INSTITUT NATIONAL POLYTECHNIQUE DE LORRAINE
UNIVERSITE HENRI POINCARE - NANCY I

Surveillance des processus

Didier Maquin
Professeur à l'INPL

$3^{ème}$ année ENSEM
et
Diplôme d'Etudes Approfondies
Contrôle, Signaux et Communications

Vandœuvre-les-Nancy, février 2003

1 Théorie logique du diagnostic

1.1 Introduction

L'idée de s'appuyer sur des modèles pour réaliser un diagnostic de fonctionnement s'est développée parrallèlement dans deux communautés différentes. La première est celle des automaticiens et les travaux qui ont été développés sont relatés dans les paragraphes qui précèdent. La seconde est celle des chercheurs en Intelligence Artificielle. Pour cette communauté, le terme "modèle" est employé par opposition aux connaissances associationnistes[1]. Les connaisances incluses dans ces modèles décrivent la *structure* du système à diagnostiquer (connexions entre les *composants*) et son comportement (obtenu par composition à partir des comportements des différents composants du système). Ces connaissances structurelles sont en général exprimées sous la forme de contraintes entre les variables physiques. L'idée fondamentale, pour effectuer un diagnostic, est la même que celle qui a déjà été utilisée précédemment ; il s'agit de comparer le comportement réel du système tel qu'il peut être observé par l'intermédiaire de capteurs et son comportement attendu tel qu'il peut être prédit grâce aux *modèles de bon comportement*. Si ces modèles sont corrects, en ce sens qu'ils sont effectivement vérifiés par un système en bon fonctionnement, toute contradiction entre les *observations* et les *prédictions* déduites des modèles est nécessairement la manifestation d'un dysfonctionnement, c'est-à-dire de la présence d'un ou plusieurs défauts. Ce type de raisonnement par l'absurde, où un défaut est, par définition, n'importe quoi d'autre que le comportement attendu s'avère être une méthode très puissante et qui est logiquement fondée : la détection de dysfonctionnement par réfutation du bon comportement prédit est un raisonnement logiquement correct contrairement à la détection de dysfonctionnement par corroboration avec un mauvais comportement prédit.

Les contradictions entre observations et prédictions ne se contentent pas de manifester la présence de défauts (détection) mais renseignent aussi sur la localisation de ces défauts. Il suffit pour cela d'utiliser les prédictions préalablement enregistrées qui mènent aux contradictions en question : si une prédiction a été faite en utilisant les modèles de bon comportement de composants $C_1, \ldots, C_n$, et qu'elle est en contradiction avec une observation, c'est donc (raisonnement par l'absurde) que les composants $C_1, \ldots, C_n$ ne peuvent être tous correct et que l'un deux est nécessairement défectueux ; on dit que ces composants forment un *conflit*. Plus on effectue d'observations, plus on a de chances d'obtenir des contradictions avec les prédictions, donc de générer de nouveaux conflits. En recoupant ces conflits, on affine progressivement la localisation du ou des défauts.

La détection de conflits constitue la première phase du diagnostic. La seconde phase consiste à engendrer des hypothèses (sur les *modes* de fonctionnement des composants) qui rendent compte de tous les conflits, c'est-à-dire de toutes les contradictions détectées. Logiquement, cela signifie le changement d'hypothèses de fonctionnement correct de certains composants en une hypothèse de dysfonctionnement, de manière à ce que toutes les contradictions disparaissent c'est-à-dire qu'il n'y ait plus de conflit. Un ensemble de composants qui, cessant d'être supposés corrects, rétablit la cohérence avec les observations est précisément appelé un *diagnostic*.

[1] Les connaissances associationnistes sont issues d'une expertise relative aux relations entre symptômes observés et causes de dysfonctionnement ; cette connaissance heuristique est le plus souvent codée sous la forme de règles associant les causes aux symptômes

1.2 Cadre théorique et exemple traité

Le cadre théorique global du diagnostic logique a été initialement établi par Reiter (1987) puis a été repris pour être généralisé par De Kleer (1992). De façon à faciliter la lecture, nous avons choisi d'énoncer des définitions et de les illuster immédiatement par l'utilisation d'un exemple[2]. Celui-ci est constitué de cinq composants élémentaires, trois "multiplicateurs" et deux "additionneurs" interconnectés de la manière suivante :

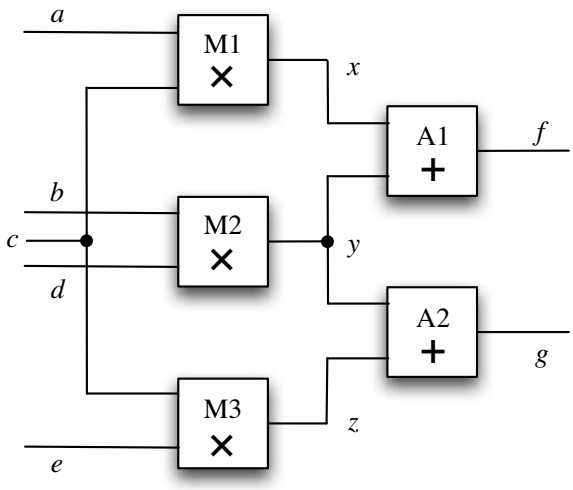

FIG. 1 – Polybox example

Le choix de ce système élémentaire et l'hypothèse que le système fonctionne dans un environnement idéal, non perturbé et non bruité ont été retenus volontairement pour se focaliser sur les principales caractéristiques du diagnostic logique, sans être gêné par les détails de la modélisation ou par les critères de détection. Cette approche permet cependant de traiter des systèmes continus et dynamiques en utilisant des modèles différentiels ou récurrents.

Définition : un *système* est une paire (DS, COMPS) où DS, la description du système, est un ensemble de formules de la logique des prédicats du premier ordre avec égalité et où COMPS, les composants du système, est un ensemble fini de constantes.

Définition : un *ensemble d'observations* OBS est un ensemble de formules du premier ordre avec égalité.

Les éléments de COMPS, qui sont les objets du diagnostic, figurent dans DS et éventuellement dans OBS. Si, par exemple, un capteur peut être défaillant, c'est-à-dire s'il peut faire l'objet d'un diagnostic, il sera déclaré comme composant. L'ensemble DS inclut un prédicat unaire noté AN qui signifie *anormal*. Pour un composant c particulier de COMPS, ¬AN(c) signifie que le composant c fonctionne correctement. On remarquera que les formules de DS décrivent généralement le comportement normal des composants.

[2]Cet exemple classique dû à De Kleer et Williams (1987), est connu sous le nom de "polybox example" dans la littérature internationale

Exemple – Pour le système de la figure 1, on a :

```
COMPS = /* composants
        (A1, A2, M1, M2, M3).

DS = {  /* modèles de bon comportement des composants
        ADD(x) ∧ ¬AN(x) ⇒ sortie(x) = entrée1(x) + entrée2(x),
        MULT(x) ∧ ¬AN(x) ⇒ sortie(x) = entrée1(x) × entrée2(x),

        /* instanciation des composants
        ADD(A1), ADD(A2), MULT(M1), MULT(M2), MULT(M3),

        /* connexions
        sortie(M1) = entrée1(A1),
        sortie(M2) = entrée2(A1),
        sortie(M2) = entrée1(A2),
        sortie(M3) = entrée2(A2),
        entrée2(M1) = entrée1(M3)
        }.

OBS = { /* valeurs des mesures
        entrée1(M1) = 2, entrée2(M1) = 3,
        entrée1(M2) = 2, entrée2(M2) = 3,
        entrée2(M3) = 2,
        sortie(A1) = 10, sortie(A2) = 12
        }.
```

Définition : un *système observé* est un triplet (DS, COMPS, OBS) où (DS, COMPS) est un système et OBS un ensemble d'observations.

Pour $\Delta \subseteq$ COMPS, notons D(Δ)=$\{$AN(c) | c $\in \Delta\} \cup \{\neg$ AN(c) | c $\in$ COMPS $\setminus \Delta\}$.

Définition : un *diagnostic* pour un système observé (DS, COMPS, OBS) est un ensemble de composants $\Delta \subseteq$ COMPS tel que DS $\cup$ COMPS $\cup$ {D(Δ)} est satisfiable (ou consistante).

En effet, un système fonctionnant correctement est défini par $\alpha :=$ DS $\cup \{\neg$AN(c) | c $\in$ COMPS$\}$. Le système est en défaut si les observations et les valeurs prédites par le modèle sont en désaccord, c'est-à-dire $\alpha \cup$ OBS non satisfiable (ou inconsistante). Elaborer un diagnostic revient à retirer certaines hypothèses $\neg$AN(C_1), ..., $\neg$AN(C_n) (fonctionnement correct de composants) de manière à rendre consistante la relation précédente.

Lorsqu'aucune confusion n'est possible, on identifiera le diagnostic D(Δ), qui est une conjonction, avec Δ qui est un ensemble de composants. Comme il y a potentiellement $2^{|COMPS|}$ diagnostics possibles, on est conduit à appliquer un principe de parcimonie fondé sur la notion de diagnostic minimal.

Définition : un *diagnostic minimal* est un diagnostic D(Δ) tel que $\forall \Delta' \subset \Delta$, D($\Delta'$) n'est plus un diagnostic.

Un diagnostic pour un système observé (DS, COMPS, OBS) existe si et seulement si DS $\cup$ OBS est satisfiable, ce que l'on supposera toujours par la suite. L'ensemble vide $\emptyset$ est un diagnostic pour (DS, COMPS, OBS) si et seulement si DS $\cup$ OBS $\cup \{\neg$AN(c) | c $\in$ COMPS$\}$ est satisfiable, c'est-à-dire si et seulement si les observations sont compatibles

avec un fonctionnement correct de tous les composants. Tant que $\emptyset$ est un diagnostic, il n'y a aucune raison de suspecter une faute dans le système.

Exemple – Pour le système de la figure 1, en mettant en œuvre un simulateur, on peut obtenir :

$\neg$AN(M1) $\Rightarrow$ sortie(M1) = 6
$\neg$AN(M2) $\Rightarrow$ sortie(M2) = 6
$\neg$AN(M3) $\Rightarrow$ sortie(M3) = 6
$\neg$AN(M1) $\wedge$ $\neg$AN(M2) $\wedge$ $\neg$AN(A1) $\Rightarrow$ sortie(A1) = 12
$\neg$AN(M2) $\wedge$ $\neg$AN(M3) $\wedge$ $\neg$AN(A2) $\Rightarrow$ sortie(A2) = 12

Définition : un *R-conflit*[3] pour un système observé (DS, COMPS, OBS) est un ensemble de composants C $\subseteq$ COMPS tel que DS $\cup$ OBS $\cup$ $\{\neg$AN(c) | c $\in$ C$\}$ n'est pas satisfiable. Un *R-conflit minimal* est un conflit n'incluant aucun autre R-conflit (minimalité de l'inclusion ensembliste des R-conflits).

Un R-conflit peut être interprété de la manière suivante : l'un au moins des composants du R-conflit est en défaut.

Exemple – Considérons dans un premier temps l'observation de la sortie de l'additionneur A1 (sortie(A1) = 10). Cette observation n'est pas cohérente avec la prédiction du modèle. La valeur de cette sortie ne peut être expliquée que si l'un au moins des composants M1, M2 ou A1 est en défaut. On conclut que {M1, M2, A1} constitue un R-conflit minimal. Considérons maintenant l'observation de la sortie de l'additionneur A2 (sortie(A2) = 12). Celle-ci est en accord avec la prédiction faite par le modèle. Cependant, compte-tenu de la symétrie du montage étudié, cette observation met en évidence un autre R-conflit minimal. En effet, si les composants M1, A1, M3 et A2 fonctionnent correctement, on ne peut observer simultanément sortie(A1) = 10 et sortie(A2) = 12 (ces deux observations devraient être identiques quelque soit la valeur en sortie de M2). On en conclut que {M1, A1, M3, A2} forme un second R-conflit minimal. Pour ce jeu d'observations, on peut montrer que ce sont les deux seuls R-conflits possibles. La démarche exposée peut être systématisée ; on trouvera en annexe quelques éléments permettant d'obtenir ces résultats.

L'analyse de ces R-conflits minimaux permet d'engendrer tous les diagnostics minimaux d'un système observé. Cette analyse s'appuie sur la notion d'"ensemble échantillon" (traduction libre du vocable anglo-saxon *hitting set*).

Définition : considérons un ensemble de R-conflits minimaux $\mathcal{C}$ alors H $\subseteq$ COMPS est un *ensemble échantillon* si et seulement si $\forall$ c $\in \mathcal{C}$, c $\cap$ H $\neq \emptyset$. un ensemble échantillon est minimal s'il n'inclut aucun autre ensemble échantillon.

Proposition : l'ensemble Δ est un diagnostic minimal pour le système observé (DS, COMPS, OBS) si et seulement si Δ est un ensemble échantillon minimal de l'ensemble des R-conflits minimaux du système (DS, COMPS, OBS).

Exemple – A partir des deux R-conflits minimaux {M1, M2, A1} et {M1, A1, M3, A2}, on peut engendrer les quatre diagnostics minimaux suivants : {A1}, {M1}, {A2, M2} et {M2, M3}. Cela signifie que les observations effectuées peuvent être expliquées par deux

[3]Cette dénomination provient des travaux de Reiter, on définit là un conflit au sens de Reiter

situations de défaut simple {A1} ou {M1} et deux situations de défauts doubles {A2, M2} ou {M2, M3}

Considérons maintenant quatre jeux d'observations distincts des sorties du système :

	OBS0	OBS1	OBS2	OBS3
sortie(A1)	12	10	10	10
sortie(A2)	12	12	10	14

En utilisant la procédure précédemment décrite, le lecteur pourra vérifier que l'on peut établir, pour chaque situation, les R-conflits minimaux suivants :

	R-conflits minimaux
OBS0	$\emptyset$
OBS1	{A1, M1, M2}, {A1, A2, M1, M3}
OBS2	{A1, M1, M2}, {A2, M2, M3}
OBS3	{A1, M1, M2}, {A2, M2, M3}, {A1, A2, M1, M3}

On peut alors facilement en déduire les diagnostic minimaux correspondants :

	Diagnostics minimaux
OBS0	$\emptyset$
OBS1	{A1}, {M1}, {A2, M2}, {M2, M3}
OBS2	{M2}, {A1, A2}, {A1, M3}, {A2, M1}, {M1, M3}
OBS3	{A1, A2}, {A1, M2}, {A1, M3}, {A2, M1} {A2, M2}, {M1, M2}, {M1, M3}, {M2, M3}

1.3 Retour sur les méthodes de redondance analytique

Les techniques relatives aux méthodes de redondance analytique peuvent être décrites dans un cadre formel proche de celui employé pour l'approche diagnostic logique.

Un *système* est un ensemble interconnecté de composants. Chaque *composant* est décrit par un modèle comportemental défini par un ensemble de contraintes statiques ou dynamiques liant ses variables d'entrée et de sortie.

Définition : le *modèle comportemental* (MC) d'un système est constitué de l'ensemble des contraintes décrivant le comportement de ses composants ainsi que de la structure qui décrit les liens entre les composants.

Définition : le *modèle d'observation* (MO) énumère le sous-ensemble des variables observées sur le système.

Définition : le *modèle du système* (MS) est défini par la paire (MC, MO).

Définition : une *relation de redondance analytique* (RRA) est une relation issue de MS ne faisant intervenir que des variables observées ; on la note généralement $\omega(\text{OBS}) = 0$.

Cela signifie qu'en fonctionnement normal, les mesures satisfont les relations de redondance analytique. En présence de défauts, elles ne sont plus satisfaites et l'on a $\omega(\text{OBS}) = r \neq 0$; r est appelé *résidu*. Les RRA sont obtenues à partir de MS en

éliminant les variables inconnues. Cette élimination peut être formalisée dans différents cadres théoriques et en particulier celui de la théorie des graphes.

Exemple – Pour le système de la figure 1, on a :

MC := {M1 : $x = a \times c$, M2 : $y = b \times d$, M3 : $z = c \times e$, A1 : $f = x + y$, A2 : $g = y + z$ }

MO := {Ma : $a = a_{obs}$, Mb : $b = b_{obs}$, Mc : $c = c_{obs}$, Md : $d = d_{obs}$, Me : $e = e_{obs}$, Mf : $f = f_{obs}$, Mg : $g = g_{obs}$}

OBS := {$a_{obs} = 2$, $b_{obs} = 2$, $c_{obs} = 3$, $d_{obs} = 3$, $e_{obs} = 2$, $f_{obs} = 10$, $g_{obs} = 12$}

L'élimination des variables inconnues x et y dans A1 et y et z dans A2 conduit aux relations de redondance analytique :

$$\mathrm{RRA}_1 := f - (a \times c) - (b \times d) = 0$$

$$\mathrm{RRA}_2 := g - (b \times d) - (c \times e) = 0$$

On observe que l'on peut également facilement éliminer la variable $y = b \times d$ entre A1 et A2 ou RRA_1 et RRA_2 ; on obtient une troisième relation de redondance analytique :

$$\mathrm{RRA}_3 := f - g - c \times (a - e) = 0$$

Définition : la *structure* d'une relation de redondance analytique est la liste minimale des contraintes devant être satisfaites pour que celle-ci le soit également.

Chaque contrainte étant associée à un composant, la structure d'une RRA sera notée en utilisant l'ensemble des composants correspondants. Par exemple, la structure de RRA_1 est {A1, M1, M2}, celle de RRA_2, {A2, M2, M3} et celle de RRA_3, {A1, A2, M1, M3}. Bien que RRA_3 soit issue d'une combinaison linéaire de RRA_1 et RRA_2, on remarquera que sa structure n'est pas constituée de l'union des structures de RRA_1 et RRA_2.

Définition : étant donné un ensemble R = {RRA_1, …, RRA_n} de n RRA et un ensemble F = {F_1,…, F_m} de m défauts, la signature du défaut F_j est donnée par le vecteur binaire $\mathrm{FS}_j = (s_{1j}, \ldots, s_{nj})^T$ dans lequel s_{ij} est donné par : (RRA_j, F_j) $\rightarrow s_{ij} = 1$ si des composants impliqués dans F_j sont impliqués dans RRA_i ; sinon $s_{ij} = 0$.

Si l'on a $s_{ij} = 0$, c'est que l'occurrence du défaut F_j n'affecte pas RRA_i, c'est-à-dire $r_i = 0$.

Définition : étant donné un ensemble R de n RRA, les signatures de l'ensemble F des m défauts, prises ensemble constituent ce que l'on appelle la matrice de signatures des défauts.

Exemple – Pour l'exemple considéré, la matrice de signature des défauts (simples) s'écrit :

	F_{M1}	F_{M2}	F_{M3}	F_{A1}	F_{A2}
RRA_1	1	1	0	1	0
RRA_2	0	1	1	0	1
RRA_3	1	0	1	1	1

Le cas des défauts multiples peut être traité en augmentant le nombre de colonnes de la matrice de signature, menant à un nombre total de colonnes égal à $2m-1$ où m est le nombre de défauts simples, si tous les défauts multiples possibles sont considérés. Soit F_j un défaut multiple correspondant à l'occurrence de k défauts simples F_{j1}, ... , F_{jk}, alors le vecteur signature de F_j est donné par :

$s_{ij} = 0$ si $s_{i(j1)} = \ldots = s_{i(jk)} = 0$

$s_{ij} = 1$ si $\exists\, l, 1 \leq l \leq k$, tel que $s_{i(jl)} = 1$

Exemple – Par extension de la matrice ci-dessus, les 26 colonnes additionnelles ont une signature égale à $(1, 1, 1)^T$ sauf pour $\mathrm{F}_{A1,M1}$ qui a $(1, 0, 1)^T$ pour signature et $\mathrm{F}_{A2,M3}$ qui a $(0, 1, 1)^T$ pour signature.

Les ensembles de diagnostic dans l'approche FDI sont donnés en termes de défauts présents dans la matrice de signature. La génération des ensembles de diagnostic est basée sur une interprétation des colonnes de la matrice de signature et consiste à comparer la signature des observations avec celles des défauts. Cette comparaison est traitée comme un problème de décision statistique.

Définition : la signature d'une observation OBS est un vecteur binaire

$\mathrm{OS} = (\mathrm{OS}_1, \ldots, \mathrm{OS}_n)^T$ où $\mathrm{OS}_i = 0$ si et seulement si $r_i = 0$.

La première étape (tâche de détection) est de construire la signature des observations, *i.e.* de décider si la valeur d'un résidu est nulle ou non, en présence de bruit et de perturbations. Ce problème a été largement étudié en FDI. Il est généralement abordé comme un problème de décision statistique, en utilisant les modèles connus de bruit et de perturbations.

Exemple – Les signatures des différents jeux d'observations sont données dans le tableau ci-dessous :

Jeux d'observations	Vecteur signature
OBS0	$(0, 0, 0)^T$
OBS1	$(1, 0, 1)^T$
OBS2	$(1, 1, 0)^T$
OBS3	$(1, 1, 1)^T$

La seconde étape (tâche de localisation) consiste à comparer la signature des observations avec celle des défauts. Une solution au problème de décision est de définir un critère de cohérence.

Définition : une signature d'observation $\mathrm{OS} = (\mathrm{OS}_1, \ldots, \mathrm{OS}_n)^T$ est cohérente avec une signature de défaut $\mathrm{FS}_j = (s_{1j}, \ldots, s_{nj})^T$ si et seulement si $\mathrm{OS}_i = s_{ij}$ quel que soit i.

Définition : les ensembles de diagnostic sont donnés par les défauts dont la signature est cohérente avec la signature des observations.

Exemple – Les ensembles de diagnostic obtenus pour les signatures suivantes des observations sont :

Signatures d'observation	Ensembles de diagnostic
$(0, 0, 0)^T$	$\emptyset$
$(1, 0, 1)^T$	{A1}, {M1}, {A1, M1}
$(1, 1, 0)^T$	{M2}
$(1, 1, 1)^T$	tout défaut multiple sauf {A1, M1} et {A2, M3}

Pour permettre la prise en compte des erreurs de décision, l'approche FDI utilise généralement un critère de cohérence entre signatures résultant de la définition d'une distance plutôt que le critère d'égalité défini ci-dessus.

1.4 Comparaison des deux approches

Dans les deux approches, le diagnostic est déclenché quand des *divergences* apparaissent entre le comportement modélisé (correct) et les observations. Dans l'approche "redondance analytique", appelée ultérieurement FDI, les divergences proviennent des relations qui ne sont pas satisfaites par les observations. Dans l'approche "diagnostic logique", appelée par la suite DX, les divergences permettent l'identification de R-conflits qui correspondent à des ensembles de composants dont le bon fonctionnement implique une divergence. Un concept analogue peut être défini dans l'approche FDI.

Définition : le *support* d'une RRA est l'ensemble des composants impliqués dans celle-ci, c'est-à-dire les colonnes de la matrice de signatures qui possèdent un élément non nul sur la ligne correspondant à cette relation. Il est aussi appelé un *R-conflit potentiel*. Ce nom est justifié par le résultat suivant.

Proposition : soit OBS un ensemble d'observations. Il y a identité entre l'ensemble des R-conflits minimaux pour OBS et l'ensemble des R-conflits minimaux potentiels associés aux RRA qui ne sont pas satisfaites par OBS.

Ce résultat est une conséquence directe de la manière dont les RRA sont élaborées à partir des modèles des composants. La violation d'une RRA (non nullité – statistique – du résidu correspondant) incrimine au moins l'un des modèles de bon fonctionnement des composants ayant servi à son élaboration. On en déduit donc de manière évidente que le support de chaque RRA constitue bien un R-conflit potentiel au sens du diagnostic logique en ce sens que lorsque la RRA est effectivement non satisfaite, son support devient un R-conflit.

D'un point de vue calculatoire, la principale différence entre les deux approches réside dans le fait que pour l'approche redondance analytique, la plus grande partie du travail est faite hors ligne. Utilisant seulement la connaissance des variables observées, c'est-à-dire les positions des capteurs, la connaissance fournie par le modèle est compilée : les RRA sont obtenues par combinaison des contraintes du modèle et par élimination des variables non observées. La seule chose qui doit être faite en ligne, lorqu'un vecteur d'observation OBS est acquis, est de calculer la valeur de vérité de chaque RRA et de comparer la signature des observations obtenues avec celle des défauts. En termes de R-conflits, cela signifie que les R-conflits potentiels sont compilés et que, pour tout OBS, les R-conflits sont exactement les R-conflits potentiels qui sont les supports des RRA non satisfaites par OBS.

L'approche FDI utilise la matrice de signatures, croisant sur les lignes, les RRA et sur les colonnes, les ensembles de composants. On a montré au paragraphe 1.3 que, étant donnée une observation OBS, le diagnostic est obtenu en identifiant les colonnes identiques à une signature d'observation (ou les signatures les plus proches, en tenant compte d'une fonction distance)

Dans l'approche DX, comme vu au paragraphe 1.2, les diagnostics minimaux sont obtenus comme ensembles échantillons de la collection des R-conflits (établis à partir de OBS). De tels R-conflits peuvent être vus comme les supports des RRA qui ne sont pas satisfaites par OBS, c'est-à-dire en observant l'ensemble I des lignes correspondantes de la matrice de signatures. Un ensemble échantillon minimal de la collection des R-conflits est alors un ensemble minimal J de colonnes singletons (relatives à un seul composant), tel que chacune des lignes de I intercepte au moins une colonne de J (i.e. possède au-moins un élément non nul dans cette colonne). Il est donc naturel d'adopter cette structure de matrice comme la base formelle suivant laquelle on peut comparer les deux approches. On peut remarquer que chaque vecteur d'observation OBS divise l'ensemble R en deux sous-ensembles :

- Le sous-ensemble R_{faux} des RRA qui sont incohérentes, $\mathrm{R}_{faux} = \{\mathrm{RRA}_i / r_i \neq 0\}$
- Le sous-ensemble $\mathrm{R}_{vrai} = \mathrm{R} \setminus \mathrm{R}_{faux}$ des RRA qui sont cohérentes, *i.e.* $\mathrm{R}_{vrai} = \{\mathrm{RRA}_i / r_i = 0\}$.

OBS est donc décrit à travers sa signature OS qui est un vecteur colonne binaire défini par : $\forall i, i = 1..n$, $\mathrm{OS}_i = 1$ si $\mathrm{RRA}_i \in \mathrm{R}_{faux}$ et $\mathrm{OS}_i = 0$ si $\mathrm{RRA}_i \in \mathrm{R}_{vrai}$.

L'approche FDI compare les signatures des observations à celles des défauts alors que l'approche DX considère séparément chaque ligne correspondant à une RRA dans R_{faux}, isolant les R-conflits avant de rechercher une explication commune. Dans la suite, ces approches sont appelées respectivement approche colonne et approche ligne.

L'originalité et la puissance des deux approches FDI et DX proviennent du fait qu'elles sont basées uniquement sur le comportement normal des composants : aucun modèle de comportement défaillant n'est nécessaire. Néanmoins, différentes hypothèses concernant la manifestation des pannes au travers des observations sont adoptées par défaut par chaque approche, conduisant à différentes méthodes de calcul des diagnostics, ce qui explique les résultats différents obtenus sur l'exemple. Ces hypothèses concernent :

- les manifestations des pannes au travers des observations et
- le cas des pannes simultanées et leur interaction.

En plus du fait évident qu'une panne ne peut pas affecter une RRA dans laquelle elle n'est pas impliquée, qui est la forme directe du raisonnement dans l'approche DX, l'idée utilisée dans l'approche FDI est qu'une panne se manifeste nécessairement en affectant les RRA dans lesquelles elle est impliquée, les rendant non satisfaites par les vecteurs d'observations donnés. Il en résulte non seulement, comme dans DX, que chaque colonne impliquée dans une ligne non satisfaite est une panne candidate, mais aussi que chaque colonne impliquée dans une RRA satisfaite est implicitement disculpée (les lignes satisfaites sont donc ainsi utilisées dans le raisonnement). En fait, ce résultat n'est pas logiquement cohérent : il repose sur l'hypothèse d'exonération qui est implicitement faite dans l'approche FDI et qui doit être considérée explicitement si l'on veut comparer l'approche FDI avec l'approche DX.

Définition : (Hypothèse d'exonération) Un ensemble de composants défaillants montre nécessairement son comportement défectueux, *i.e.* rend chaque RRA dans laquelle il est impliqué non satisfaites par les OBS donnés. Ou bien, de manière équivalente, pour les vecteurs d'observations donnés, chaque ensemble de composants impliqué dans une RRA satisfaite est disculpé, *i.e.* chaque composant de son support est supposé fonctionner correctement.

On remarque que cette hypothèse d'exonération se compose de :

- une hypothèse d'exonération des pannes uniques (chaque composant individuel montre son comportement défectueux) et
- une hypothèse de non compensation (les effet individuels des composants défaillants ne se compensent jamais les uns les autres).

Exemple – Pour OBS_1 dont la signature est $(1, 0, 1)^T$, l'approche FDI disculpe les composants (considère qu'ils fonctionnent correctement) A2, M2 et M3 conduisant aux seuls ensembles de diagnostic {A1}, {M1}, {A1, M1}. Pour OBS_2, de signature $(1, 1, 0)^T$, elle disculpe A1, A2, M1 et M3 et le seul diagnostic possible est {M2}.

En fait, ce résultat n'est pas fondé d'un point de vue logique (l'hypothèse sous-jacente est relative à la détectabilité des défauts : le ou les défauts recherchés ont-ils une amplitude suffisante pour "sensibiliser" tous les relations au sein desquelles ils interviennent ?). Cependant, l'hypothèse d'exonération, implicite dans l'approche FDI, se justifie en termes de propriétés structurelles.

On pourra remarquer que pour l'exemple considéré, quelque soit le jeu d'observations, les diagnostics relatifs à la présence d'un défaut unique sont identiques pour les deux approches (l'hypothèse d'exonération est licite dans ce cas).

Dans l'approche DX, il n'y a aucune limitation sur le nombre de fautes simultanées (pour expliquer un dysfonctionnement). Les diagnostics minimaux sont construits de manière systématique comme ensembles échantillons de la collection des R-conflits sans aucune limitation sur le nombre de composants impliqués. A ce titre, il n'y a aucune différence de traitement relative au traitement de défauts multiples par rapport aux défauts simples. Il est donc admis que plusieurs défauts peuvent se compenser conduisant à la satisfaction de relations de redondance analytique au sein desquelles ces défauts sont impliqués.

Dans l'approche FDI, l'hypothèse de défaut unique est fréquemment posée. En effet, la probabilité d'apparition de fautes simultanées est souvent faible (et surtout ... cela simplifie le traitement !). Lorsque cette hypothèse ne peut être retenue, l'approche FDI nécessite l'élaboration des signatures de défauts multiples. Ces dernières sont obtenues à partir des signatures de défauts simples et selon l'idée intuitive qu'un défaut multiple peut affecter une relation de redondance si et seulement si au moins l'un des défaut le constituant peut affecter cette relation (voir en haut de la page 9). Implicitement, la construction de ces signatures s'effectue en supposons que les défauts sont détectables et qu'ils ne se compensent pas.

Exemple – Pour OBS_1 et OBS_2 toutes les situations de défauts doubles obtenues par l'approche DX sont rejetées par l'approche FDI à cause de l'hypothèse de non-compensation.

Une fois encore, l'approche FDI n'est pas *logiquement* correcte mais elle est justifiée du point de vue structurel (elle est valide pour *presque* tous les défauts sans tenir compte du cas très particulier de compensation totale qui est peu probable). Par exemple, pour OBS_2, les diagnostics $\{A2, M2\}$ et {M2, M3} correspondent respectivement aux cas exceptionnels de compensation produits par le fonctionnement suivant des composants : M2 : $2 \times 3 = 4$, A2 : $4 + 6 = 12$ et M2 : $2 \times 3 = 4$, M3 : $3 \times 2 = 8$.

1.5 Annexe

(à développer !)