Diagnosticabilité des systèmes à événements discrets

Yannick Pencolé

31 mars 2008

Plan du cours

Diagnosticabilité : introduction informelle

- On considère un système quelconque
  - Soit Δ l'algorithme de diagnostic suivant :
    1. Attendre une observation du système
    2. Afficher **Tout est possible**
    3. Aller en 1
- L'algorithme de diagnostic Δ est correct
  - Peu importe ce qui s'est réellement passé, le résultat de Δ n'est pas remis en question
- L'algorithme de diagnostic Δ est inutile
  - Il n'y a aucune discrimination entre les situations
  - Les observations ne sont d'aucune utilité pour raffiner le diagnostic

Diagnosticabilité : introduction informelle

- Diagnosticabilité d'un système
  - Mesure de la capacité de diagnostic d'un algorithme Δ sur un système
  - Quelles pannes peuvent être discriminées par Δ et les observations du système ?
  - En général, c'est une propriété logique qu'un algorithme vérifie sur un système

Diagnosticabilité : motivations

1. Établir la qualité, les limites d'un algorithme Δ sur un système S
   - Est-il possible avec Δ d'identifier dans tous les cas l'occurrence d'une panne P ?
2. Sélectionner l'algorithme Δ le mieux adapté au système S afin de répondre aux objectifs de diagnostic (détection, localisation, ...)
3. Améliorer l'observabilité du système (placement intelligent de capteurs)
4. Revoir la conception du système
   1. pour faciliter sa maintenance (diagnostic précis)
   2. pour améliorer sa robustesse face aux pannes (autoguérison)

Diagnosticabilité : une première définition très générale

Définition

Diagnosticabilité = capacité pour un système et ses mécanismes de surveillance d'exhiber des observations associées à chaque situation fautive anticipée.

- système : S
- mécanismes de surveillance : algorithme Δ (au sens large incluant les capteurs)
- situation fautive anticipée : situation de panne P connue et décrite dans le modèle $M(S)$ sur lequel s'appuie Δ
- observations associées : ensemble des observations possibles de S par Δ dont l'origine est une panne P selon le modèle $M(S)$

Plan du cours

Diagnosticabilité dans les SED : intuition

- Soit $G = (X, T, \Sigma, x_0)$ un système de transition représentant un modèle global
- Soit F un événement de panne $F \in \Sigma \cap \Sigma_{no}$

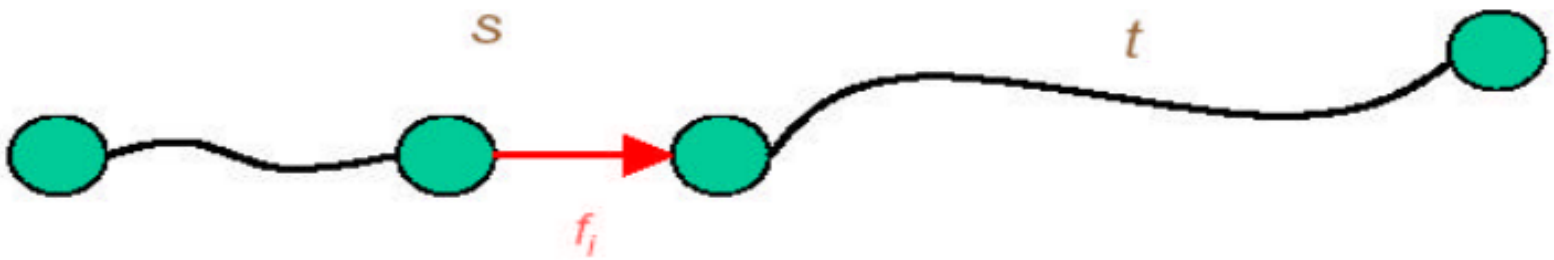
Définition

L'occurrence de l'événement F est diagnosticable s'il est toujours possible de diagnostiquer l'occurrence de F sans ambiguité après un nombre fini d'observations qui suivent cette occurrence.

Autrement dit, si F est diagnosticable :

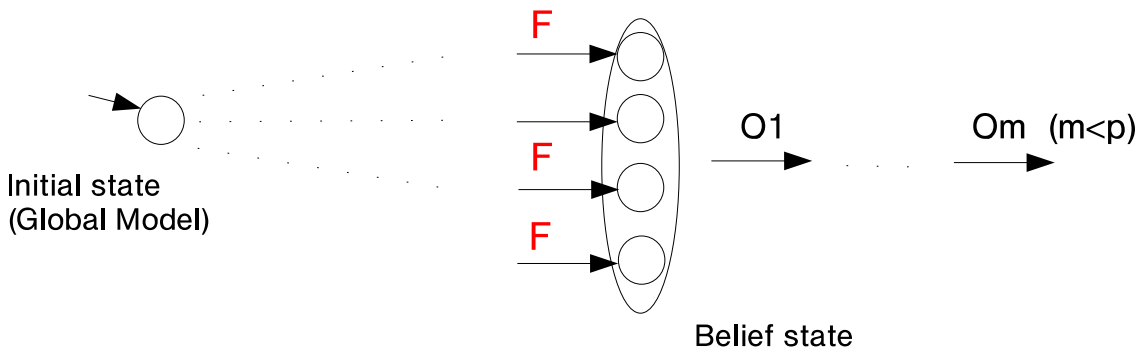
1. Il est toujours possible de conclure sur la présence certaine de F (d'après le modèle G)
2. Cette conclusion est établie en attendant un nombre fini d'observations

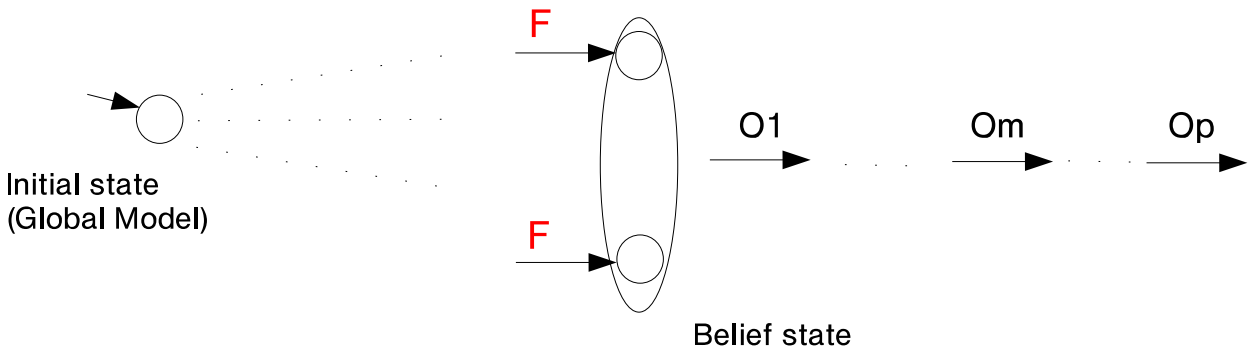
Diagnosticabilité dans les SED : intuition (2)



- Trajectoire $s \in \Sigma^\star$ terminée par un événement de panne F
- Trajectoire $t \in \Sigma^\star$ continuation suffisamment longue
- Toute trajectoire "ressemblant" à $s.t$ doit contenir un événement F
  - Ressemblance $\equiv$ Même comportement observable

Diagnosticabilité dans les SED : intuition (2)





Diagnosticabilité dans les SED : définition classique

Définition

Soit $F \in \Sigma \cap \Sigma_{no}$ un événement de panne,
F diagnosticable $\equiv$

$$\exists n \in \mathbb{N}, \forall s \in L(G) \cap (\Sigma^{\star}.F), \forall t \in L(G)/s,$$

$$|t| \geq n \Rightarrow$$

$$(\omega \in P^{-1}_{L(G)}(P_{\Sigma_o}(st)) \Rightarrow F \in \omega$$

Décryptage

- $\exists n \in \mathbb{N}$: il existe un entier n (nombre fini)
- $\forall s \in L(G) \cap (\Sigma^\star.F)$: pour toute trajectoire s de G finissant par l'événement de panne F
- $\forall t \in L(G)/s$: pour toute continuation t de s dans G
  - $L(G)/s \triangleq \{t | st \in L(G)\}$
- $|t| \geq n$: la longueur de t est plus grande que n
- $\sigma = P_{\Sigma_o}(st)$ projection observable de st (sequence d'observations $P_{\Sigma_o}(st) \in \Sigma_o^\star$)
- $P^{-1}_{L(G)}(\sigma) = \{\omega \in L(G) \wedge P_{\Sigma_o}(\omega) = \sigma\}$: ensemble des trajectoires de G dont la projection observable est σ
- $\omega \in P^{-1}_{L(G)}(P_{\Sigma_o}(st))$: ω est une trajectoire de G dont la trace observable est identique à celle de la trajectoire st
- $F \in \omega$: F est dans la trajectoire ω

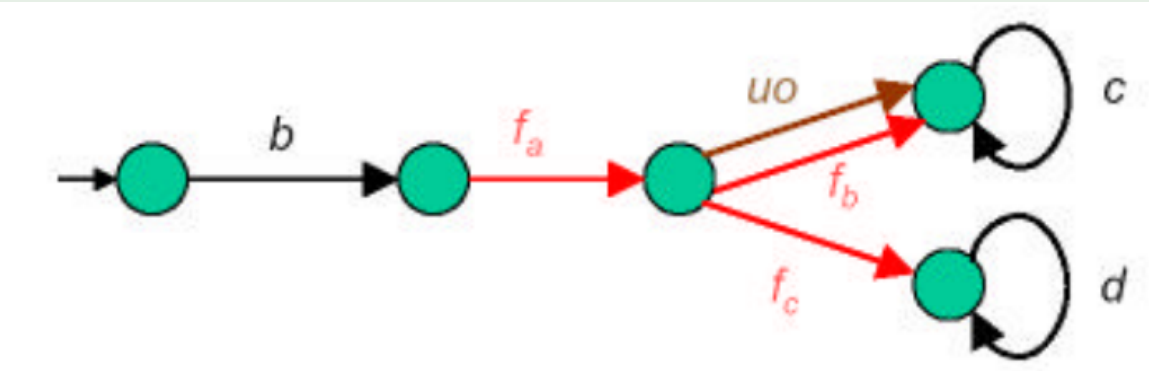
Traduction

Définition

F diagnosticable $\equiv$
"Il existe un entier n tel que pour toute trajectoire s de G menant à l'événement de panne F et toute continuation t de s dans G, si cette continuation est plus grande que n alors tout comportement de G dont la trace observable est identique à celle de $s.t$ contient nécessairement l'événement F."

À vous de jouer

Exemple

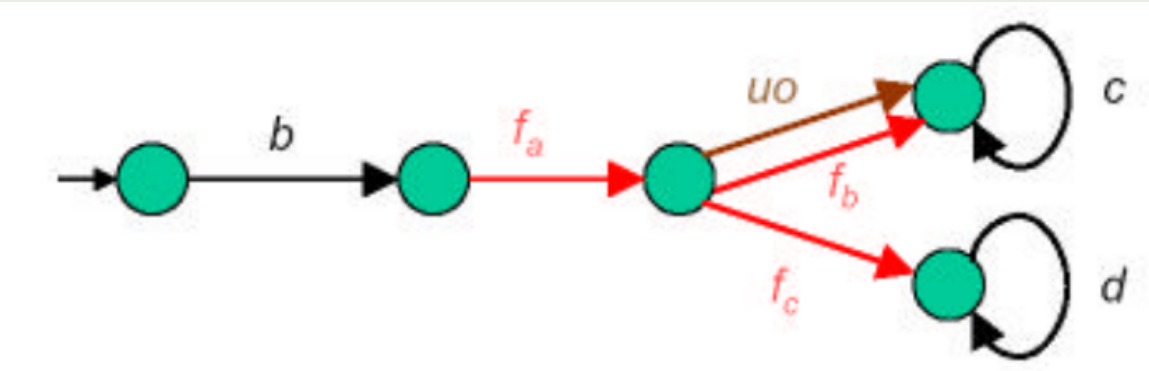


b, c, d sont les événements observables
uo est un événement observable
f_a, f_b, f_c événements de panne (non observables)
Questions :

- f_a **diagnosticable ?**
- f_b **diagnosticable ?**
- f_c **diagnosticable ?**

Résultat pour f_a

Exemple

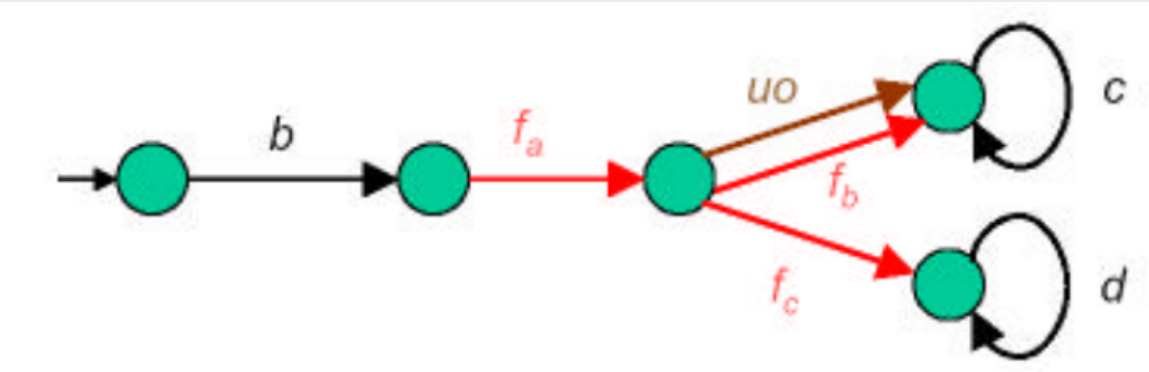


Application de la définition :

- Un seul s : $s = b.f_a$
- Tous les t sont de la forme : $\varepsilon + uo.c^\star + f_b.c^\star + f_c.d^\star$
- Soit $n = 2$ et $|t| \geq 2$, la trace observable de st est alors de la forme $bcc^\star + bdd^\star$
- Tout ω de $P^{-1}_{L(G)}(P_{\Sigma_o}(st))$ est de la forme $b.f_a.f_c.d.d^\star + b.f_a.(f_b + uo).c.c^\star$
- Donc $f_a \in \omega$, **$\mathbf{f_a}$ est diagnosticable**.

Résultat pour f_b

Exemple

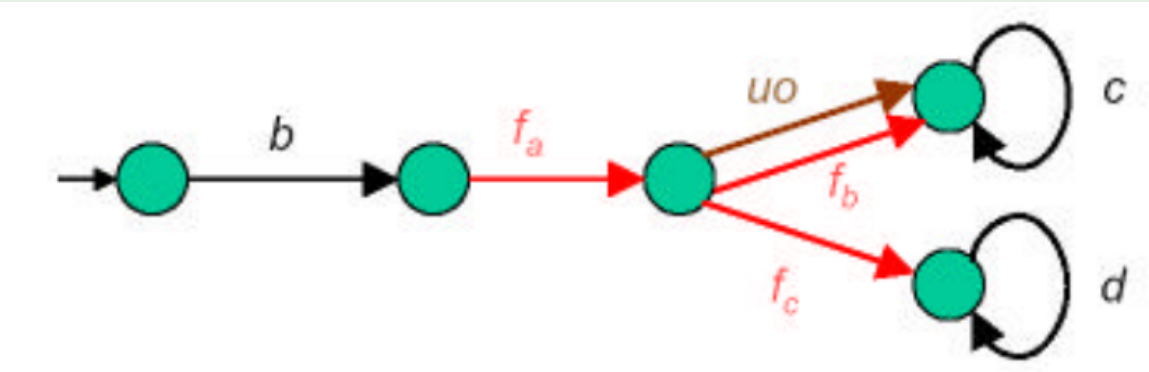


Application de la définition :

- Un seul s : $s = b.f_a.f_b$
- Tous les t sont de la forme : $c^\star$
- Pour tout $n \in \mathbb{N}$ soit $|t| = n$ donc $t = c^n$ et $P_{\Sigma_o}(st) = b.c^n$
- Il existe toujours ω tel que $P_{\Sigma_o}(\omega) = b.c^n$ et $f_b \notin \omega$, à savoir $\omega = b.f_a.uo.c^n$
- Donc $\mathbf{f_b}$ **n'est pas diagnosticable**.

Résultat pour f_c

Exemple



Application de la définition :

- Un seul s : $s = b.f_a.f_c$
- Tous les t sont de la forme : $d^\star$
- Soit $n = 1$ soit $|t| \geq 1$ donc t est de la forme $d.d^\star$ $P_{\Sigma_o}(st) = b.d.d^\star$
- Tout ω tel que $P_{\Sigma_o}(\omega) = b.d.d^\star$ est de la forme $= b.f_a.f_c.d.d^\star$
- Donc $\mathbf{f_c}$ **est diagnosticable**.

Généralisation de la définition

- Un événement de panne f appartient à un type de panne F ($f \in F$)
- De façon générale, on considère un ensemble de types de panne $F_1, \ldots, F_m$
  - Partition des pannes $\Pi_f = \{F_1, \ldots, F_m\}$

Définition

G est diagnosticable $\equiv$

$$\forall F_i \in \Pi_f, \exists n \in \mathbb{N}, \forall s \in L(G) \cap (\Sigma^\star.f_1) \wedge f_1 \in F_i, \forall t \in L(G)/s,$$

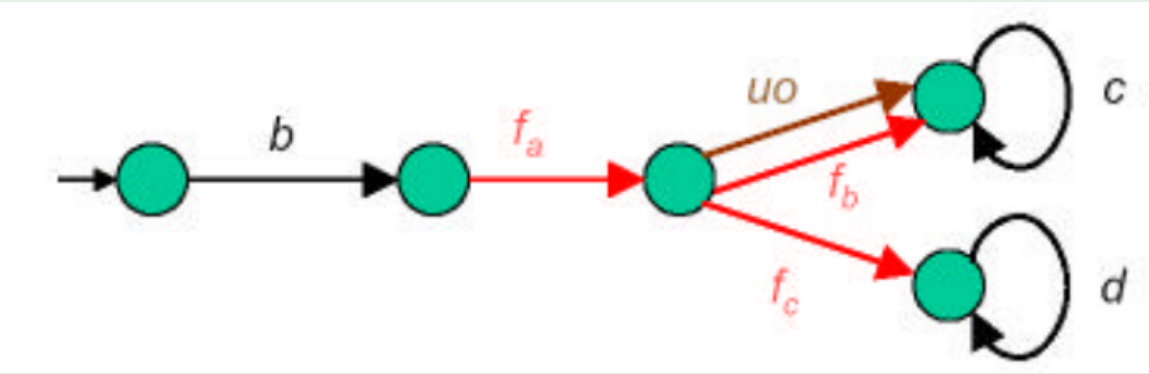
$$|t| \geq n \Rightarrow$$

$$(\omega \in P^{-1}_{L(G)}(P_{\Sigma_o}(st)) \Rightarrow \exists f_2 \in \omega \wedge f_2 \in F_i$$

En pratique, si on renomme dans G tout f de F_i par F_i, c'est équivalent à la définition précédente.

Exemple

Exemple



Questions :

- Soit $\Pi_f = \{F_1 = \{f_a\}, F_2 = \{f_b\}, F_3 = \{f_c\}\}$, G **diagnosticable ?**
- Soit $\Pi_f = \{F_1 = \{f_a, f_b\}, F_2 = \{f_c\}\}$, G **diagnosticable ?**

Plan du cours

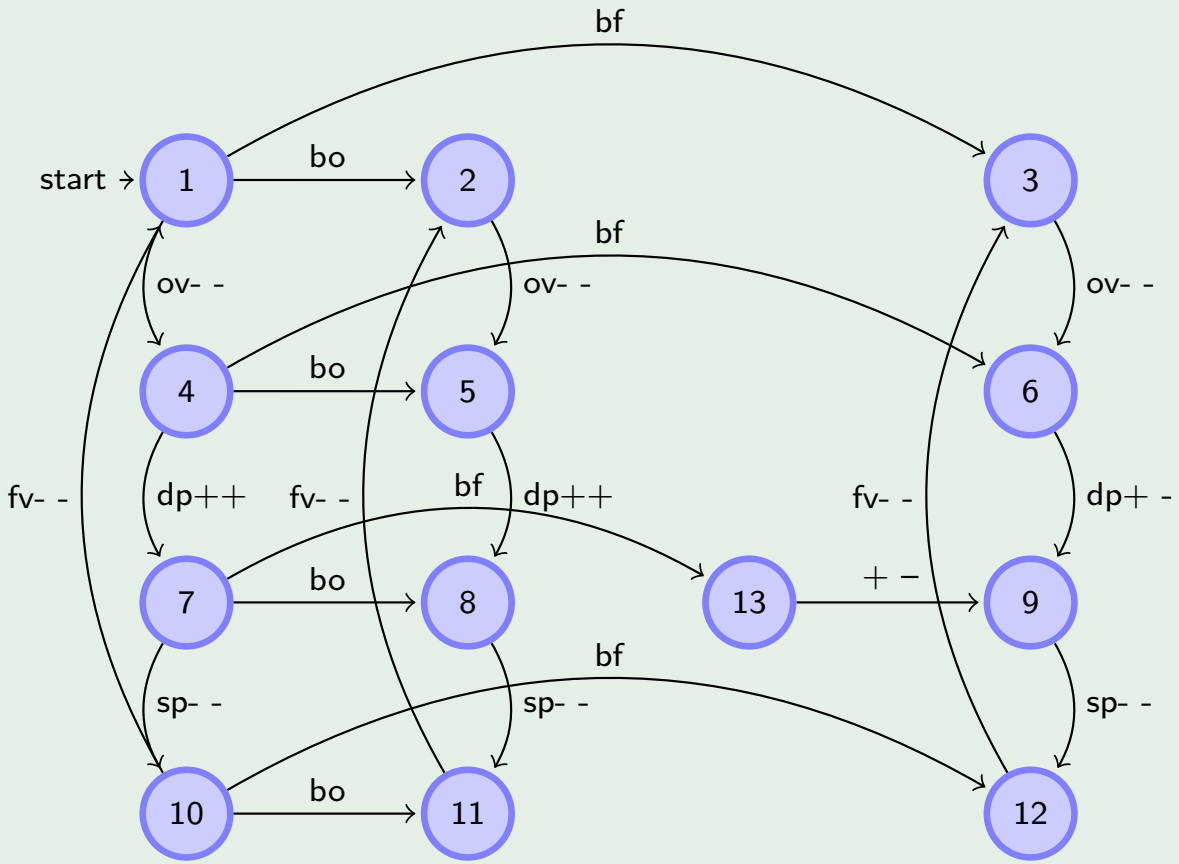
Analyse automatique de la diagnosticabilité

- Etant donné un modèle M
- Comment établir automatiquement si les pannes dans M sont diagnosticables ?
- Diagnostiqueur : cette machine est idéale je vous dis ! !

Diagnosticabilité : approche diagnostiqueur (1)

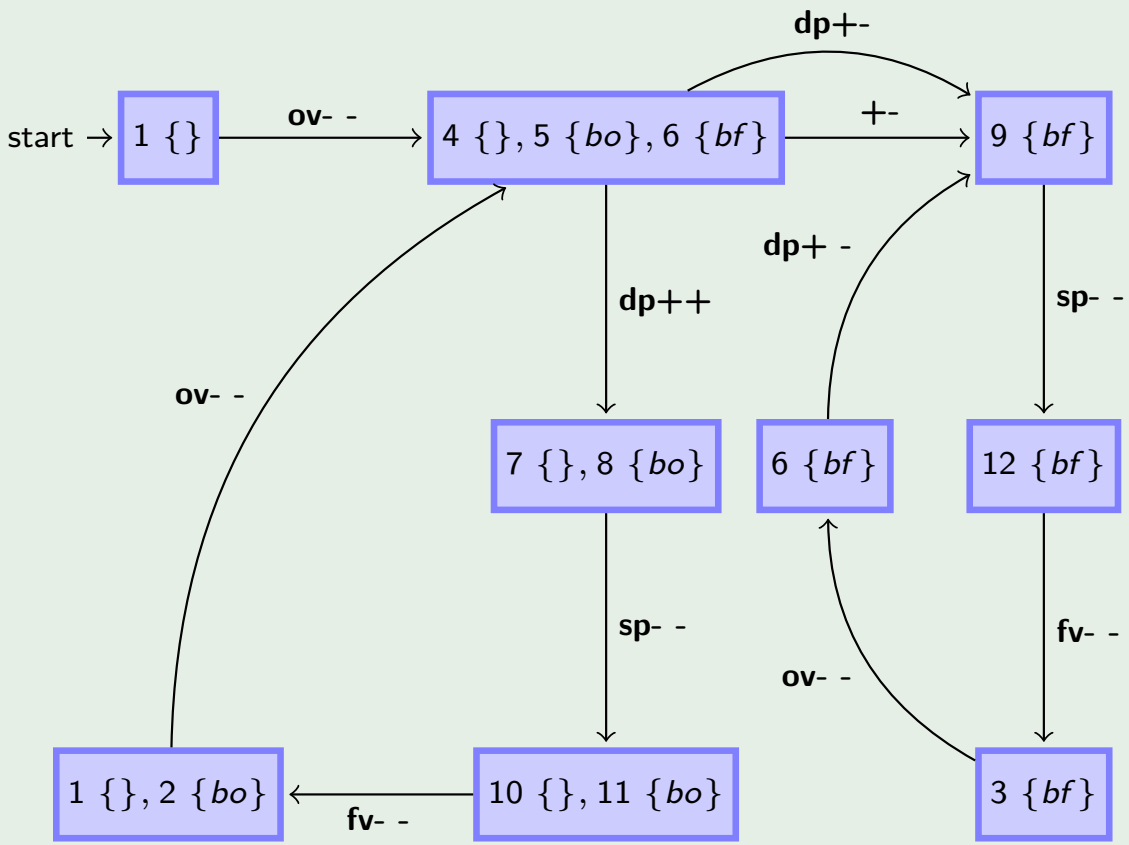
Exemple

bo : bloqué ouverte
bf : bloqué fermé
ov : ouvre valve
fv : ferme valve
dp : démarrre pompe
fp : ferme pompe
++ : débit
- - : pas débit
+- : plus aucun débit



Diagnosticabilité : approche diagnostiqueur (2)

Exemple



Diagnosticabilité : approche diagnostiqueur (3)

- Soit x un état du diagnostiqueur
  - x est de la forme $((x_1, F_1), \ldots, (x_m, F_m))$
  - x_i état du modèle global
  - F_i un ensemble de fautes
- Soit f une faute
- x est f-sain ssi $\forall F_i, f \notin F_i$
- x est f-sure ssi $\forall F_i, f \in F_i$
- x est f-incertain ssi $\exists F_i, f \in F_i \wedge \exists F_j, f \notin F_j$

Diagnosticabilité : approche diagnostiqueur (4)

- Soit x un état du diagnostiqueur
- Soit $L_{OBS}(x) \subseteq L_{OBS}(M) = L(diagnostiqueur)$ tel que : $\forall m \in L_{OBS}(x)$ si le diagnostiqueur reçoit m alors le diagnostiqueur atteint l'état x

Exemple

Soit $x = 7\{\}, 8\{bo\}$ alors
$L_{OBS}(x) = ov--.dp++.(sp--.fv--ov--.dp++)^{\star}$

Soit $x = 9\{bf\}$ alors
$L_{OBS}(x) = ov--.(dp+-\oplus+-).(sp--.fv--ov--.dp+-)^{\star}$

Diagnosticabilité : approche diagnostiqueur (4)

- Si x est f-sain
  - sur toute évolution $m \in L(M)$ du système tel que $P_{OBS}(m) \in L_{OBS}(x)$, f n'est pas présente
  - dans toutes ces évolutions f est donc diagnosticable
- Si x est f-sure
  - sur toute évolution $m \in L(M)$ du système tel que $P_{OBS}(m) \in L_{OBS}(x)$, f est présente
  - dans toutes ces évolutions f est donc diagnosticable
  - f panne permanente donc tout successeur de x est f-sain.

Diagnosticabilité : approche diagnostiqueur (5)

- Si x est f-incertain
  - sur une évolution $m_1 \in L(M)$ du système tel que $P_{OBS}(m) \in L_{OBS}(x)$, f est présente
  - sur une évolution $m_2 \in L(M)$ du système tel que $P_{OBS}(m) \in L_{OBS}(x)$, f n'est pas présente
  - si m_1 et m_2 sont infinis alors f n'est pas diagnosticable

Diagnosticabilité : approche diagnostiqueur (5)

- Hypothèse 1 : le modèle ne contient pas de cycles non observables
  - Pas restrictif car si de tels cycles existent, le système est probablement pas diagnosticable
- Hypothèse 2 : $L_{obs}(M)$ est un langage vivant
  - $\forall \sigma \in L_{obs}(M), \exists o \in \Sigma_o, \sigma.o \in L_{obs}(M)$
  - Le cas où le langage observable n'est pas vivant est un cas particulier

Diagnosticabilité : approche diagnostiqueur (6)

- Soit x un état f-incertain, m_1 et m_2 deux évolutions infinies et contradictoires menant à x
  - Si Hyp1 est vraie alors $P(m_1) = P(m_2) = \sigma \in L_{OBS}(x)$ avec σ infiniment grand.

- **Question : quelle condition doit remplir x dans le diagnostiqueur pour que le diagnostiqueur puisse atteindre x après un nombre infiniment grand d'observations ?**

Diagnosticabilité : approche diagnostiqueur (7)

Théorème

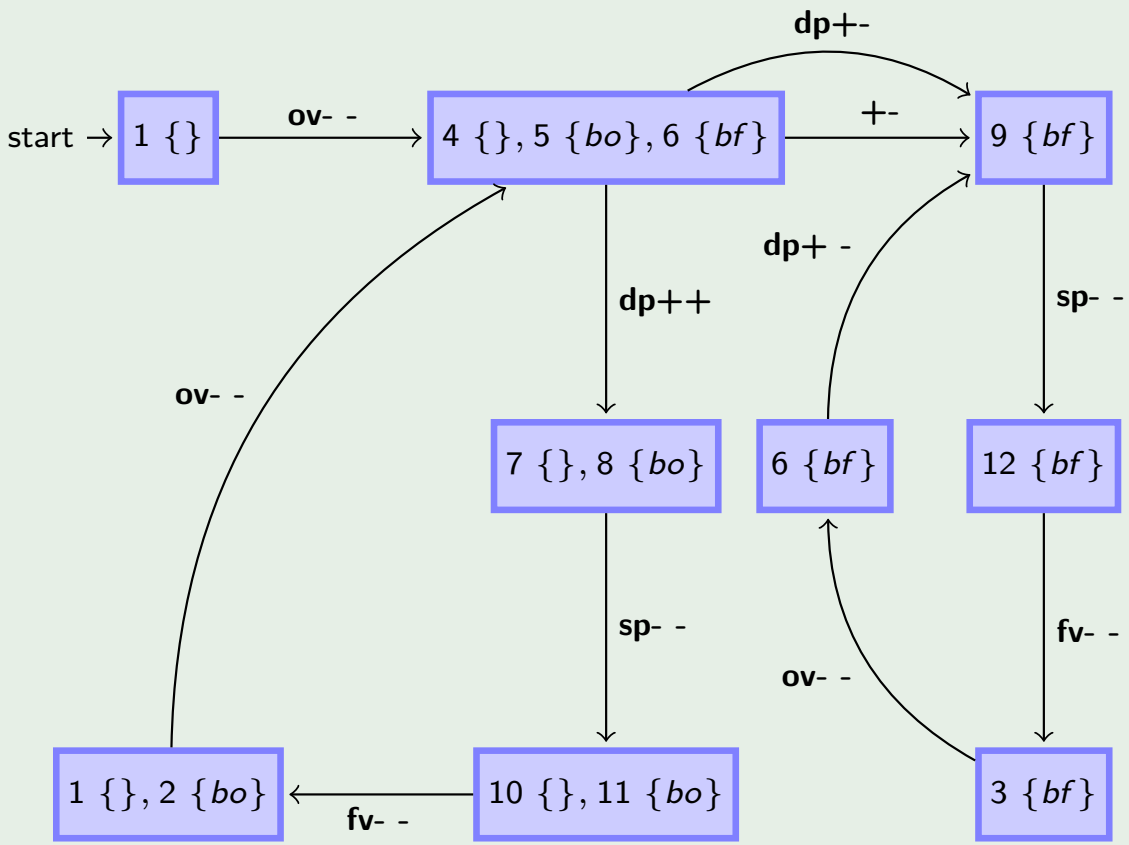
Soit M un modèle vérifiant les hypothèses 1 et 2, f est diagnosticable ssi il n'existe pas d'état f-incertain dans un cycle du diagnostiqueur.

Théorème

Soit M un modèle vérifiant les hypothèses 1 et 2, soit Π_f une partition de panne sur M, Π_f est diagnosticable ssi il n'existe pas d'état Π_f-incertain dans un cycle du diagnostiqueur.

À vous de jouer

Exemple



Résumé de l'approche

- Diagnosticabilité $\equiv$ Vérification d'un critère sur le diagnostiqueur de Sampath
- Recherche d'un cycle dans le diagnostiqueur
- Inconvénient : au pire cas, on construit entièrement le diagnostiqueur
  - Algorithme en $O(2^N)$ où N est le nombre d'états dans le modèle global
  - Algorithme en $O(2^{2^n})$ où n est le nombre de composants du système ! !
- Cette machine est utopique je vous dis ! !
- Peut mieux faire ! !

La méthode des modèles jumeaux

- Le diagnostiqueur est une machine trop riche
- Pas besoin de l'utiliser pout tester la diagnosticabilité
- Technique des modèles jumeaux (*twin-plant*) bien meilleure

Couples critiques

- Une panne F n'est pas diagnosticable ssi
  - il existe une trajectoire infinie m_1 du système dans laquelle F a lieu
  - il existe une trajectoire infinie m_2 du système dans laquelle F n'a pas lieu
  - $P_{OBS}(m_1) = P_{OBS}(m_2)$ même trace observable
- Un couple (m_1, m_2) est un couple critique de F

Théorème

F est diagnosticable dans le modèle M ssi il n'existe pas de couple critique de F.

Couples critiques (2)

Exemple

Système d'air conditionné :
Soit $m1 = (ov--.dp++.sp--)^{\infty}$

Soit $m2 = bo.(ov--.dp++.sp--)^{\infty}$

Le couple (m_1, m_2) est un couple critique de **bo**. **bo** n'est pas diagnosticable.

Comment déterminer un couple critique

- Confronter deux évolutions différentes du même modèle qui ont la même trace observable
- Principe des modèles jumeaux :
  - Soit M un modèle et $L(M)$ son langage, $L(M) \subseteq \Sigma_M^\star$
  - Soit $\Sigma_{M'} = \{l' | l \in \Sigma_M \setminus \Sigma_{OBS}\} \cup \{l | l \in \Sigma_{OBS}\}$ (on renomme avec des ' les symboles non-observables de Σ_M)
  - Soit M' le jumeau (duplication et renommage de M), $L(M') \subseteq \Sigma_{M'}^\star$
  - On fait jouer M et M' en parallèle et on synchronise sur les observations :

$$L(M)||_{OBS}L(M')$$

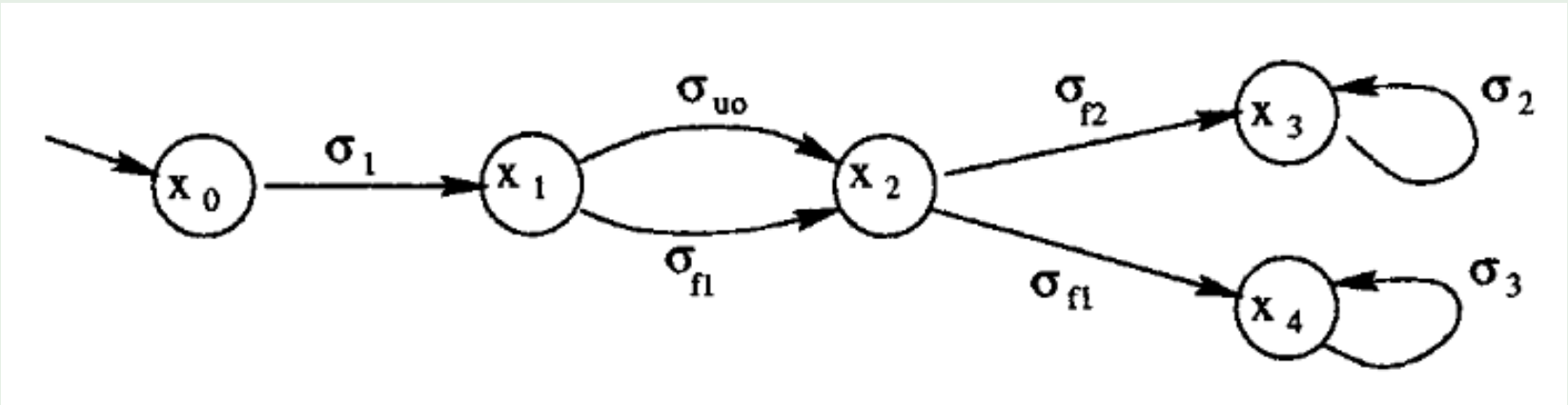
Comment déterminer un couple critique (2)

- Soit $m \in L(M)||_{OBS} L(M')$ trajectoire infinie
  - $m_1 = P_{\Sigma_M}(m)$ est une trajectoire infinie de M (Hypothèse 1)
  - $m_2 = P_{\Sigma_{M'}}(m)$ est une trajectoire infinie de M'
  - $P_{OBS}(m) = P_{OBS}(m_1) = P_{OBS}(m_2)$
- Si $f \in m_1$ et $f \notin m_2$, alors (m_1, m_2) est un couple critique

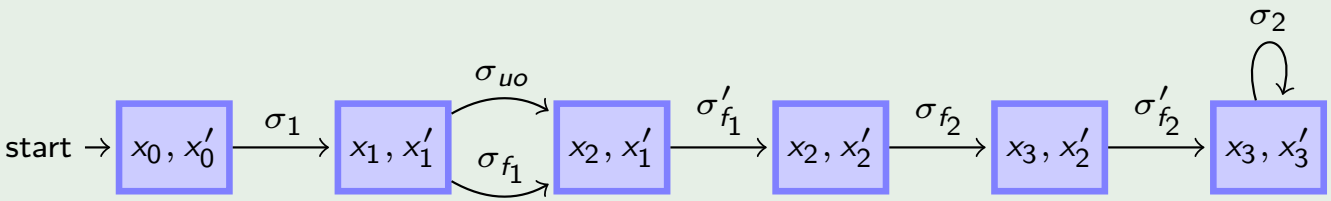
Exemple

Exemple

Modèle global M

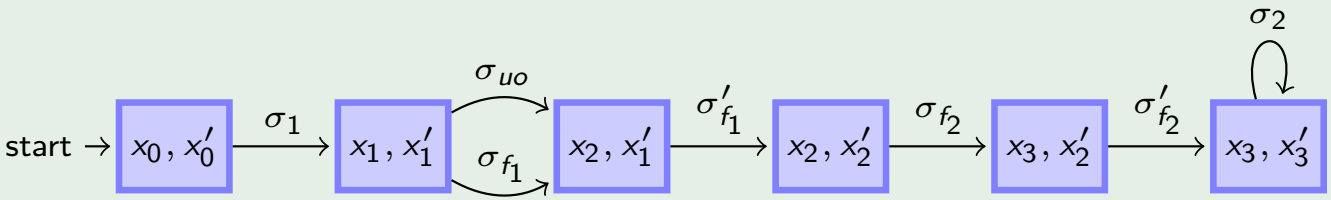


Une partie de $M||_{obs}M'$



À vous de jouer

Exemple

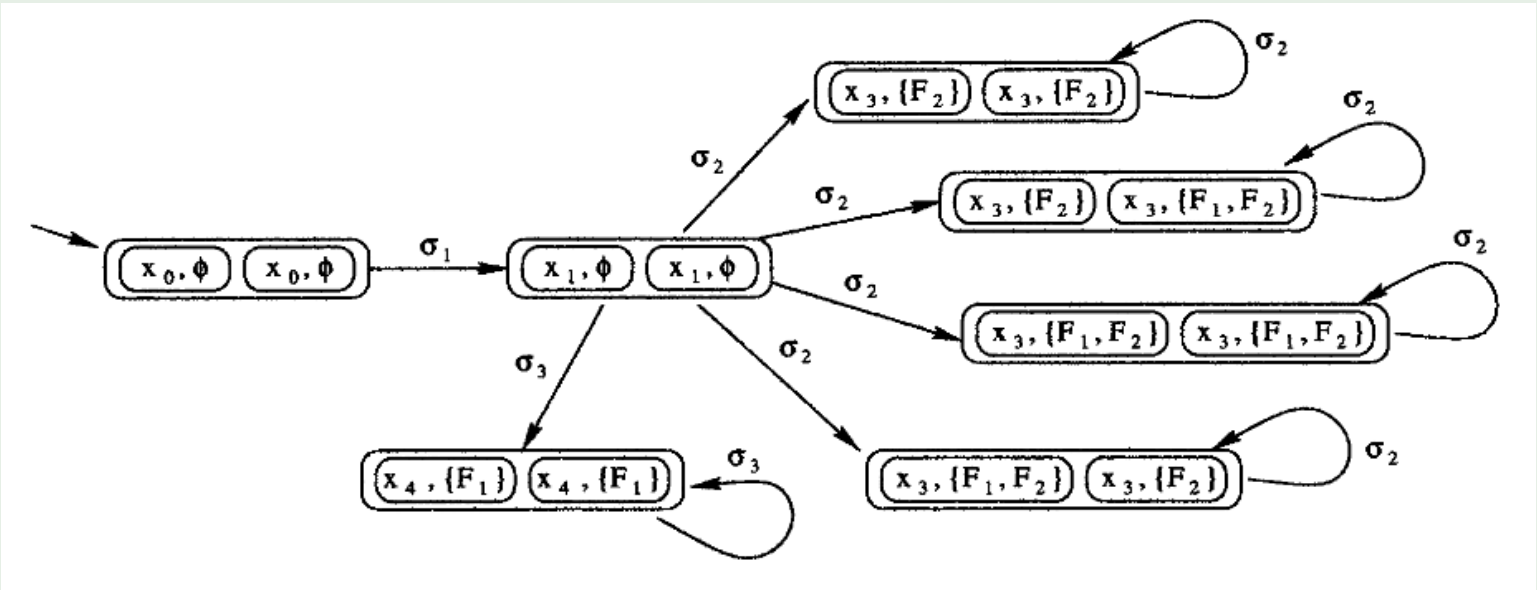


Questions : y-a-t-il un couple critique de σ_{f_1} ? de σ_{f_2} ?

Exemple

Exemple

Modèle des jumeaux (les événements non-observables sont abstraits)

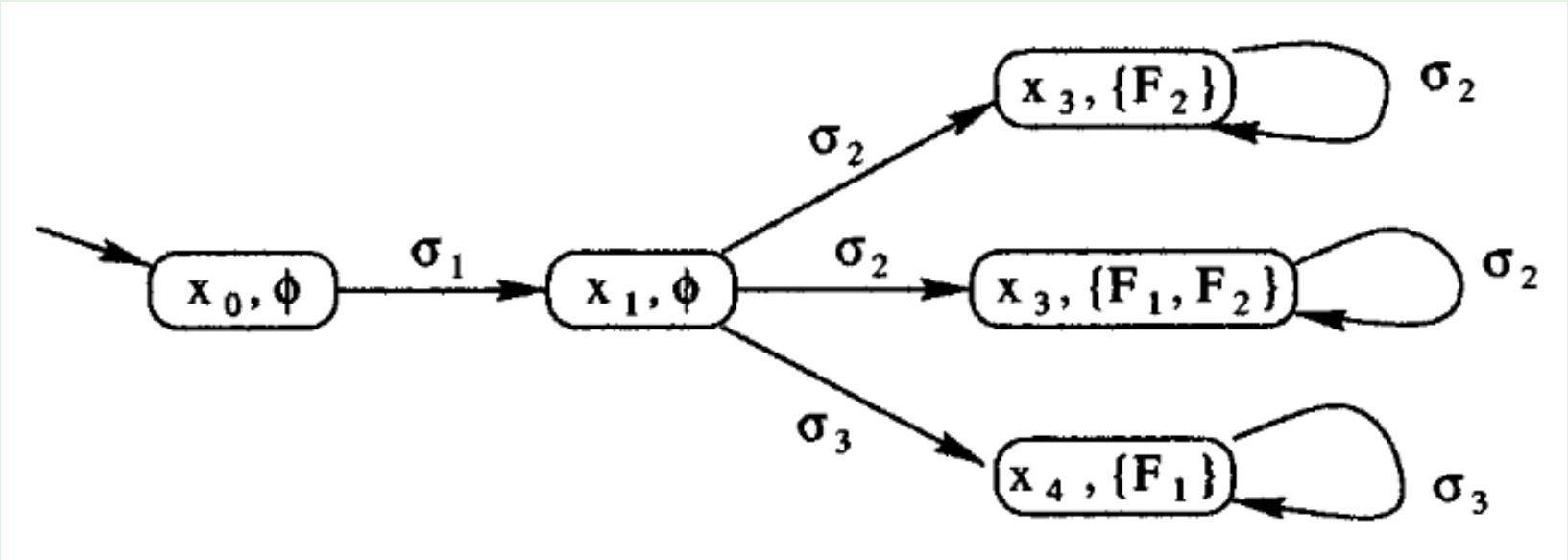


Diagnosticabilité de $F1$ et $F2$??

Exemple

Exemple

Diagnostiqueur



Diagnosticabilité de $F1$ et $F2$??

Un peu de complexité algorithmique

- Soit N le nombre d'états du modèle global
- Au pire, le nombre d'états dans le produit des jumeaux est N^2
- Algorithme de diagnosticabilité au pire : calcul exhautif des jumeaux
  - Algorithme polynomial en N, algorithme en $O(N^2)$
- Rappel : approche diagnostiqueur
  - Algorithme polynomial en N, algorithme en $O(2^N)$
- La méthodes des jumeaux est bien plus efficace
- MAIS les jumeaux sont toujours en $O(2^{2n})$ avec n le nombre de composants

Résumé de l'approche

- Recherche de couples critiques
- Composition parallèle d'un modèle global avec lui-même
- Bien meilleur que l'approche diagnostiqueur
- Mais c'est toujours une méthode centralisée

Plan du cours

Analyse décentralisée : Principe

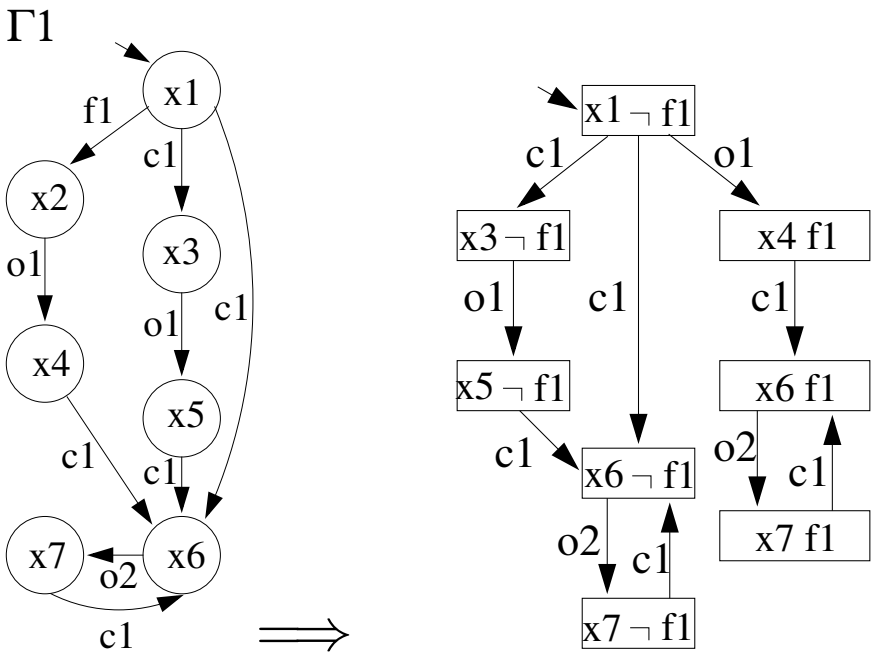
- Analyse “locale” de la diagnosticabilité
- Analyse sur un composant seul (et non pas sur le système)
  - Notion de diagnosticabilité locale
- Si l’analyse n’est pas concluante,
  - Analyse hiérarchique de la diagnosticabilité locale sur le composant et son voisinage jusqu’à ce qu’on puisse décider

Diagnosticabilté locale

- F est localement diagnosticable ssi :
  - il existe un nombre fini p d'observations issues de sous-système après l'occurrence de F qui permet de décider avec certitude que F a eu lieu.
- Propriété :
  - (Pas de famine d'observations) $\wedge$ (F localement diagnosticable) $\Rightarrow$ (F diagnosticable)
- Objectif : trouver un sous-système dans lequel F est localement diagnosticable
  - Utilisation de diagnostiqueurs locaux et d'analyseurs locaux

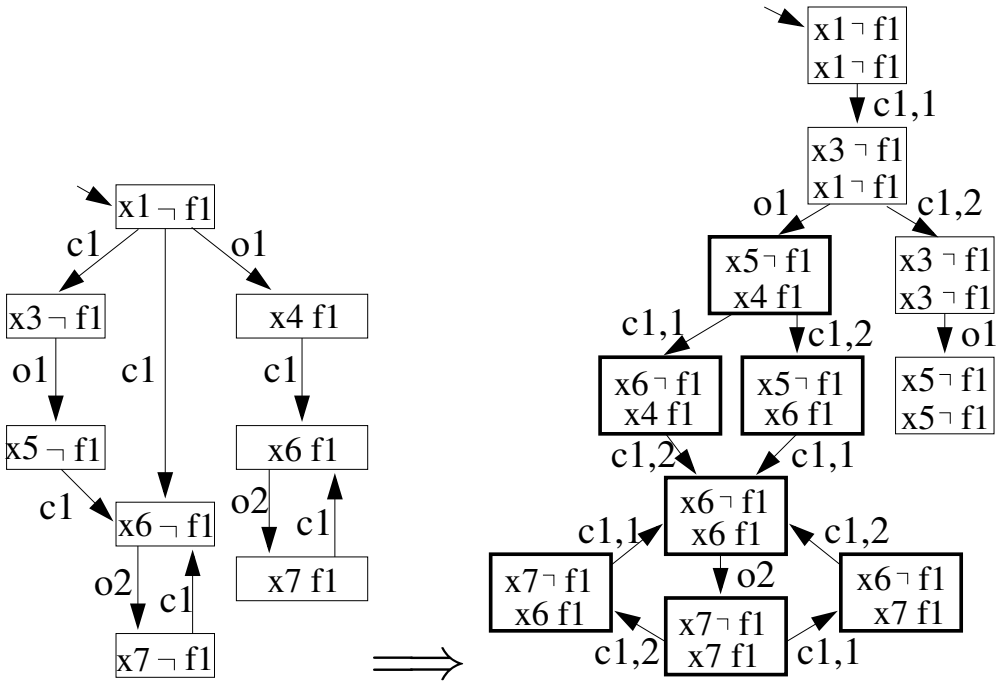
Diagnostiqueur local

- Fondé sur un composant et sur l'anlyse d'un événement F
- Etat : état du composant et son diagnostic
- Label de transitions : événmenent observable ou communicants
- Suit le comportement observable et interactif du composant



Analyseur local

- Synchronisation de deux diagnostiqueurs locaux sur les événements observables
- Un chemin de transition représente deux exécutions différentes d'un même composant produisant le même séquence observable.



Détection de l'ambiguité

- Dans un analyseur, un état est *ambigu* si les parties gauche et droite sont en désaccord.
  - $(x3, \{\}), (x1, \{\})$ n'est pas ambigu
  - $(x5, \{\}), (x6, \{f1\})$ est ambigu
- Dans un analyseur local, si il y a un cycle contenant des états ambigus et au moins une transition observable, la faute f_1 n'est pas diagnosticable dans Γ_1
- Dans l'analyseur local s'il existe un chemin infini d'événements observables (pas d'événements communicants) avec un ensemble infini d'états ambigus, la faute n'est pas diagnosticable dans le système

Analyseur d'un sous-système

- Sous-système : sous-ensemble de composants du système
- Fusion "intelligente" des analyseurs locaux aux composants du sous-système
  1. Synchronisation sur les événements de communications (gauche avec gauche, droite avec droite)
  2. Suppression des parties non-ambiguës du résultat de la synchronisation
  3. Suppression des événements de communications validées (communications internes au sous-système)
  4. Stratégie de fusion
     - On utilise la même stratégie que pour le diagnostic décentralisé
     - Fusion des analyseurs interagissants
  5. Détection de l'ambiguité : idem à celle effectuée dans l'analyseur local

Principe de l'algorithme

Cas 1 Pas de cycle d'états ambigus dans l'analyseur de F local à un sous-système γ

- F est localement diagnosticable. STOP

Cas 2 Présence de cycles d'états ambigus dans l'analyseur

Cas 1 Il existe des événements de communications dans un cycle

- Pas bon, il faut vérifier leur validité par fusion avec un autre analyseur.

Cas 2 Un cycle ne contient que des observations (pas de communication)

- F n'est pas diagnosticable. STOP

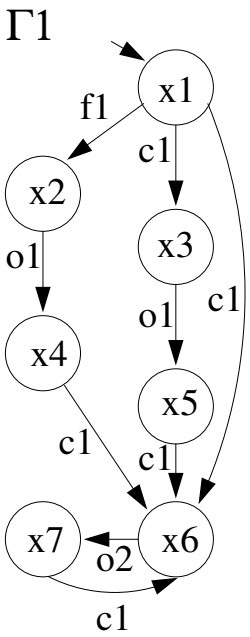
Sortie

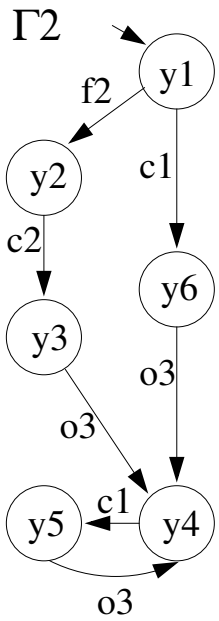
- Oui, F est diagnosticable ou
- Non, F n'est pas diagnosticable. Les cylces détectés fournissent un langage ambigu

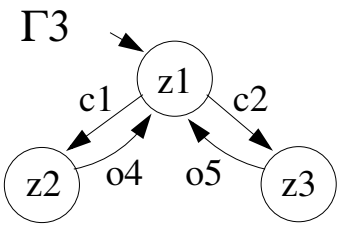
Langage ambigu

- Langage observable L produit par un sous-système
- Chaque séquence observée σ de ce sous-système appartenant à L est tel que l'occurrence de F est ambigu.
- Pour tout système non diagnosticable, il existe au moins un sous-système qui peut produire un langage ambigu infini.

Un petit exemple







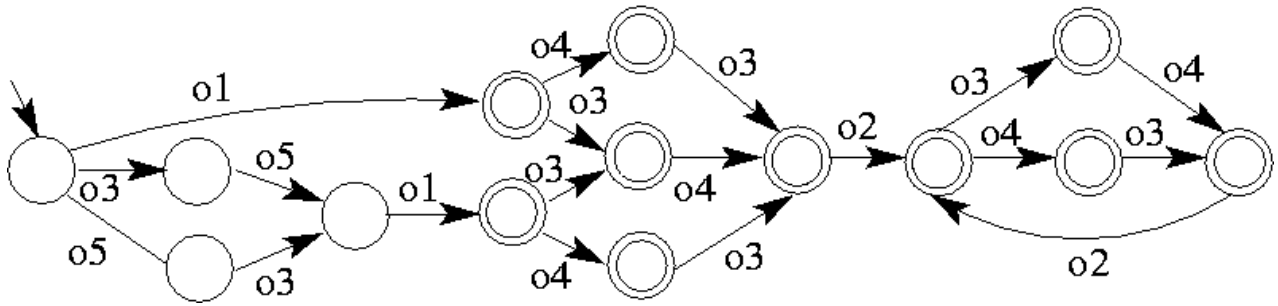
- f1 est-il diagnosticable ?
- f2 est-il diagnosticable ?

Diagnosticabilité de f2

1. L'analyseur local contient des cycles d'états ambigus Le composant $\Gamma 2$ n'a qu'un type d'observation (o3).
   - f2 n'est pas diagnosticable sur $\Gamma 2$.
2. Après fusion avec l'analyseur de $\Gamma 3$, le résultat ne contient plus de cycles.
   - f2 est diagnosticable. La présence de f2 est diagnostiquée grâce à l'observation $o5$ issu de $\Gamma 3$
3. f2 est localement diagnosticable dans le sous-système $\{\Gamma 2, \Gamma 3\}$

Exemple : Ambiguïté liée à f1

- f1 n'est pas diagnosticable
- L'analyseur contient des cycles d'états ambigus
- Après la fusion de tous les analyseurs, on obtient un langage d'observations ambiguës :



Résumé de cette approche

- Cadre de l'analyse décentralisé de la diagnosticabilité dans les SED
- Fondé sur la notion de diagnosticabilité locale
  - Fusion "intelligente" et successive d'analyseurs locaux
- Pas besoin de modèle global
- Fourni en résultat un langage observable ambigu

Diagnosticabilité : une simple vérification de modèle ?

- Dans la litérature classique : oui
  - Problème de répondre oui ou non à la question : **le système est-il diagnosticable ?**
  - On peut utiliser des vérificateurs de modèles génériques
- En pratique, les systèmes sont rarement diagnosticables
  - D'où une meilleure question : **pourquoi le système n'est pas diagnosticable ?**
  - Recherche des raisons (scénarios non-diagnosticables, couples critiques) le plus localement possibles
- Finalité de cette analyse :
  - Synthétiser des recommandations pour le retour sur conception
  - Placement de capteurs aux bons endroits pour améliorer la diagnosticabilité
  - Un capteur = un coût supplémentaire $\Rightarrow$ Diagnosticabilité $\equiv$ Problème d'optimisation des coûts