207	5.4	Oui
2	3	2	6552732	55877578	141.884	Oui
3	2	1	22817	117993	0.26	Oui
3	3	1	10032272	92786651	251.288	Oui

Note : le motif *2 événements sur n* n'est pas diagnosticable.

LAAS CNRS

Autre exemple : système de transport d'objets

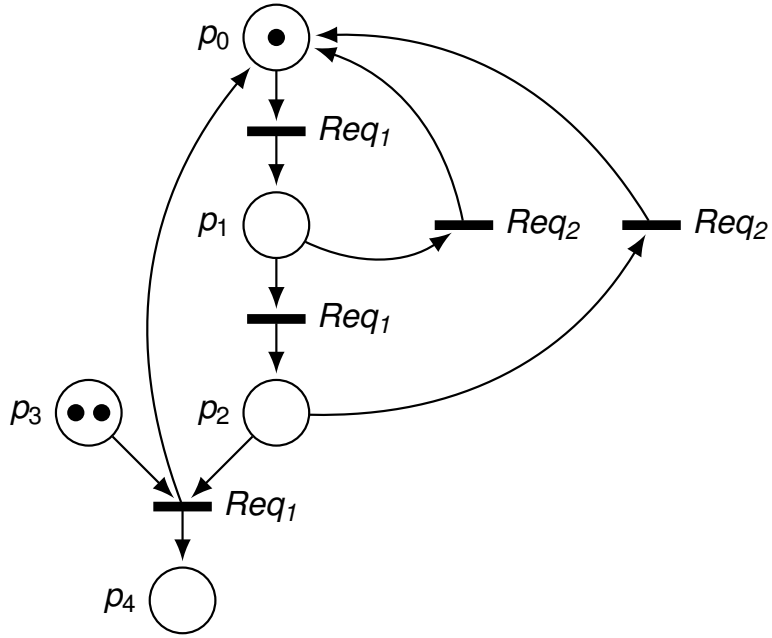


- 4 tapis roulants + un ascenseur
- Les tapis du haut envoient des objets dans un ascenseur
- Les tapis du bas recoivent les objets et les délivrent
- Tapis en haut à gauche prioritaire sur celui en haut à droite
- Pas d'événements fautifs.

LAAS CNRS

Motif : occurrences consécutives

- Peut-on diagnostiquer avec certitude k fois l'occurrence consécutive de n requêtes Req_1 ? Pour $n = 3$ et $k = 2$:



- φ_{DIAG}

$$\forall\Box((p_4 \geq 2 \wedge \overline{p_4} \leq 1) \Rightarrow (\Diamond(\overline{p_4} \geq 2 \vee \mathbf{dead})))$$

LAAS CNRS

Résultats

n	k	$nP(\Gamma_7)$	$nT(\Gamma_7)$	$nS(K(\Gamma_7))$	$nT(K(\Gamma_7))$	Temps(s)	Résultat
2	2	44	48	4092	12616	0.032	Oui
3	2	46	52	6126	18886	0.052	Oui
4	3	48	56	10890	33558	0.088	Oui
10	4	60	80	33960	104660	0.296	Oui

LAAS CNRS

Conclusions

- Méthode générique pour la vérification automatique de la diagnosticabilité de motif dans des SED
- Gestion des systèmes à priorités
- Combine le principe du projet jumelé (recherche de cycles ambigus) avec le principe de la vérification de modèles
- S'appuie sur l'outil d'analyse TINA.

LAAS CNRS

Perspectives

- Augmenter l'expressivité des motifs (motifs non réguliers)
- Intégration des aspects temporels
- Analyse de discriminabilité des motifs.

LAAS CNRS