Caractérisation des systèmes autoguérissants : diagnostiquer ce que l'on va réparer

Diagnose what you will repair : characterizing and checking self-healability

Marie-Odile Cordier[1] Yannick Pencolé[2] Louise Travé-Massuyès[2] Thierry Vidal[1]

[1] IRISA, INRIA/Université de Rennes 1
[2] LAAS-CNRS, Université de Toulouse

Résumé

Les systèmes complexes basés sur des architectures informatiques se doivent d'être capables "d'autoguérison", *c'est-à-dire capables, sans intervention extérieure, de détecter, diagnostiquer et réparer les effets de l'occurrence de fautes, pour continuer à assurer leurs fonctionnalités. Les concepteurs de tels systèmes ont besoin d'outils permettant de vérifier avant leur mise en œuvre opérationnelle qu'ils sont bien "autoguérissants". Mais auparavant, il est nécessaire de définir précisément et formellement ce qu'autoguérison signifie. La diagnosticabilité, qui est la capacité d'un système à déterminer l'état fautif dans lequel il se trouve à partir des observations dont il dispose, est une propriété bien connue, mais qui néglige les capacités de réparation de ces fautes. La réparabilité au contraire, vue comme la capacité d'un système à disposer de plans de réparation adaptés aux fautes, ne prend pas en compte les capacités de diagnostic. Notre article établit le lien entre ces deux propriétés, définissant la capacité d'autoguérison comme une combinaison de la diagnosticabilité, dont il nous a fallu étendre la définition classique, et de la réparabilité, dont nous proposons une première définition formelle. Nous suggérons à partir de là un algorithme de vérification pratique et des stratégies pour aider les concepteurs à rendre leur système autoguérissant.*

Mots Clef

Diagnostic, Réparation, Autoguérison, Agents autonomes, Systèmes à événements discrets

Abstract

Modern systems, such as web services, need to be self-healing, which means capable of surviving autonomously the occurrence of faults, still managing to provide the desired functionality. Designers of such systems need tools helping them to assess beforehands the self-healability of their system, but as a first step towards such tools, one needs to better define what self-healability precisely means in those applications. Diagnosability, which is the ability of a system to be self-aware about its current state by analysing the observations that are received, has been thoroughly defined, but it totally disregards repair capabilities. On the other hand, repairability considered as the ability of a system to react to faults by applying repair actions is useless if it disregards diagnosis. This paper goes further, defining self-healability as a joint property, which achieves a bridge between diagnosability, for which we had to extend the classical definition, and repairability, of which we provide a first formal definition ; we then propose a practical and tractable self-healability checking algorithm and suggest strategies to help designers building self-healing systems.

Keywords

Diagnosis, Repair, Self-healability, Autonomous agents, Discrete event systems

1 Introduction

Les systèmes dynamiques complexes, de plus en plus présents au sein des applications industrielles, se doivent de disposer d'un niveau élevé d'autonomie, y compris en présence d'états fautifs avérés. Ils doivent pouvoir connaître à tout instant leur état courant et être réactifs vis-à-vis des fautes, par l'application de plans de réparation susceptibles de les ramener à leur fonctionnement nominal. En d'autres termes, ces systèmes doivent être "autoguérissants"[1] [4].
De nombreuses applications illustrent ce besoin, de la robotique mobile à la surveillance de centrales énergétiques ; nous nous sommes plus particulièrement intéressés au développement des services web (notamment dans le cadre du projet européen WS-DIAMOND, voir [13] pour plus de détails), comme par exemple la réservation de voyages sur Internet : un ensemble de services distribués se coordonnent par l'intermédiaire de processus décrits à l'aide de diagrammes d'activités (*workflows*) prédéfinis, pour fournir à un utilisateur une réponse à sa requête. Qui plus est, des exigences en termes de qualité de service doivent généralement être satisfaites (par exemple le délai de réponse, ou le nombre de solutions testées). De tels systèmes sont clairement basés sur une approche de type "récupération"

[1] Traduction littérale du terme anglais *self-healing*.

des fautes (par opposition à la tolérance aux fautes) : lorsqu'une faute apparaît (par exemple une donnée est corrompue lors d'une communication, ou un service est temporairement inaccessible), une exception est émise et un plan de réparation (précompilé ou bien construit dynamiquement) est exécuté, censé ramener le système dans un état de fonctionnement normal. Ces plans utilisent des actions de base, du style *refaire l'activité "Louer voiture" avec comme nouveau paramètre "économique"*, ou *remplacer le service "Réservation de train" par le service "Réservation de bus"*. Il est crucial d'être capable de vérifier, dès la conception, que de tels services web sont sûrs, c'est-à-dire qu'ils sont autoguérissants. Pour cela, il convient d'analyser et définir précisément ce concept d'autoguérison dans les systèmes orientés récupération, de manière générique et formelle.

Concevoir des systèmes autoguérissants exige d'évaluer conjointement les deux propriétés connues sous les noms de diagnosticabilité et de réparabilité. La première définit la capacité d'un système à produire via ses moniteurs des "observables" distincts pour chaque situation fautive envisagée ; la seconde définit la capacité à sortir de telles situations fautives en choisissant parmi un ensemble d'actions correctrices connues. Pour autant ces deux propriétés sont généralement étudiées de manière indépendante. La communauté du diagnostic a pour sa part proposé une définition formelle de la diagnosticabilité [10] et développé différentes approches pour sa vérification. La réparabilité par contre a été beaucoup moins étudiée, les chercheurs du domaine du génie logiciel se tournant plus volontiers vers des approches de type contrôlabilité ou tolérance aux fautes, alors que le domaine de la planification a su modéliser des plans de réparation mais sans s'intéresser explicitement aux conditions formelles de leur applicabilité.

Une première approche naïve consiste, après avoir identifié l'ensemble de toutes les fautes possibles, à analyser séparément leur diagnosticabilité (les observables issus de fautes peuvent-ils toujours être rattachés à ces fautes sans ambiguïté ?), puis leur réparabilité (existe-t-il pour chaque faute, après chacune de ses occurrences possibles, au moins un plan d'actions capable de la réparer ?). Si les deux réponses sont positives, alors le système est autoguérissant. Mais il s'agit d'une exigence trop forte : la diagnosticabilité de chaque faute élémentaire n'est en effet pas nécessairement requise... Imaginons par exemple que nos observations permettent de toujours déterminer que l'une ou l'autre des fautes f_1 et f_2 a eu lieu, mais sans pour autant pouvoir les discriminer. Notre système n'est alors pas diagnosticable vis-à-vis des fautes élémentaires. Pourtant, si le plan de réparation r s'avère adapté pour réparer aussi bien f_1 que f_2, alors cela suffit pour assurer la capacité d'autoguérison ! Cet exemple illustre la nécessité de définitions conjointes de la diagnosticabilité, de la réparabilité, et de l'autoguérison. L'idée sous-jacente que nous allons exploiter dans cet article est d'identifier un ensemble de ce que nous appellerons des *macrofautes* (comme "f_1 ou f_2"), tel que ces macrofautes soient à la fois diagnosticables et réparables.

Notre travail montre qu'il convient tout d'abord de redéfinir le concept classique de diagnosticabilité : ce dernier ne se conçoit en effet que vis-à-vis de partitions des fautes élémentaires, alors que nous montrons qu'il peut être avantageux de le définir vis-à-vis d'ensembles de macrofautes susceptibles de se recouvrir, deux macrofautes pouvant contenir des fautes élémentaires communes. Pour la forme stricte de la capacité d'autoguérison, on vérifie qu'il existe au moins un ensemble de macrofautes qui peut être diagnostiqué avec certitude puis réparé. Cela étant, des formes affaiblies d'autoguérison peuvent également être proposées. La première, dénommée autoguérison *faible*, exige la réparabilité forte de l'ensemble des macrofautes mais autorise que ces dernières ne soient diagnosticables que pour un sous-ensemble des comportements possibles du système. La seconde propriété que nous appelons autoguérison *partielle* guarantit la diagnosticabilité et la réparabilité des macrofautes en toutes occasions mais pour un ensemble de macrofautes ne couvrant qu'un ensemble réduit de fautes élémentaires.

La section 2 commence par situer nos travaux dans le domaine, puis la section 3 pose un certain nombre de définitions préliminaires et d'hypothèses concernant les fautes, les observables et les actions correctrices. La section 4 se concentre alors sur la propriété d'autoguérison, partant d'une définition étendue de la diagnosticabilité et d'une première définition de la réparabilité. Il nous a alors semblé important de fournir dans la section 5 un algorithme pratique permettant de vérifier la capacité d'autoguérison en temps polynômial. Lorsqu'un système apparaît ne pas être autoguérissant, la section 6 propose d'abord de définir formellement les propriétés d'autoguérison faible et partielle, avant d'aborder de manière plus opérationnelle dans la section 7 les stratégies possibles pour aider un concepteur à identifier les causes et à trouver une solution adéquate pour rendre le système autoguérissant, soit en rajoutant des moniteurs pour disposer de plus d'événements observables, soit en diversifiant les plans de réparation à sa disposition. Une conclusion est donnée dans la section 8 à travers quelques perspectives d'extension et d'application concrète de notre travail.

2 État de l'art

Dans [4], les systèmes autoguérissants sont présentés comme un nouveau domaine de recherche en informatique, leur définition restant relativement générale, à savoir :

> *Un système est autoguérissant s'il a la capacité de percevoir ses propres dysfonctionnements et, sans intervention humaine, d'effectuer les ajustements nécessaires pour recouvrer son fonctionnement normal.*

Cette définition est liée à la notion plus générale encore de *fiabilité*. Un système est fiable (ou sûr) si sa capacité à

délivrer son service en permanence est garantie. L'autoguérison est aussi liée à la notion de *tolérance aux fautes* (ou encore *tolérance aux pannes*). Un système est dit tolérant aux fautes s'il demeure fonctionnel malgré certaines fautes de ses constituants.

Il existe différentes façons de garantir ce type de propriétés. La *contrôlabilité* des systèmes dynamiques proposée dans [8] est un moyen de modifier de façon proactive l'architecture d'un système lors de sa phase de spécification afin d'empêcher l'occurrence d'une faute irréversible. Une autre approche pour améliorer la tolérance aux fautes est d'utiliser pendant la phase opérationelle des mécanismes prédéfinis se déclenchant après l'occurrence d'une faute : ces approches dites *passives* s'appuient sur des mécanismes robustes de retour en bon fonctionnement qui détectent les potentiels écarts du système par rapport à son comportement nominal attendu (voir par exemple [3] dans le domaine des systèmes continus). En génie logiciel, [12] s'appuie sur la même idée en argumentant que la distinction entre un état de bonne et de mauvaise santé est parfois délicate et que l'objectif est plutôt de maintenir un état interne stable du système malgré les variations extérieures (principe de l'homéostasie[2]).

Dans les systèmes autoguérissants et contrairement à ce qui précède, les aspects de remise en état sont clairement mis en avant : la distinction entre les états de bonne et de mauvaise santé est très nette. Un tel système dispose de moyens de surveillance afin de (1) détecter quand il passe d'un mode nominal à un mode de faute, (2) diagnostiquer la situation et (3) choisir et exécuter une stratégie de réparation appropriée.

Ce principe peut être considéré comme une *approche active* dans la littérature sur les systèmes tolérants aux fautes. Cette approche peut néanmoins conduire, comme il est souligné dans [9], à l'intégration de modes de réparation dans le modèle global du système, ce qui rend les limites entre les deux approches plus ou moins floues.

Notre contribution est clairement positionnée sur l'autoguérison par l'adoption du point de vue *diagnostic/réparation*. Le modèle spécifiant les comportements du système (fautifs ou non) est clairement séparé des stratégies disponibles pour la remise en état nominal du système à partir d'un état fautif. Dans la communauté de la planification, la *révision de plans*, l'*adaptation de plan* ou encore les *techniques de replanification* sont des variations de la même idée : en cas de perturbation dans l'exécution courante d'un plan, le plan nominal est arrêté et une séquence alternative d'actions est exécutée, cette dernière étant soit précalculée (hors ligne) soit calculée en ligne. Dans cette optique, notre contribution est à rapprocher de travaux [15] dans lesquels des *plans alternatifs* ont été précalculés et intégrés dans l'espace d'états du système. Un module de surveillance est en charge de détecter les déviations du système et fait commuter vers un des plans alternatifs si nécessaire afin de remettre le système dans un état dans lequel le plan nominal peut redémarrer. Néanmoins ce type d'approches a généralement deux défauts :

– l'observabilité du système est supposée totale rendant ainsi l'activité de diagnostic triviale ;
– il n'y a pas d'analyse formelle d'une propriété qui garantirait qu'il existe toujours une exécution de plan, réparant avec succès le système, quelle que soit la faute.

Cet article traite de ces deux points. La suppression de l'hypothèse d'observabilité totale implique une analyse de la *diagnosticabilité* du système : cette notion couvre un ensemble de propriétés qui sont étudiées depuis des années par différentes communautés. Dans le cadre des systèmes à événements discrets (SED), les premières définitions ont été proposées par [10] et de nombreuses extensions ont suivi notamment pour aborder des motifs plus génériques [5]. La vérification de la diagnosticabilité est un problème complexe et plusieurs algorithmes existent [16, 1, 11, 7], l'un des objectifs de cette vérification étant de reboucler sur la conception du système, par l'ajout de capteurs [14], ou encore par la respécification de protocoles de communications entre composants du système [6].

Pour le second point, la garantie du succès d'une réparation requiert une définition formelle de la notion de *réparabilité* qui, à notre connaissance, n'a jamais été clairement établie. Finalement, notre objectif est de combiner la diagnosticabilité et la réparabilité afin d'établir les conditions nécessaires à l'autoguérison afin d'en extraire des recommandations pour la spécification de systèmes autoguérissants.

3 Préliminaires

Le cadre formel introduit dans cet article peut être utilisé dans le cas de systèmes à dynamique continue ou discrète (en adoptant le point de vue décrit dans [2]). Pour des raisons de clarté et de concision, cet article ne traite que des systèmes à événements discrets. Cette section définit les notions préliminaires qui sont utilisées ultérieurement.

3.1 Événements : Observations et Fautes

Un système à événements discrets évolue avec l'apparition d'événements de plusieurs types. On distingue les événements observables (ou observations) $\mathcal{O} = \{o_1, ..., o_{no}\}$ et les événements non observables $\mathcal{U} = \{u_1, ..., u_{nu}\}$. Un système est en mesure de produire un ensemble de séquences σ d'événements observables. σ est appelé un *observable* et l'ensemble est noté OBS.

L'ensemble des événements de faute (ou plus simplement fautes) *élémentaires*, qui conduisent à un état fautif du système, est noté $\mathcal{F} = \{f_1, \ldots, f_{nf}\}$, et toute faute est considérée comme non-observable $\mathcal{F} \subseteq \mathcal{U}$. Nous supposons dans cet article que le système ne peut pas subir de fautes multiples, et donc seule une faute au plus peut être présente dans le système à un instant donné, ou autrement dit, une faute ne peut apparaître que lorsque le système fonctionne correctement. Cet ensemble d'événements de faute va nous permettre de caractériser également les "comportements" correspondants, notre but étant de les discriminer.

[2] Traduction littérale de *homeostasis*.

Nous devons alors par souci de généricité inclure le comportement normal, noté ok : c'est pourquoi nous étendons par convention l'ensemble $\mathcal{F}$ en y ajoutant le symbole ok, bien qu'il ne corresponde à aucun événement.

Définition 1 (Macrofaute) *Une* macrofaute F_j *est un ensemble de fautes élémentaires,* $F_j \subseteq \mathcal{F}, F_j \neq \emptyset$ *tel que* F_j *est présent ssi une des fautes élémentaires* $f_i \in F_j$ *est présente dans le système (et seulement une de par l'absence de fautes multiples).*

Par exemple, la macrofaute $\{f_1, f_2\}$ représente soit la présence de f_1, soit la présence de f_2. La macrofaute $\{f_2, ok\}$ signifie la présence de f_2 ou l'absence de faute.
Une macrofaute peut être un singleton ($F_j = \{f_i\}$), autrement dit, toute faute élémentaire peut être vue comme une macrofaute particulière. Un ensemble de macrofautes est noté $E(\mathcal{F})$ (avec $E(\mathcal{F}) \subseteq 2^{\mathcal{F}}$). Si chaque faute élémentaire est incluse dans au moins un élément de $E(\mathcal{F})$ alors cet ensemble $E(\mathcal{F})$ est un *ensemble couvrant* de $\mathcal{F}$.

Définition 2 (Ensemble couvrant) *Un ensemble de macrofautes* $E(\mathcal{F})$ *est* couvrant *si et seulement si* $\forall f_i \in \mathcal{F}, \exists F_j \in E(\mathcal{F})$ *tel que* $f_i \in F_j$.

3.2 Réparations

La notion de plan de réparation est introduite ici de façon simplifiée. Il est possible de définir cette notion de façon plus élaborée en fonction du contexte de planification choisi, néanmoins, les propriétés globales exposées dans cet article sont conservées. En effet, il n'est pas nécessaire de connaître exactement la sémantique d'un plan de réparation, il suffit d'être capable de les associer avec les fautes élémentaires à réparer[3].

Définition 3 (Plan de réparation) *Un* plan de réparation r_k *est une séquence d'actions* $A_k = \{a_{k1}, ..., a_{kn}\}$ *où chaque* a_{ki} *appartient à l'ensemble des actions élémentaires de réparations. Un plan de réparation est supposé toujours applicable (pas de prérequis). Il a un but* g_k *constitué d'un état nominal dans lequel le système doit se retrouver après l'application du plan.*

L'ensemble des plans de réparations est noté $\mathcal{R} = \{r_1, ..., r_{nr}\}$.
On peut ainsi voir que la définition d'un plan de réparation est indépendante des fautes sur lesquelles on peut les appliquer ; il faut pouvoir maintenant les mettre en relation explicitement. Cette relation entre plan et faute est définie à l'aide du prédicat $Répare$: $Répare(r_k, F_i)$ signifie que le plan de réparation r_k, s'il est appliqué dans un état dans lequel la macrofaute F_i est présente, est en mesure de remettre le système dans un état où le but g_k est atteint et où toute faute élémentaire est absente (c.-à-d. ok est présent).[4]

[3]De tels plans peuvent être construits dynamiquement, il suffit de savoir que la génération de ces plans est toujours possible. Cette analyse n'est pas le sujet de l'article.

[4]Nous considérons ici qu'il existe toujours un plan de réparation r_{ok} tel que $Répare(r_{ok}, \{ok\})$, le plan r_{ok} étant le plan vide (ensemble d'actions $A_{ok} = \emptyset$).

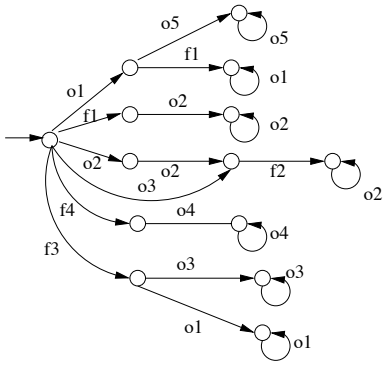

FIG. 1 – Un exemple.

Disposer d'un plan de réparation pour une macrofaute donnée signifie que l'on dispose d'un plan capable de réparer au moins toutes les fautes élémentaires incluses dans la macrofaute :

Propriété 1 $Répare(r_k, F_j) \equiv \forall f_i \in F_j, Répare(r_k, \{f_i\})$.

4 Autoguérison

L'autoguérison peut se définir intuitivement comme suit :

Un système est autoguérissant ssi, après l'occurrence d'une faute, un diagnostic peut être fait à la suite duquel un plan de réparation adapté à la situation est automatiquement déclenché.

Deux propriétés du système se cachent derrière cette définition, la diagnosticabilité et la réparabilité. Dans cette section, nous introduisons ces deux propriétés et donnons une définition de l'autoguérison.

4.1 Diagnosticabilité

Une condition pour qu'un système soit diagnosticable est que celui-ci ne soit pas *silencieux* : tout comportement (qu'il soit fautif ou non) doit produire des observations. Dans les systèmes à événements discrets, cette propriété est appelée la *vivacité* du système [10].
La diagnosticabilité repose sur la notion de *signature des fautes*[2].

Définition 4 (e-signature) *Une* e-signature *(signature élémentaire)* σ *de la macrofaute* F_j *est un observable qui est obtenu pour au moins un comportement du système* $f_i \in F_j$.

Exemple :
La figure 1 représente le modèle global d'un système à événements discrets Σ. L'ensemble des fautes élémentaires non observables est $\mathcal{F} = \{ok, f_1, f_2, f_3, f_4\}$. Les autres événements notés o_i sont tous observables. $o1o5^\infty$ est la e-signature du comportement normal ; elle est composée de l'observation $o1$ suivie d'une suite infinie de $o5$. $o2^\infty$ est

une e-signature de la faute $\{f_1\}$ et de la faute $\{f_2\}$, c'est donc aussi une e-signature de $\{f_1, f_2\}$, et ce peut être aussi une e-signature, par exemple, de $\{f_1, f_2, f_3\}$.

L'observation d'une e-signature σ indique que la macro-faute F_j peut avoir eu lieu. L'occurrence de F_j n'est pas certaine car σ peut être la e-signature d'une autre faute $F_{j'}$.

Définition 5 (e-signature caractéristique) *Une e-signature* σ caractérise F_j *ssi tout comportement produisant* σ *correspond nécessairement à l'un des* $f_i \in F_j$.

Lorsqu'une e-signature σ *caractérise* F_j, on peut être sûr, en observant σ, que la macro-faute F_j a eu lieu. Remarquons qu'une e-signature qui caractérise la faute F_j peut aussi caractériser une faute $F_{j'}$ tel que $F_{j'} \cap F_j \neq \emptyset$, et que toute e-signature caractérise la macrofaute $\mathcal{F}$.
Autrement dit, si on observe une e-signature σ caractéristique de F_j, on est sûr qu'exactement une des fautes $f_i \in F_j$ a eu lieu. Mais chaque faute $f_i \in F_j$ peut avoir d'autres e-signatures qui sont caractéristiques d'autres macrofautes incluant f_i.
Exemple : $o3o2^\infty$ est une e-signature caractéristique de la faute $\{f_2\}$ et de la faute $\{f_1, f_2\}$. $o2^\infty$ est une e-signature caractéristique de la faute $\{f_1, f_2\}$.

Définition 6 (Signature caractéristique) *Une signature* caractéristique *de* F_j *est un ensemble de e-signatures qui caractérisent* F_j. *Un tel ensemble est noté* $Sig(F_j)$.

Exemple : $\{o1^\infty, o2^\infty\}$, $\{o2^\infty, o3o2^\infty\}$,$\{o1^\infty, o3^\infty\}$ sont les ensembles de toutes les e-signatures de $\{f_1\}$,$\{f_2\}$, $\{f_3\}$ mais ce ne sont pas des signatures caractéristiques. $\{o4^\infty\}$ est l'ensemble de toutes les signatures de $\{f_4\}$ et est une signature caractéristique de $\{f_4\}$, notée $Sig(\{f_4\})$. $\{o1^\infty, o3^\infty\}$ est une signature caractéristique de $\{f_1, f_3\}$, comme le sont aussi $\{o3^\infty\}$ et $\{o1^\infty\}$.

Maintenant, nous pouvons proposer une définition de la diagnosticabilité qui convient pour l'autoguérison. Classiquement, la diagnosticabilité est définie formellement à partir d'une partition de fautes élémentaires de $\mathcal{F}$ [2]. Dans cet article, la définition de diagnosticabilité est étendue à un ensemble couvrant de macro-fautes $E(\mathcal{F}) = \{F_1, \ldots, F_m\}$.

Définition 7 (Diagnosticabilité d'un ensemble $E(\mathcal{F})$)
L'ensemble couvrant $E(\mathcal{F})$ *est* diagnosticable, *noté* $Diagnosticable(E(\mathcal{F}))$, *ssi il existe* m *signatures caractéristiques* $Sig(F_1), \ldots, Sig(F_m)$ *telles que*

1. $\bigcup_{i=1}^{m} Sig(F_i) = OBS$;
2. $\forall i, j, i \neq j, Sig(F_i) \cap Sig(F_j) = \emptyset$.

Autrement dit, l'ensemble $PSig = \{Sig(F_1), \ldots, Sig(F_m)\}$ est une *partition des e-signatures*, et $E(\mathcal{F})$ est *diagnosticable* ssi il existe une partition $PSig$, telle que l'on soit sûr en observant $\sigma \in Sig(F_j)$ que la faute F_j a eu lieu.

Exemple : Un ensemble évident de macrofautes est $E_{all}(\mathcal{F})$=$\{\mathcal{F}\}$=$\{\{ok, f_1, f_2, f_3, f_4\}\}$ pour lequel on ne peut pas distinguer les fautes élémentaires. Cet ensemble est naturellement diagnosticable, la partition des e-signatures étant $PSig_{all} = \{\{o1o5^\infty, o_1^\infty, o_2^\infty, o_3o_2^\infty, o_3^\infty, o_4^\infty\}\}$.
L'ensemble $E_1(\mathcal{F}) = \{\{ok\}, \{f_1, f_2, f_3\}, \{f_4\}\}$ est diagnosticable, avec $PSig_1 = \{\{o1o5^\infty\}, \{o_1^\infty, o_2^\infty, o_3o_2^\infty, o_3^\infty\}, \{o_4^\infty\}\}$.
$E_2(\mathcal{F}) = \{\{ok\}, \{f_1, f_2\}, \{f_1, f_3\}, \{f_4\}\}$ est aussi diagnosticable avec $PSig_2 = \{\{o1o5^\infty\}, \{o_2^\infty, o_3o_2^\infty\}, \{o_1^\infty, o_3^\infty\}, \{o_4^\infty\}\}$.
$E_3(\mathcal{F}) = \{\{ok\}, \{f_1\}, \{f_2\}, \{f_3\}, \{f_4\}\}$ n'est pas diagnosticable car il y a des cas où f_1 et f_2 ne peuvent pas être discriminées (idem pour f_1 and f_3), tout comme $E_4(\mathcal{F}) = \{\{ok\}, \{f_1\}, \{f_2, f_3\}, \{f_4\}\}$ et $E_5(\mathcal{F}) = \{\{ok\}, \{f_1, f_3\}, \{f_2\}, \{f_4\}\}$.

On pourrait alors définir qu'un système est diagnosticable, noté $Diagnosticable$, ssi $\exists E(\mathcal{F})$ tel que $Diagnosticable(E(\mathcal{F}))$. Mais on peut remarquer que du fait de la présence de ok parmi les fautes élémentaires, $Diagnosticable$ est toujours vrai, car on a toujours au moins $Diagnosticable(\{\mathcal{F}\})$ (dans notre exemple, $Diagnosticable(\{\{ok, f_1, f_2, f_3, f_4\}\})$). Le recours aux macro-fautes permet en fait de caractériser un système "plus ou moins" diagnosticable : au minimum, lorsque seul $\mathcal{F}$ est diagnosticable, cela signifie que l'on ne peut discriminer aucun des comportements ; au maximum, si les macro-fautes se réduisent aux fautes élémentaires, on pourra toujours discriminer parfaitement toutes les fautes.
Deux cas particuliers intéressants se retrouvent également dans cette définition générique. Si $\{ok\} \in E(\mathcal{F})$ et $E(\mathcal{F})$ est diagnosticable et qu'aucune des autres macrofautes ne contient ok, alors le système est *détectable* : tout comportement de faute peut être distingué du comportement normal. Enfin, si $E(\mathcal{F})$ est une partition des fautes élémentaires avec $\{ok\} \in E(\mathcal{F})$, la diagnosticabilité de $E(\mathcal{F})$ correspond à la définition classique (voir [2]).

4.2 Réparabilité

La propriété de réparabilité découle directement des définitions de macrofautes grâce au prédicat $Répare$.
Ainsi, une macrofaute F_j est réparable ssi il existe un plan de réparation qui la répare :

Définition 8 (Réparabilité d'une macrofaute)
$Réparable(F_j) \equiv \exists r_k$ *tel que* $Répare(r_k, F_j)$.

Nous pouvons en déduire l'implication suivante pour les fautes élémentaires d'une macrofaute :

Propriété 2 $Réparable(F_j) \models \forall f_i \in F_j$, $Réparable(\{f_i\})$.

L'inverse n'est pas toujours vrai (vrai uniquement s'il existe un même plan réparant tous les f_i).
La réparabilité d'un ensemble de macrofautes est alors définie comme la réparabilité de toutes les macrofautes de

cet ensemble, et la réparabilité d'un système comme l'existence d'un ensemble réparable de macrofautes.

Définition 9 (Réparabilité) *Un ensemble de macrofautes $E(\mathcal{F})$ est réparable, ce qui est noté $Réparable(E(\mathcal{F}))$, ssi $\forall F_j \in E(\mathcal{F})$ $Réparable(F_j)$.*
Le système est réparable, ce qui est noté $Réparable$, ssi $\exists E(\mathcal{F})$ tel que $Réparable(E(\mathcal{F}))$ et $E(\mathcal{F})$ est un ensemble couvrant.

Exemple : Si le seul plan de réparation est r, avec $Répare(r, \{f_1, f_3\})$, on a $Réparable(\{f_1,f_3\})$, et aussi $Réparable(\{f_1\})$ et $Réparable(\{f_3\})$. Cependant le système n'est pas réparable car les fautes f_2 and f_4 ne sont pas réparables.

4.3 Autoguérison

La définition d'autoguérison découle directement de celles de diagnosticabilité et de réparabilité.

Définition 10 (Ensemble autoguérissant de macrofautes) *Un ensemble $E(\mathcal{F})$ est* autoguérissant *ssi il est diagnosticable et réparable, i.e. $Autoguérissant(E(\mathcal{F})) \equiv Diagnosticable(E(\mathcal{F}))$ et $Réparable(E(\mathcal{F}))$*

Etant donné un ensemble autoguérissant $E(\mathcal{F})$, l'observation de $\sigma \in OBS$ est toujours associée à une macrofaute $F_\sigma \in E(\mathcal{F})$ puisque $E(\mathcal{F})$ est diagnosticable. De plus, puisque $E(\mathcal{F})$ est réparable, il existe un plan de réparation pour F_σ (plan de réparation qui répare toute faute élémentaire de F_σ), donc F_σ peut être réparée.
Pour que le système soit autoguérissant, il faut ajouter la condition que $E(\mathcal{F})$ est un ensemble couvrant, de manière à ce que toute faute élémentaire soit couverte par au moins une macrofaute et puisse donc être réparée.

Définition 11 (Système autoguérissant) *Un système est* autoguérissant *ssi il existe un ensemble couvrant autoguérissant $E(\mathcal{F})$, i.e. $Autoguérissant \equiv \exists E(\mathcal{F})$ tel que $E(\mathcal{F})$ est un ensemble couvrant et $Autoguérissant(E(\mathcal{F}))$.*

Exemple :
- Cas 1 : $Réparable(\{ok\})$ et $Réparable(\{f_1, f_3\})$ et $Réparable(\{f_1, f_2\})$ et $Réparable(\{f_4\})$
  L'ensemble $E_2(\mathcal{F}) = \{\{ok\}, \{f_1, f_2\}, \{f_1, f_3\}, \{f_4\}\}$ est diagnosticable et réparable. Le système est donc autoguérissant.
- Cas 2 : $Réparable(\{ok\})$ et $Réparable(\{f_1, f_3\})$ et $Réparable(\{f_2\})$ et $Réparable(\{f_4\})$
  Aucun ensemble de macrofautes n'est autoguérissant puisqu'il n'existe pas de plan de réparation pour $\{f_1, f_2\}$. Le système n'est donc pas autoguérissant.

Comme dit plus haut, dans un système autoguérissant, toute faute élémentaire doit pouvoir être réparée (même lorsqu'elle ne peut pas être complètement distinguée des autres fautes). Cette propriété est forte et nous verrons dans la section 6 comment elle peut être affaiblie. Mais tout d'abord nous proposons un algorithme permettant de vérifier l'autoguérison d'un système.

5 Vérifier la capacité d'autoguérison

Vérifier la capacité d'autoguérison revient à déterminer un ensemble couvrant de macrofautes ayant des propriétés particulières. Nous proposons dans cette section un algorithme qui détermine un tel ensemble particulier. Dans un premier temps, il est nécessaire d'introduire quelques notations.

Notation 1 *$MF(\sigma)$ est la macrofaute constituée de l'ensemble des fautes élémentaires qui ont en commun la signature élémentaire σ.*

Par construction, σ est une signature élémentaire qui caractérise $MF(\sigma)$ (voir la définition 5). De plus, $MF(\sigma)$ est l'ensemble *minimal* de fautes élémentaires que σ caractérise.

Notation 2 *$RP(f_i)$ est l'ensemble des plans de réparation r_k tel que $Répare(r_k, f_i)$. $AP(\sigma)$ est l'ensemble des plans applicables après l'observation de σ et ramenant le système dans un état nominal.*

$AP(\sigma)$ peut être défini comme l'intersection des ensembles de plans qui réparent toute faute élémentaire dont σ est une signature : $AP(\sigma) = \bigcap_{f_i \in MF(\sigma)} RP(f_i)$.

L'algorithme vérifiant la capacité d'autoguérison est le suivant :

pour tout $\sigma \in OBS$ **faire**
  Calculer $AP(\sigma) = \bigcap_{f_i \in MF(\sigma)} RP(f_i)$
  si $AP(\sigma) = \emptyset$ **alors**
    retourne(Pas Autoguérissant) ; fin
  fin si
fin pour
retourne(Autoguérissant) ; fin

En d'autres termes, l'algorithme conclut que le système n'est pas autoguérissant si et seulement s'il existe une signature élémentaire σ pour laquelle $AP(\sigma)$ est vide.

	$o_1o_5^\infty$	o_1^∞	o_2^∞	$o_3o_2^\infty$	o_3^∞	o_4^∞
ok	r_{ok}					
f_1		r_1, r_2	r_1, r_2			
f_2			r_1, r_3	r_1, r_3		
f_3		r_2, r_3			r_2, r_3	
f_4						r_4
	$\mathbf{r_{ok}}$	$\mathbf{r_2}$	$\mathbf{r_1}$	$\mathbf{r_1/r_3}$	$\mathbf{r_2/r_3}$	$\mathbf{r_4}$

FIG. 2 – Algorithme appliqué à l'exemple.

Exemple : L'algorithme est illustré sur l'exemple de la figure 1 par le tableau de la figure 2. Chaque colonne représente une des six signatures élémentaires. Chaque ligne est associée à une faute élémentaire et l'on suppose dans cet exemple qu'il existe quatre plans de réparations :
$RP(ok) = \{r_{ok}\}$
$RP(f_1) = \{r_1, r_2\}$

$RP(f_2) = \{r_1, r_3\}$
$RP(f_3) = \{r_2, r_3\}$
$RP(f_4) = \{r_4\}$
L'algorithme considère chaque cellule du tableau. La cellule de ligne f_i et de colonne σ est active si σ est une signature élémentaire de f_i. Si la cellule est active, l'algorithme y ajoute l'ensemble des plans réparant la faute f_i. Une fois le tableau ainsi rempli, il suffit d'attribuer à chaque colonne les plans qui sont présents dans toutes les cellules actives de la colonne (ce résultat est donné par la dernière ligne du tableau). Dans cet exemple, aucun des ensembles résultant n'est vide ce qui signifie que l'exemple de la figure 2 est autoguérissant.
Montrons maintenant que cet algorithme est complet et correct. On constate d'abord que l'algorithme construit en fait un ensemble de macrofautes particulier $E_0(\mathcal{F}) = \bigcup_{\sigma \in OBS}\{MF(\sigma)\}$ et qu'il en teste la réparabilité. Dans l'exemple, $E_0(\mathcal{F}) = \{\{ok\}, \{f_1, f_3\}, \{f_1, f_2\}, \{f_2\}, \{f_3\}, \{f_4\}\}$ (chaque macrofaute correspond ici à une colonne du tableau de la figure 2). Montrer la correction et la complétude de l'algorithme revient donc à démontrer le résultat suivant.

Propriété 3 $Autoguérissant \Leftrightarrow R\acute{e}parable(E_0(\mathcal{F}))$

Preuve : (1) Prouvons tout d'abord que $R\acute{e}parable(E_0(\mathcal{F})) \Rightarrow Autoguérissant$. Il est facile de voir que $E_0(\mathcal{F})$ est un ensemble couvrant : dans le cas contraire, cela impliquerait qu'une faute élémentaire n'a pas de signature élémentaire, ce qui contredit l'hypothèse de vivacité (voir la section 4.1). Par construction, $E_0(\mathcal{F})$ correspond à une partition des signatures élémentaires, d'où $Diagnosticable(E_0(\mathcal{F}))$. $E_0(\mathcal{F})$ étant couvrant, diagnosticable et réparable, le système est autoguérissant.
(2) Prouvons maintenant que $\neg R\acute{e}parable(E_0(\mathcal{F}))) \Rightarrow \neg Autoguérissant$. Pour cela, il suffit de montrer que si $E_0(\mathcal{F})$ n'est pas réparable alors aucun autre ensemble couvrant $E(\mathcal{F})$ ne peut l'être. Ceci s'appuie sur le fait, comme nous l'avons signalé, que $MF(\sigma)$ est l'ensemble *minimal* de fautes élémentaires que σ caractérise : pour tout σ, et pour tout autre ensemble $E(\mathcal{F})$ couvrant, il existe nécessairement une macrofaute F qui englobe $MF(\sigma)$ ($MF(\sigma) \subseteq F$). Or si $E_0(\mathcal{F})$ n'est pas réparable, il existe donc $\sigma \in OBS$ tel que $\neg R\acute{e}parable(MF(\sigma))$. Par définition de la réparabilité (propriété 2), tout sur-ensemble sera nécessairement non réparable, donc F n'est pas réparable, et $E(\mathcal{F})$ non plus. □
Cet algorithme de vérification peut être étendu afin de fournir une stratégie complète pour la réparation en-ligne. Comme on peut le constater dans l'exemple, chaque colonne est associée à un ensemble de plans possibles. Ces plans peuvent être classés selon la qualité de l'état de bon fonctionnement retrouvé. Le meilleur plan sera alors sélectionné pour chaque colonne : cette association directe entre signatures élémentaires et plans à appliquer peut alors "oublier" les fautes sous-jacentes. De plus, en fusionnant les colonnes correspondant au même plan choisi, on construit de facto un ensemble de macro-fautes $E(\mathcal{F})$ diagnosticable et réparable, qui est le $E(\mathcal{F})$ finalement retenu et qui dérive de l'ensemble primaire $E_0(\mathcal{F})$ par fusions successives.
Dans l'exemple de la figure 2, on peut choisir les plans r_1 pour la signature $o_3 o_2^\infty$ et r_2 pour la signature o_3^∞ si bien que $E(\mathcal{F})) = \{\{ok\}, \{f_1, f_2\}, \{f_1, f_3\}, \{f_4\}\}$ est associé aux plans $\{r_{ok}, r_1, r_2, r_4\}$ alors que si l'on choisit d'associer r_3 pour les deux signatures $o_3 o_2^\infty$ et o_3^∞, il en résulte que $E(\mathcal{F})) = \{\{ok\}, \{f_1, f_2\}, \{f_1, f_3\}, \{f_2, f_3\}, \{f_4\}\}$ est associé aux plans $\{r_{ok}, r_1, r_2, r_3, r_4\}$.

6 Formes affaiblies d'autoguérison

L'autoguérison telle que définie précédemment est parfaitement appropriée pour vérifier un système puisqu'elle indique que chaque faute élémentaire peut toujours être réparée, soit parce qu'elle est elle-même diagnosticable et réparable, soit parce que c'est le cas d'une macrofaute la couvrant. En d'autres termes, lors de l'occurrence d'une faute, les observations et plans de réparation sont suffisants pour garantir un diagnostic permettant de déclencher un plan de réparation adapté.
Cependant, identifier un sous-ensemble autoguérissant lorsque le système entier ne l'est pas peut aussi revêtir un intérêt : en phase de conception d'un système, on peut alors guider le concepteur pour qu'il améliore la capacité d'autoguérison existante.
Dans la suite, nous définissons deux formes affaiblies d'autoguérison. La première, appelée *autoguérison faible*, consiste à garantir que chaque faute peut être diagnostiquée et réparée au moins dans certains contextes. La seconde, appelée *autoguérison partielle*, consiste à garantir qu'il existe un sous-ensemble de fautes qui sont toujours autoguérissantes.

6.1 Autoguérison faible

Une faute élémentaire se manifeste par un ensemble de e-signatures. L'autoguérison faible est un moyen de décider si, au moins pour un sous-ensemble de ses e-signatures, chaque faute élémentaire est réparable. Nous nous appuyons pour cela sur une définition préalable de diagnosticabilité faible.

Diagnosticabilité faible. Un ensemble $E(\mathcal{F})$ est faiblement diagnosticable ssi pour chaque macrofaute de $E(\mathcal{F})$, il existe au moins une e-signature qui la caractérise. Cependant, il peut aussi exister des e-signatures qui ne caractérisent aucune macrofaute de $E(\mathcal{F})$.

Définition 12 (Diagnosticabilité faible) *L'ensemble de n macrofautes $E(\mathcal{F})$ est* faiblement diagnosticable*, ce qui se note $FaiblementDiagnosticable(E(\mathcal{F}))$, ssi $E(\mathcal{F})$ est un ensemble couvrant et il existe une partition de e-signatures $PSig = \{Sig_1, \ldots, Sig_r\}$ telle que $r \geq n$, pour tout $i \in \{1, \ldots, r\}, Sig_i \neq \emptyset$ et pour tout $i \in \{1, \ldots, n\}$, la signature Sig_i caractérise la macrofaute F_i. Un système est faiblement diagnosticable, ce qui se*

note $FaiblementDiagnosticable$*, ssi* $\exists E(\mathcal{F})$ *tel que* $FaiblementDiagnosticable(E(\mathcal{F}))$

On peut remarquer que $Diagnosticable(E(\mathcal{F})) \models FaiblementDiagnosticable(E(\mathcal{F}))$. En conséquence, un système étant, comme nous l'avons vu, toujours diagnosticable, il est également toujours faiblement diagnosticable.

Exemple :
$E_{all}(\mathcal{F})$, $E_1(\mathcal{F})$, $E_2(\mathcal{F})$ sont faiblement diagnosticables puisqu'ils sont diagnosticables. $E_3(\mathcal{F})$ et $E_4(\mathcal{F})$ ne sont pas faiblement diagnosticables car $\{f_1\}$ n'a pas de e-signature caractéristique. Par contre $E_5(\mathcal{F})$ est faiblement diagnosticable et la partition de e-signatures correspondante est $PSig_5 = \{\{o_1o_5^\infty\}, \{o_1^\infty o_3^\infty\}, \{o_3o_2^\infty\}, \{o_4^\infty\}, \{o_2^\infty\}\}$. Les quatre premières e-signatures caractérisent les quatre macrofautes de $E_5(\mathcal{F})$; la dernière, o_2^∞, est additionnelle et ne caractérise aucune macrofaute de $E_5(\mathcal{F})$.

Autoguérison faible. La définition d'autoguérison faible suit :

Définition 13 (Autoguérison faible) *L'ensemble couvrant de macrofautes* $E(\mathcal{F})$ *est* faiblement autoguérissant, *ce qui est noté* $FaiblementAutoguérissant(E(\mathcal{F}))$*, ssi il est faiblement diagnosticable et réparable.*
Le système est faiblement autoguérissant, ce qui est noté $FaiblementAutoguérissant$*, ssi* $\exists E(\mathcal{F})$ *tel que* $FaiblementAutoguérissant(E(\mathcal{F}))$.

Exemple :
- Cas 1 : $Réparable(\{ok\})$ et $Réparable(\{f_1, f_3\})$ et $Réparable(\{f_2\})$ et $Réparable(\{f_4\})$
  Aucun ensemble de macrofautes n'est autoguérissant. $E_5(\mathcal{F}) = \{\{ok\}, \{f_1, f_3\}, \{f_2\}, \{f_4\}\}$ n'est pas autoguérissant car il n'est pas diagnosticable, mais il est faiblement autoguérissant car il est faiblement diagnosticable et réparable. Par conséquent, le système n'est pas autoguérissant mais faiblement autoguérissant.
- Cas 2 : $Réparable(\{ok\})$ et $Réparable(\{f_1\})$ et $Réparable(\{f_2\})$ et $Réparable(\{f_3\})$ et $Réparable(\{f_4\})$
  Aucun ensemble de macrofautes n'est ni autoguérissant ni faiblement autoguérissant car f_1 ne peut jamais être diagnostiqué avec certitude (même dans certains contextes spécifiques). Par conséquent, le système n'est pas faiblement autoguérissant.

6.2 Autoguérison partielle

Une autre forme d'autoguérison consiste à garantir qu'un sous-ensemble seulement de fautes élémentaires est couvert par des macrofautes autoguérissantes. Nous devons en premier lieu introduire la définition suivante.

Définition 14 (Propriété de non chevauchement)
L'ensemble d'ensembles Y *ne chevauche pas l'ensemble d'ensembles* X *ssi* $Y \subseteq X$ *et* $\forall y \in Y \ \forall x \in X \setminus Y \ x \cap y = \emptyset$.

Si $X = \{\{f_1\}, \{f_1, f_2\}, \{f_3\}\}$ alors $Y = \{\{f_1\}, \{f_1, f_2\}\}$ ne chevauche pas X mais $Y = \{\{f_1\}\}$ le chevauche.

Définition 15 (Autoguérison Partielle) *L'ensemble (non couvrant) de macrofautes* $E(\mathcal{F})$ *est* partiellement autoguérissant, *ce qui est noté* $PartiellementAutoguérissant(E(\mathcal{F}))$*, ssi il existe un ensemble de macrofautes* $E'(\mathcal{F})$ *tel que* $E'(\mathcal{F})$ *est diagnosticable et* $E(\mathcal{F})$ ne chevauche pas $E'(\mathcal{F})$ *et* $E(\mathcal{F})$ *est réparable.*
Le système est partiellement autoguérissant, ce qui est noté $PartiellementAutoguérissant$*, ssi* $\exists E(\mathcal{F})$ *tel que* $PartiellementAutoguérissant(E(\mathcal{F}))$

La propriété de non chevauchement est importante puisqu'elle garantit que chaque macrofaute de $E(\mathcal{F})$ peut être diagnostiquée dans n'importe quel contexte.
Remarquons que le comportement normal ok étant considéré comme une faute élémentaire, et comme il existe un plan de réparation (le plan vide) associé à ok, alors un système détectable est toujours partiellement autoguérissant.

Exemple :
- Cas 1 : $Réparable(\{ok\})$ et $Réparable(\{f_1, f_3\})$ et $Réparable(\{f_2\})$ et $Réparable(\{f_4\})$
  $E_6(\mathcal{F}) = \{\{f_4\}\}$ est partiellement autoguérissant car il existe un ensemble couvrant de macrofautes $E_2(\mathcal{F})$ tel que $E_6(\mathcal{F}) \subset E_2(\mathcal{F})$, $E_6(\mathcal{F})$ et $E_2(\mathcal{F})$ ne se chevauchent pas, $E_2(\mathcal{F})$ est diagnosticable, et $E_6(\mathcal{F}) = \{\{f_4\}\}$ est réparable. Cela montre que la faute élémentaire f_4 peut être réparée pour n'importe laquelle de ses occurrences.
  L'ensemble $E_9(\mathcal{F}) = \{\{f_1, f_3\}\}$ n'est pas partiellement autoguérissant. Il existe un ensemble couvrant de macrofautes $E_2(\mathcal{F})$ tel que $E_9(\mathcal{F}) \subset E_2(\mathcal{F})$, $E_2(\mathcal{F})$ est diagnosticable, et $E_9(\mathcal{F}) = \{\{f_1, f_3\}\}$ est réparable mais $E_9(\mathcal{F})$ et $E_2(\mathcal{F})$ ne satisfont pas la propriété de non chevauchement ; cela signifie qu'il existe au moins une e-signature, ici o_2^∞, qui est une e-signature d'une macrofaute de l'ensemble considéré, ici de $\{f_1, f_3\}$, mais également d'une autre macrofaute n'appartenant pas à l'ensemble considéré, ici, $\{f_1, f_2\}$. Même si $E_9(\mathcal{F})$ est réparable, cela signifie que la faute élémentaire f_1 ne peut être réparée dans aucun contexte. Ce serait uniquement vrai dans le cas où il existerait aussi un plan de réparation pour $\{f_1, f_2\}$.
  Le système n'est donc pas autoguérissant mais faiblement autoguérissant et partiellement autoguérissant.
- Cas 2 : $Réparable(\{ok\})$ et $Réparable(\{f_1, f_2\})$ et $Réparable(\{f_1, f_3\})$
  A nouveau, le système n'est ni autoguérissant ni faiblement autoguérissant. Cependant, $E_7(\mathcal{F}) = \{\{f_1, f_2\}, \{f_1, f_3\}\}$ est partiellement autoguérissant puisqu'il existe un ensemble couvrant de macrofautes $E_2(\mathcal{F})$ tel que $E_7(\mathcal{F}) \subset E_2(\mathcal{F})$, $E_7(\mathcal{F})$ et $E_2(\mathcal{F})$ ne se chevauchent pas, $E_2(\mathcal{F})$ est diagnosticable, et $E_7(\mathcal{F}) = \{\{f_1, f_2\}, \{f_1, f_3\}\}$ est réparable. Les deux macrofautes $\{f_1, f_2\}$ et $\{f_1, f_3\}$ peuvent être diagnostiquées avec

certitude et sont toutes deux réparables. Cela prouve que les fautes élémentaires f_1, f_2 et f_3 peuvent donc être réparées pour n'importe laquelle de leurs occurrences. Le système est donc partiellement autoguérissant.
$E_8(\mathcal{F}) = \{\{f_1, f_2, f_3\}\}$ n'est pas partiellement autoguérissant car il n'existe aucun plan de réparation pour $\{f_1, f_2, f_3\}$. Dans le cas où il y aurait un plan de réparation pour $\{f_1, f_2, f_3\}$, $E_7(\mathcal{F}) = \{\{f_1, f_2, f_3\}\}$ serait partiellement autoguérissant (en lien avec $E_1(\mathcal{F})$).

Pour finir, notons que l'autoguérison partielle pourrait être mise en relation avec une propriété de réparation partielle. La recherche d'un ensemble couvrant de macrofautes est en effet généralement guidée par la réparation partielle : si l'on sait que certaines fautes ne sont pas réparables, il suffit de vérifier la diagnosticabilité pour les autres.
La réparation partielle signifie qu'il existe un ensemble de macrofautes (ne couvrant pas nécessairement toutes les fautes élémentaires) qui est réparable.

Définition 16 (Réparabilité partielle du système) $PartiellementRéparable \equiv \exists E(\mathcal{F})$ *tel que* $Réparable(E(\mathcal{F}))$

On obtient de manière évidente :

Propriété 4 *Réparable* $\models$ *PartiellementRéparable*
Autoguérissant $\models$ *Réparable*
FaiblementAutoguérissant $\models$ *Réparable*
PartiellementAutoguérissant $\models$ *PartiellementRéparable*

En d'autres termes, l'autoguérison partielle peut concerner (mais pas obligatoirement) un système qui est seulement partiellement réparable. Par ailleurs, un système qui est autoguérissant ou faiblement autoguérissant doit nécessairement être (complètement) réparable.
Pour résumer, un ensemble de macrofautes autoguérissant est tel que chaque macrofaute est diagnosticable et réparable, et chaque faute élémentaire est réparable (mais pas nécessairement diagnosticable).
Un ensemble de macrofautes faiblement autoguérissant est tel que, pour chaque macrofaute, il existe au moins un contexte dans lequel les macrofautes sont diagnosticables et réparables, et il existe au moins un contexte dans lequel chaque faute élémentaire est réparable.
Un ensemble de macrofautes partiellement autoguérissant est diagnosticable et réparable dans tous les contextes, mais ne couvre pas toutes les fautes élémentaires, dont certaines ne sont pas réparables.
D'autres formes affaiblies d'autoguérison pourraient être définies, notamment en couplant l'autoguérison faible et partielle.

7 Faciliter la conception d'un système autoguérissant

En contrepoint de l'étude théorique qui vient d'être menée sur les formes affaiblies de la capacité d'autoguérison, un concepteur aura généralement à faire face à la préoccupation plus prosaïque de ce qu'il convient de faire en présence d'un système non (fortement) autoguérissant... Il serait alors judicieux de l'aider à trouver des moyens d'améliorer les caractéristiques de son système afin de le rendre autoguérissant. Nous allons montrer rapidement que les structures que nous venons de mettre en place pour la vérification de l'autoguérison peuvent être avantageusement utilisées pour prendre les bonnes décisions.
La question est donc : que faire lorsque, après avoir exécuté l'algorithme, l'un des ensemble de plans applicables $AP(\sigma)$ est vide ? En premier lieu, il convient de modifier l'algorithme pour le forcer à calculer toutes les colonnes au lieu de s'arrêter à la première colonne vide... Ensuite, chaque colonne pour laquelle $AP(\sigma) = \emptyset$ indique qu'il n'y a aucun plan réparant toutes les fautes élémentaires présentes dans $MF(\sigma)$. Une décision possible, si tant est qu'elle soit possible, est justement de concevoir un nouveau plan qui serait à même de réparer indistinctement l'ensemble de ces fautes. Une autre possibilité est d'augmenter l'observabilité du système, par exemple grâce à de nouveaux moniteurs, pour récupérer des observations supplémentaires qui permettront de distinguer les trajectoires correspondant aux fautes élémentaires incriminées.
Dans notre exemple, supposons que r_2 ne répare pas f_1. Alors aucun plan ne peut être associé à o_1^∞. Augmenter les capacités de réparation revient ici à construire un plan r_5 capable de réparer aussi bien f_1 que f_3, plan qui serait alors exécuté après observation de o_1^∞. Augmenter à l'opposé les capacités d'observation exige de produire et/ou de détecter de nouveaux événements sur au moins l'une des deux trajectoires $o_1 f_1 o_1^\infty$ et $f_3 o_1 o_1^\infty$ de la figure 1, afin que leurs projections sur les observables diffèrent. Par exemple la seconde trajectoire pourrait devenir $f_3 o_1 o_6 o_1^\infty$, faisant apparaître un nouvel événement observable et donc une nouvelle e-signature $o_1 o_6 o_1^\infty$, qui pourrait être associée à r_2 ou r_3, o_1^∞ étant dès lors associée au plan r_1 seul.
Le résultat intéressant que nous souhaitons mettre en avant est que notre algorithme fournit également un outil facilitant l'identification des actions qui peuvent être entreprises, au niveau de la conception du système, pour assurer sa capacité d'autoguérison.

8 Conclusion

La principale contribution de cet article est de proposer une définition formelle et intégrée de la capacité d'*autoguérison* d'un système dynamique, qui s'appuie sur ce dont le système a besoin, pour se remettre d'une faute, en termes de capacités de diagnostic et de réparation. Il est intéressant de constater qu'il n'est pas nécessaire que le système soit diagnosticable vis-à-vis de chacune des fautes élémentaires, ni de disposer de plans de réparations distincts, spécialisés, pour chaque faute. Il convient plutôt de rechercher la présence d'un ensemble "suffisant" de situations diagnosticables pouvant être associés à un ensemble "suffisant" de réparations disponibles. Pour autant

que nous sachions, une telle définition n'avait jusqu'alors pas été proposée.

Bien entendu ce travail est une première étape qui se doit d'être prolongée de plusieurs manières. A l'heure actuelle, nous souhaitons appliquer ces résultats au domaine d'application suggéré dans l'introduction, à savoir les services web, dans le cadre du projet européen WS-DIAMOND [13], dans lequel nous étudions un certain nombre d'extensions permettant d'aborder des exemples plus sophistiqués et réalistes, concernant pour l'essentiel les propriétés et les conditions d'applicabilité des plans de réparation :

- Conditions temporelles : un premier et important défi est de prendre en compte le délai nécessaire à l'obtention d'un diagnostic, provenant de la nécessité d'attendre d'avoir un nombre suffisant d'observations ; ce délai peut entrer en conflit avec un délai de péremption associé aux plans de réparation, au-delà duquel il sera trop tard pour pouvoir appliquer le plan (par exemple parce que certains effets de la faute ne peuvent plus être compensés). Plus généralement, il convient de caractériser les observations qui rendent valide ou caduque un plan, et de les comparer temporellement aux observations qui valident un diagnostic, ces informations étant alors intégrées dans notre algorithme, afin de ne relier un plan à une faute que s'il est encore applicable lorsque le diagnostic est disponible.
- Fautes multiples : si f_2 est susceptible de se produire quelque temps après f_1, il peut s'avérer plus judicieux d'attendre et d'appliquer un plan qui réparera les deux fautes que d'appliquer deux plans successifs... ? Nous allons avoir besoin ici de préciser la définition sémantique des plans de réparation, en termes de capacité de réparer une ou plusieurs fautes en même temps (c'est-à-dire cette fois-ci "f_1 ET f_2"), ou de réparer une faute y compris lorsqu'une autre s'est également produite, etc.
- Caractérisation des solutions : les deux points précédents suggèrent également la nécessité plus générale d'optimisation dynamique de la réparation, en partant du principe qu'un système potentiellement fautif évolue entre des états de diagnostic partiel, dans lesquels on peut soit appliquer un plan de réparation, soit attendre un raffinement du diagnostic. Il s'agit alors de comparer ces stratégies afin de pouvoir prendre les "meilleures" décisions en ligne, ce qui requiert un raisonnement en termes d'utilité des décisions de réparation.

Références

[1] A. Cimatti, C. Pecheur, and R. Cavada. Formal verification of diagnosability via symbolic model checking. In *Proceedings of the 18th International Joint Conference on Artificial Intelligence IJCAI'03*, Acapulco, Mexico, 2003.

[2] M.-O. Cordier, L. Travé-Massuyès, and X. Pucel. Comparing diagnosability in continous and discrete-event systems. In C.A. González, T. Escobet, and B. Pulido, editors, *17th International Workshop on Principles of Diagnosis*, pages 55–60, June 2006.

[3] G. Garcia, J. Bernussou, and D. Arzelier. Robust stabilization of discrete-time linear systems with norm-bounded time-varying uncertainty. *Systems & Control Letters archive, Volume 22 , Issue 5*, pages 327–339, 1994.

[4] D. Ghosh, R. Sharman, H. R. Rao, and S. Upadhyaya. Self-healing systems - survey and synthesis. *Decision Support Systems*, 42(4) :2164–2185, 2007.

[5] T. Jéron, H. Marchand, S. Pinchinat, and M-O. Cordier. Supervision patterns in discrete event systems diagnosis. In *Workshop on Discrete Event Systems, WODES'06*, Ann-Arbor (MI, USA), July 2006.

[6] Y. Pencolé. Assistance for the design of a diagnosable component-based system. In *17th International Conference on Tools with Artificial Intelligence (ICTAI 05)*, pages 549–556. IEE Computer Society, 2005.

[7] X. Pucel, S. Bocconi, C. Picardi, D. Theseider Dupre, and L. Travé-Massuyès. Diagnosability analysis for web services with constraint-based models. In *18th International Workshop on Principles of Diagnosis, DX'07*, pages 360–367, Nashville (TN, USA), May 2007.

[8] P.J.G. Ramadge and W.M. Wonham. The control of discrete event systems. *Proceedings of the IEEE*, pages 81–98, 1989.

[9] A. Saboori and S. H. Zad. Fault recovery in discrete event systems. In *Proceedings of the ICSC congress on Computational Intelligence Methods and Applications (CIMA'05)*, Istanbul, Turkey., 2005.

[10] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis. Diagnosability of discrete event system. *IEEE Transactions on Automatic Control*, 40(9) :1555–1575, 1995.

[11] A. Schumann and Y. Pencolé. Scalable diagnosability checking of event-driven system. In *Proceedings of the Twentieth International Joint Conference on Artificial Intelligence (IJCAI07)*, pages 575–580, Hyderabad, India., 2007.

[12] M. Shaw. Self-healing : Softening precision to avoid brittleness. In *Proceedings of the First Workshop on Self-Healing Systems WOSS '02, Charleston, South Carolina, USA, November 18-19.*, pages 111–113. ACM, 2002.

[13] The Ws-DIAMOND team. Ws-DIAMOND : Web services DIagnosability, MOnitoring and DIagnosis. In *18th International Workshop on Principles of Diagnosis, DX'07*, pages 243–250, Nashville (TN, USA), May 2007.

[14] L. Travé-Massuyès, T. Escobet, and R. Milne. Model-based diagnosability and sensor placement application to a frame 6 gas turbine subsystem. In *Proceedings of the Seventeenth International Joint Conference on Artificial Intelligence, IJCAI'01*, volume 1, pages 551–556, 2001.

[15] R. Washington, K. Golden, and J. Bresina. Plan execution, monitoring, and adaptation for planetary rovers. In *Proceedings of the IJCAI'99 Workshop on 'Scheduling and Planning meet Real-time Monitoring in a Dynamic and Uncertain World'*, Stockholm, Sweden., 1999.

[16] T. Yoo and S. Lafortune. Polynomial-time verification of diagnosability of partially-observed discrete-event systems. *IEEE Transactions of Automatic Control*, 47(9) :1491–1495, 2002.