Diagnostic et contrôle de la dégradation des systèmes probabilistes

Nathalie Bertrand, Serge Haddad, Engel Lefaucheux

Diagnostic et contrôle de la dégradation des systèmes probabilistes

Nathalie Bertrand[1], Serge Haddad[12] *, and Engel Lefaucheux[12]

[1] Inria, France nathalie.bertrand@inria.fr
[2] LSV, ENS Paris-Saclay, CNRS, France prenom.nom@lsv.fr

Résumé

Le diagnostic actif est opéré par un contrôleur en vue de rendre un système diagnosticable. Afin d'éviter que le contrôleur ne dégrade trop fortement le système, on lui affecte généralement un second objectif en termes de qualité de service. Dans le cadre des systèmes probabilistes, une spécification possible consiste à assurer une probabilité positive qu'une exécution infinie soit correcte, ce qu'on appelle le diagnostic actif sûr. Nous introduisons ici deux spécifications alternatives. La gamma-correction du système affecte à une exécution une valeur de correction dépendant d'un facteur de décote gamma et le contrôleur doit assurer une valeur moyenne supérieure à un seuil fixé. La alpha-dégradation requiert qu'asymptotiquement, à chaque unité de temps une proportion supérieure à alpha des exécutions jusqu'alors correctes le demeure. D'un point de vue sémantique, nous explicitons des liens significatifs entre les différentes notions. Algorithmiquement, nous établissons la frontière entre décidabilité et indécidabilité des problèmes et dans le cas positif nous exhibons la complexité précise ainsi qu'une synthèse, potentiellement à mémoire infinie.

1 Introduction

Diagnostic. La conception d'un système vise entre autres à éliminer les fautes que pourrait entraîner des comportements indésirables. Cependant pour des systèmes embarqués dans des environnements matériels, l'absence de fautes n'est pas une hypothèse raisonnable. Aussi le diagnostic dont l'objectif est de détecter une faute au vu des observations de l'exécution du système est une tâche cruciale. L'une des approches fréquemment utilisée pour analyser la *diagnostiquabilité* (i.e. l'existence d'un diagnostiqueur) consiste à modéliser le système par un système de transitions dont les états (internes au système) sont inobservables et dont les événements peuvent être selon leur nature observables ou pas. On exige alors d'un diagnostiqueur deux propriétés : la *correction* et la *réactivité*. Un diagnostiqueur est correct s'il n'annonce jamais une faute à tort et il est réactif si toute faute est annoncée après un délai fini. Dans le cadre d'un système fini le problème de la diagnostiquabilité se décide en temps polynomial tandis que la synthèse d'un diagnostiqueur s'effectue en temps exponentiel [5].

Diagnostic actif. Le systèmes embarqués sont souvent dotés d'un (ou plusieurs) contrôleur(s) dans le but de maintenir certaines fonctionnalités du système en présence d'un comportement imprévu de l'environnement. Il est donc tentant d'adjoindre au contrôleur une fonction de diagnostic. Formellement certains des événements observables sont contrôlables et au vu de son observation courante, le contrôleur en autorise un sous-ensemble afin de rendre (si possible) le système diagnostiquable. Un système est alors *activement diagnostiquable* s'il existe un contrôleur assurant la fonction de diagnostic. Dans [6], les auteurs ont démontré que le problème de la diagnostiquabilité active était décidable en temps doublement exponentiel. Puis dans [4], les

*Le travail de cet auteur a été financé par le projet ERC EQualIS (FP7-308087).

auteurs ont conçu une procédure simplement exponentielle et prouvé que cette complexité était optimale.

Diagnostic probabiliste. Le caractère imprévu de l'environnement est modélisé dans les systèmes de transitions par le non déterminisme des événements possibles à partir de l'état courant. Cependant afin de quantifier les risques induits par les fautes du système, il est fréquent que le modélisateur substitue à ce choix non déterministe un choix probabiliste (ou plus généralement pondéré) entre les événements. Le modèle devient alors une chaîne de Markov à temps discret dans un cadre *passif* (i.e. sans contrôleur) et un système de transition pondéré dans un cadre *actif* (i.e. avec contrôleur). L'exigence de réactivité est alors adaptée en demandant que *presque sûrement* (i.e. avec probabilité 1) une faute soit détectée [7]. La diagnostiquabilité probabiliste passive est un problème PSPACE-complet [2] tandis que la diagnostiquabilité probabiliste active est un problème EXPTIME-complet [1].

Diagnostic actif et dégradation. Cependant les choix du contrôleur associé au diagnostic actif peuvent avoir un effet pervers : afin de détecter des fautes, le contrôleur doit parfois favoriser l'occurrence de fautes ! En vue de contrôler la dégradation, un contrôleur assurant un *diagnostic actif sûr* garantit à la fois les fonctions de diagnostic mais également une probabilité non nulle d'exécution (infinie) correcte. Une version quantitative de cette exigence précise un seuil de probabilité ε à atteindre. La diagnostiquabilité probabiliste active sûre est un problème indécidable ; cependant en se restreignant aux contrôleurs à mémoire finie, ce problème redevient EXPTIME-complet [1].

Contributions. Assurer une probabilité non nulle d'exécution correcte n'est qu'une des possibilités pour exprimer une contrainte sur le contrôle de la dégradation d'un système et elle n'est pas nécessairement adaptée à tous les contextes. Ainsi certains systèmes sont conçus pour avoir un fonctionnement satisfaisant sur une période assez longue au terme de laquelle ils seront remplacés par un nouveau système. Afin de répondre à ce type d'exigence, nous introduisons deux nouvelles spécifications de contrôle de la dégradation :

- Un système est (γ, v)-*correct* si, en appliquant un facteur de décote temporelle $\gamma \leq 1$ sur la correction d'une exécution, la valeur moyenne du préfixe maximal correct d'une exécution est supérieure ou égale à v. La version qualitative de cette exigence notée *longtemps correct* est obtenue pour $\gamma = 1$ et $v = \infty$ et signifie que la longueur moyenne du préfixe maximal correct d'une exécution est infinie.
- Un système est α-*résistant* pour $\alpha < 1$ si la proportion des exécutions correctes décroit asymptotiquement moins vite que d'un facteur α à chaque unité de temps. Il y a deux versions qualitatives de cette exigence : être *fortement résistant* (respectivement *faiblement résistant*) signifie que pour tout α (respectivement qu'il existe α tel que) le système est α-résistant.

Dans un premier temps, nous étudions ces exigences dans un cadre passif. Nous nous intéressons plus particulièrement à leur version qualitative. Nous établissons que la sûreté d'un système implique sa correction longue et sa forte résistante et qu'aucune autre implication n'existe entre ces trois notions. Cependant ces trois notions coïncident dans les systèmes finis.

Puis nous analysons le cas actif. Nous démontrons que la diagnostiquabilité combinée avec la (γ, v)-correction ou avec la α-résistance est indécidable. Cependant contrairement au diagnostic actif sûr, la diagnostiquabilité combinée avec (1) la correction longue, (2) la forte résistance ou (3) la faible résistance est décidable et plus précisément EXPTIME-complète. De plus nous établissons que les contraintes supplémentaires de correction longue ou de forte résistance coïncident dans le

cadre actif. Ces résultats de décidabilité sont d'autant plus surprenants que les diagnostiqueurs correspondants peuvent nécessiter une mémoire infinie.

Organisation. Dans la section 2, nous définissons les systèmes de transitions probabilistes et introduisons le diagnostic et les différentes spécifications de la dégradation de ces systèmes. Nous exhibons aussi les liens entre les versions qualitatives. Dans la section 3 nous établissons le statut des problèmes de diagnostiquabilité active et, dans le cas décidable, leur complexité. Puis nous concluons et donnons des perspectives à ce travail dans la section 4. Certaines des preuves sont reportées en annexe.

2 Diagnostic et dégradation d'un SPTE

2.1 Système probabiliste de transition étiqueté

Nous adoptons un modèle probabiliste de systèmes d'évènements discrets basé sur les chaînes de Markov à temps discret.

Définition 1. *Un* système probabiliste de transition étiqueté *(SPTE) est un tuple* $\mathcal{A} = \langle Q, q_0, \Sigma, T, \mathbf{P}\rangle$ *où :*

- Q *est un ensemble au plus dénombrable d'états avec un état initial* $q_0 \in Q$ *;*
- Σ *est un ensemble fini d'événements ;*
- $T \subseteq Q \times \Sigma \times Q$ *est un ensemble de transitions ;*
- $\mathbf{P}$ *est une fonction de* T *vers* $\mathbb{Q}_{>0}$ *vérifiant pour tout* $q \in Q$ *:* $\sum_{(q,a,q')\in T} \mathbf{P}[q,a,q'] = 1$.

Un SPTE est un système de transition étiqueté (STE) équipé de probabilités de transition. La relation de transition du STE sous-jacent est définie par : $q \xrightarrow{a} q'$ pour $(q,a,q') \in T$; cette transition est dite *franchissable* dans l'état q. Par définition, dans chaque état q du SPTE au moins une transition est franchissable, *i.e.* un SPTE est *vivant*.

Notations. Etant donné un ensemble fini ou dénombrable E, on note $\mathsf{Dist}(\mathsf{E})$ l'ensemble des distributions de probabilité sur E. Ainsi étant donné $q \in Q$, la fonction qui associe $\mathbf{P}[q,a,q']$ à une paire (a,q') si $(q,a,q') \in T$ et 0 sinon, appartient à $\mathsf{Dist}(\mathsf{Q} \times \Sigma)$. Le support d'une distribution $p \in \mathsf{Dist}(\mathsf{E})$, noté $\mathsf{Supp}(p)$ est défini par $\mathsf{Supp}(p) = \{e \in \mathsf{E} \mid p(e) > 0\}$. Ainsi dans notre exemple, le support de la distribution est $\{(a,q') \mid (q,a,q') \in T\}$. Lorsque le support d'une distribution est un singleton $\{e\}$, on note cette distribution de Dirac $\mathbf{1}_e$.

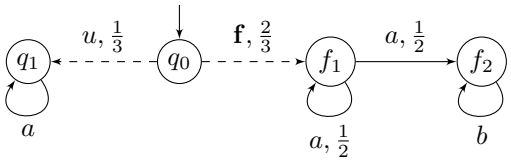

FIGURE 1 – Un exemple de SPTE (fini).

Exemple 1. *Un SPTE est représenté par un graphe étiqueté dont les sommets sont les états et dont les arcs correspondent aux transitions et sont étiquetés par l'événement associé et la probabilité de transition. Ainsi dans la figure 1, l'arc de* q_0 *à* f_1 *est déclenché par l'événement* $\mathbf{f}$

avec une probabilité $\frac{2}{3}$. *Nous omettons parfois les probabilités lorsque la distribution sortante d'un état est uniforme.*

Nous introduisons maintenant quelques notions et notations importantes utilisées dans la suite. Une *exécution* ρ d'un SPTE $\mathcal{A}$ est une séquence (finie ou infinie) $\rho = q_0 a_0 q_1 \dots$ telle que pour tout $i \geq 0$, $q_i \in Q$, $a_i \in w$ et quand q_{i+1} est définie, $q_i \xrightarrow{a_i} q_{i+1}$. La notion d'exécution se généralise, en démarrant en un état arbitraire q. Nous notons Ω l'ensemble des exécutions infinies démarrant en q_0, en supposant que le SPTE $\mathcal{A}$ est clair d'après le contexte. Une exécution ρ finie se termine dans un état et sa *longueur*, notée $|\rho|$, est le nombre d'événements de ρ. Soit une exécution finie $\rho = q_0 a_0 q_1 \dots q_n$ et une exécution (finie ou infinie) $\rho' = q_n a_n q_{n+1} \dots$ démarrant dans le dernier état ρ, nous appelons concatenation de ρ de ρ' l'exécution $\rho\rho' = q_0 a_0 q_1 \dots q_n a_n q_{n+1} \dots$. L'exécution ρ est donc un *préfixe* de $\rho\rho'$, ce que nous notons $\rho \preceq \rho\rho'$. Le *cylindre* engendré par une exécution finie ρ consiste en l'ensemble des exécution infinies qui étendent ρ : $\mathsf{Cyl}(\rho) = \{\rho' \in \Omega \mid \rho \preceq \rho'\}$. La séquence associée avec $\rho = q a_0 q_1 \dots$ est le mot $w_\rho = a_0 a_1 \dots$, et nous écrivons indifféremment $q \overset{\rho}{\Rightarrow}$ ou $q \overset{w_\rho}{\Longrightarrow}$ (resp. $q \overset{\rho}{\Rightarrow} q'$ ou $q \overset{w_\rho}{\Longrightarrow} q'$) pour une exécution infinie (resp. finie) ρ. Un état q est *accessible* (depuis l'état initial q_0) s'il existe une exécution ρ telle que $q_0 \overset{\rho}{\Rightarrow} q$, aussi noté $q_0 \Rightarrow q$. Le langage du SPTE $\mathcal{A}$ consiste en l'ensemble des mots infinis qui étiquettent les exécutions de $\mathcal{A}$ et est formellement défini comme $\mathcal{L}^\omega(\mathcal{A}) = \{\, w \in \Sigma^\omega \mid \exists\, q_0 \overset{w}{\Rightarrow} \}$.

Oubliant les étiquettes et fusionnant (et sommant les probabilités) les transitions de même source et destination, un SPTE devient une chaîne de Markov à temps discret (CMTD). Dans une CMTD, l'ensemble des exécutions infinies de $\mathcal{A}$ est le support d'une mesure de probabilité définie par le théorème d'extension de Caratheodory à partir des probabilités des cylindres :

$$\mathbb{P}_{\mathcal{A}}(\mathsf{Cyl}(q_0 a_0 q_1 \dots q_n)) = \mathbf{P}[q_0, a_0, q_1] \dots \mathbf{P}[q_{n-1}, a_{n-1}, q_n] \ .$$

Lorsque $\mathcal{A}$ est fixé, nous omettons parfois l'indice. Soit ρ une exécution finie, avec un léger abus de notation nous écrivons $\mathbb{P}(\rho)$ pour $\mathbb{P}(\mathsf{Cyl}(\rho))$. Si R est un ensemble (fini ou dénombrable) d'exécutions finies tel qu'aucune exécution n'est préfixe d'une autre, nous écrivons $\mathbb{P}(R)$ pour $\sum_{\rho \in R} \mathbb{P}(\rho)$ ce qui est consistant puisque les intersections des cylindres associés sont vides.

2.2 Observation partielle et ambiguïté

En vue de formaliser les problèmes relatifs au diagnostic de fautes, nous partitionnons l'ensemble des événements Σ en deux sous-ensembles disjoints Σ_o et Σ_u, les événements *observables* et *inobservables*, respectivement. De plus, nous distinguons un événement spécial, la *faute* $\mathbf{f} \in \Sigma_u$ et par commodité un autre événement inobservable u.

Exemple 2. *L'alphabet du SPTE de la figure 1 est défini par* $\Sigma_o = \{a, b\}$ *et* $\Sigma_u = \{\mathbf{f}, u\}$. *Les transitions étiquetées par des événements inobservables sont dessinées en pointillé.*

Soit w un mot fini d'alphabet Σ, sa longueur est notée par $|w|$. La projection des mots de Σ^* sur les événements observables est inductivement définie par : $\pi(\varepsilon) = \varepsilon$, pour $a \in \Sigma_o$, $\pi(wa) = \pi(w)a$ et pour $a \in \Sigma_u$, $\pi(wa) = \pi(w)$. Nous écrivons $|w|_o$ pour la *longueur observable* de w, c'est-à-dire $|\pi(w)|$. Lorsque w est un mot infini sur Σ, sa projection est la limite des projections des préfixes finis, et par convention $|w| = \infty$. Vis à vis de la partition $\Sigma = \Sigma_o \uplus \Sigma_u$, un SPTE $\mathcal{A}$ est dit *convergent* si, depuis tout état accessible, il n'y a pas de séquence infinie d'événements inobservables : $\mathcal{L}^\omega(\mathcal{A}) \cap \Sigma^* \Sigma_u^\omega = \emptyset$. Lorsque $\mathcal{A}$ est convergent, pour tout $w \in \mathcal{L}^\omega(\mathcal{A})$, $\pi(w) \in \Sigma_o^\omega$. Dans la suite nous supposons que les SPTE sont convergents. Nous utilisons la

terminologie *séquence* pour un mot $w \in \Sigma^* \cup \Sigma^\omega$, et *séquence observée* pour un mot $w \in \Sigma_o^* \cup \Sigma_o^\omega$. La projection d'une séquence sur Σ_o est donc une séquence observée.

La longueur observable d'une exécution ρ notée $|\rho|_o \in \mathbb{N} \cup \{\infty\}$, est le nombre d'événements observables qui y apparaissent : $|\rho|_o = |w_\rho|_o$. Une *exécution visible* est une exécution finie $q_0 a_0 q_1 \cdots a_{n-1} q_n$ telle que a_{n-1} est un événement observable. Les exécutions visibles sont précisément les exécutions pertinentes du point de vue de l'observation partielle puisque tout événement observable fournit une information supplémentaire sur l'exécution à un observateur externe. Dans la suite, SR dénote l'ensemble des exécutions visibles et SR_n l'ensemble des exécutions visibles de longueur observable n. Puisque les SPTE sont convergents, pour tout $n > 0$, SR_n est équipé d'une distribution de probabilité définie en affectant la mesure $\mathbb{P}(\rho)$ à chaque $\rho \in \mathsf{SR}_n$. Par convention, l'exécution vide q_0 est définie comme l'unique exécution de longueur nulle. Soit une séquence observée $w \in \Sigma_o^*$, nous définissons son cylindre $\mathsf{Cyl}(w) = w\Sigma_o^\omega$ et la probabilité associée $\mathbb{P}(\mathsf{Cyl}(w)) = \mathbb{P}(\{\rho \in \mathsf{SR}_{|w|} \mid \pi(\rho) = w\})$, souvent abrégée par $\mathbb{P}(w)$.

Nous classons les exécutions selon l'occurrence d'une faute. Une exécution ρ est *fautive* si sa séquence associée w_ρ contient $\mathbf{f}$, sinon elle est dite *correcte*. Soit $n \in \mathbb{N}$, nous notons F_n (resp. C_n) l'ensemble des exécutions infinies telle que le préfixe visible de longueur observable n est fautif (resp. correct). Nous définissons les ensembles des exécutions finies (resp. infinies) visibles fautives and correctes F (resp. F_∞) et C (resp. C_∞). Sans perte de généralité, en considerant deux copies par état du SPTE, nous supposons que l'espace d'état Q de $\mathcal{A}$ est partitionné entre états corrects et fautifs : $Q = Q_f \uplus Q_c$ tel que les états fautifs (resp. corrects) sont uniquement accessibles par des exécutions fautives (resp. correctes). Une sequence observée infinie (resp. finie) $w \in \Sigma_o^\omega$ (resp. Σ_o^*) est *ambiguë* s'il existe une exécution infinie (resp. visible) correcte ρ et une exécution infinie (resp. visible) fautive ρ' telle que $\pi(\rho) = \pi(\rho') = w$. Sinon, elle est soit *sûrement fautive* ou *sûrement correcte* selon que $\pi^{-1}(w) \cap \mathsf{SR} \subseteq \mathsf{F}$ ou $\pi^{-1}(w) \cap \mathsf{SR} \subseteq \mathsf{C}$. Une exécution est ambiguë, sûrement correcte ou sûrement fautive si son séquence observée est ambiguë, sûrement correcte ou sûrement fautive respectivement.

Exemple 3. *Considérons le SPTE de la figure 1. Les états corrects sont q_0 et q_1 tandis que les états fautifs sont f_1 et f_2. L'exécution $\rho_f = q_0\mathbf{f}(f_1 a)^\omega$ est fautive et ambiguë car l'unique exécution correcte $\rho_c = q_0 u(q_1 a)^\omega$ a même séquence observée a^ω. Pour tout n, la séquence finie a^n est ambiguë alors que la séquence $a^n b$ est sûrement fautive car ρ_c ne contient pas de b.*

2.3 Diagnostiquabilité d'un SPTE

La diagnostiquabilité d'un SPTE se définit en termes de probabilités d'exécutions. A cette fin, nous définissons FAmb_∞ l'ensemble des exécutions infinies fautives ambiguës de $\mathcal{A}$.

Définition 2 (Diagnostiquabilité d'un SPTE)**.** *Soit $\mathcal{A}$ un SPTE. Alors $\mathcal{A}$ est* diagnostiquable *si $\mathbb{P}(\mathsf{FAmb}_\infty) = 0$.*

Soit un entier n, FAmb_n est l'ensemble des exécutions infinies $\mathcal{A}$ dont le préfixe visible de longueur observable n est fautif et ambigu. Nous rappelons le résultat suivant qui nous permet d'utiliser une définition alternative de la diagnosabilité.

Lemme 1 ([2])**.** *Soit $\mathcal{A}$ un SPTE. Alors $\lim_{n\to\infty} \mathbb{P}(\mathsf{FAmb}_\infty \setminus \mathsf{FAmb}_n) = 0$. De plus, si $\mathcal{A}$ is finiment branchant, alors $\lim_{n\to\infty} \mathbb{P}(\mathsf{FAmb}_n \setminus \mathsf{FAmb}_\infty) = 0$ et par conséquent $\mathcal{A}$ est diagnostiquable ssi $\limsup_{n\to\infty} \mathbb{P}(\mathsf{FAmb}_n) = 0$.*

Ce résultat permet aussi de synthétiser un diagnostiqueur (à mémoire infinie) de manière évidente lorsqu'un SPTE est diagnostiquable. Après une séquence observée w, le diagnostiqueur annonce une faute si w est sûrement fautive. Par construction, le diagnostiqueur est correct et

puisque $\limsup_{n\to\infty} \mathbb{P}(\mathsf{FAmb}_n) = 0$, il est réactif. On peut en réalité construire un diagnostiqueur à mémoire finie en mémorisant uniquement les états courants possibles et annoncer une faute si ces états sont tous fautifs [7].

Exemple 4. *Considérons le SPTE de la figure 1.* FAmb_∞ *est un singleton réduit à l'exécution* $\rho_f = q_0\mathbf{f}(f_1a)^\omega$ *de probabilité nulle. Donc ce SPTE est diagnostiquable.* $\mathsf{FAmb}_n = \mathsf{Cyl}(q_0\mathbf{f}(f_1a)^n f_1) \cup \mathsf{Cyl}(q_0\mathbf{f}(f_1a)^n f_2) = \mathsf{Cyl}(q_0\mathbf{f}(f_1a)^{n-1} f_1)$. *La probabilité de* FAmb_n *est donc égale à* $\frac{2^{-n+2}}{3}$ *et tend vers 0 ainsi qu'annoncé par le lemme précédent. Dans ce cas particulier, le diagnostiqueur ne nécessite aucune mémoire et annonce une faute à la première occurrence d'un* $'b'$.

2.4 Dégradation d'un SPTE

Nous proposons et étudions trois notions de dégradation d'un système : la sûreté, la correction et la robustesse. Un SPTE est *sûr* s'il garantit une probabilité positive d'exécutions infinies correctes. On peut quantifier cette notion : SPTE est ε-sûr si cette probabilité est supérieure ou égale à ε.

Définition 3 (SPTE sûr)**.** *Soit* $\mathcal{A}$ *un SPTE.*
- *Soit* $\varepsilon > 0$, $\mathcal{A}$ *est* ε-sûr *si* $\mathbb{P}(\mathcal{C}_\infty) \geq \varepsilon$ *;*
- $\mathcal{A}$ *est* sûr *si* $\mathbb{P}(\mathcal{C}_\infty) > 0$.

Comme indiqué en introduction dans certains cas, la sûreté est une exigence trop contraignante. La correction vise à quantifier la période de temps durant laquelle le SPTE est correct. Afin de prendre (éventuellement) en compte l'importance du futur immédiat, on introduit un facteur de décote $\gamma \leq 1$ dans la mesure des instants de bon fonctionnement. L'espérance de cette mesure avec décote est alors comparée à un seuil v.

Définition 4 (SPTE correct)**.** *Soit* $\mathcal{A}$ *un SPTE,* $0 < \gamma \leq 1$ *et* $v \in [0, \infty]$.
- $\mathcal{A}$ *est* (γ, v)-correct *si* $\sum_{n\geq 1} \sum_{\rho\in\mathcal{C}_n} \mathbb{P}(\rho)\gamma^n \geq v$.
- $\mathcal{A}$ *est* longtemps correct *si* $\mathcal{A}$ *est* $(1, \infty)$*-correct.*

Observons que lorsque $\gamma = 1$, $\sum_{n\geq 1} \sum_{\rho\in\mathcal{C}_n} \mathbb{P}(\rho)\gamma^n$ est la longueur observable moyenne du préfixe visible maximal correct d'une exécution aléatoire. Ceci justifie la dénomination *longtemps correct* pour une espérance infinie.

La résistance est une mesure alternative de dégradation qui repose sur un facteur de décroissance par unité de temps $\alpha < 1$. Un SPTE est α*-résistant* si la proportion d'exécutions (finies) correctes qui restent correctes par occurrence d'événement observable est asymptotiquement supérieure à α. Cette exigence est déclinée en deux versions qualitatives : fortement résistant (respectivement faiblement résistant) si cette propriété est vraie pour tout (respectivement au moins un) α.

Définition 5 (SPTE résistant)**.** *Soit* $\mathcal{A}$ *un SPTE.*
- *Soit* $0 < \alpha < 1$. $\mathcal{A}$ *est* α-résistant *si* $\limsup_{n\to\infty} \frac{\alpha^n}{\mathbb{P}(\mathsf{C}_n)} = 0$ *;*
- $\mathcal{A}$ *est* fortement résistant *si pour tout* $0 < \alpha < 1$, $\mathcal{A}$ *est* α*-résistant ;*
- $\mathcal{A}$ *est* faiblement résistant *s'il existe* $0 < \alpha < 1$ *tel que* $\mathcal{A}$ *est* α*-résistant.*

Exemple 5. *Le SPTE* $\mathcal{A}$ *de la figure 2 comporte une unique exécution correcte* $\rho = q_0aq_1aq_2\ldots$ *alors que toutes les exécutions fautives contiennent une infinité d'occurrences de b.* $\mathcal{A}$ *est donc diagnostiquable. D'autre part, la probabilité de* ρ *est égale à* $\prod_{n\geq 1} p_n$ *et de son préfixe de longueur*

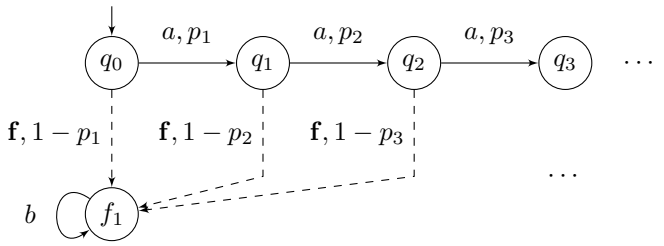

FIGURE 2 – Un exemple de SPTE infini.

n est égale à $r_n = \prod_{i\leq n} p_i$. Par conséquent, $\mathcal{A}$ est sûr ssi $\lim_{n\to\infty} r_n > 0$. Par application immédiate de la définition, $\mathcal{A}$ est longtemps correct ssi $\sum_{n\geq 1} r_n = \infty$. Examinons différentes valeurs de $(p_i)_{i\in\mathbb{N}}$.

• *Soit $p_i = \frac{i}{i+1}$. Alors $r_n = \frac{1}{n+1}$. Ainsi $\mathcal{A}$ n'est pas sûr mais longtemps correct. Pour tout $\alpha < 1$, $\lim_{n\to\infty}(n+1)\alpha^n = 0$. Ainsi $\mathcal{A}$ est aussi fortement robuste.*

• *Soit $p_i = \frac{i^2}{(i+1)^2}$. Alors $r_n = \frac{1}{(n+1)^2}$. Ainsi $\mathcal{A}$ n'est ni sûr ni longtemps correct. Pour tout $\alpha < 1$, $\lim_{n\to\infty}(n+1)^2\alpha^n = 0$. Ainsi $\mathcal{A}$ est fortement robuste.*

• *On définit inductivement deux suites m_k et n_k par :*

$$n_k = 2^{\sum_{j<k} m_j} \text{ (d'où } n_0 = 1\text{) et } m_k = n_k + \sum_{j<k} m_j + n_j.$$

Notons $I_k = [n_k + \sum_{j<k} m_j + n_j, \sum_{j\leq k} m_j + n_j[$ et $J_k = [\sum_{j\leq k} m_j + n_j, n_{k+1} + \sum_{i\leq k} m_j + n_j[$.
Lorsque $i \in I_k$, $p_i = \frac{1}{2}$. Lorsque $i \in J_k$, $p_i = 1$.
Observons que pour tout $n \in J_k$, $r_n = 2^{-\sum_{j\leq k} m_j}$.
Par conséquent $\sum_{n\geq 1} r_n \geq \sum_{k\geq 0}\sum_{n\in J_k} r_n = \sum_{k\geq 0} 2^{\sum_{j\leq k} m_j} 2^{-\sum_{j\leq k} m_j} = \infty$.
Ainsi $\mathcal{A}$ est longtemps correct.
Soit $n = \sum_{j\leq k} m_j + n_j$. Par conséquent, $r_n = 2^{-\sum_{j\leq k} m_j}$. Fixons $\alpha = \frac{1}{\sqrt{2}}$.
$\frac{\alpha^n}{r_n} = 2^{\sum_{j\leq k} m_j}(\sqrt{2})^{-\sum_{j\leq k} m_j + n_j} \geq 2^{m_k}(\sqrt{2})^{-2m_k} = 1$.
Par conséquent $\mathcal{A}$ n'est pas α-robuste.

Le théorème suivant établit précisément les liens entre les versions qualitatives des trois notions. Les deux dernières assertions de ce théorème sont des conséquences de l'exemple précédent.

Théorème 1. *Soit $\mathcal{A}$ un SPTE.*
- *Si $\mathcal{A}$ est sûr alors $\mathcal{A}$ est longtemps correct et fortement résistant ;*
- *Si $\mathcal{A}$ est fini alors :*
  $\mathcal{A}$ est sûr ssi $\mathcal{A}$ est longtemps correct ssi $\mathcal{A}$ est fortement résistant ;
- *Il existe un SPTE longtemps correct qui n'est pas fortement résistant ;*
- *Il existe un SPTE fortement résistant qui n'est pas longtemps correct.*

Démonstration. Soit $\mathcal{A}$ un SPTE sûr. Il existe $\varepsilon > 0$ tel que pour tout $n \geq 0, \mathbb{P}_{\mathcal{A}}(\mathsf{C}_n) \geq \varepsilon$. Par conséquent $\sum_{n\geq 1}\sum_{\rho\in\mathcal{C}_n} \mathbb{P}(\rho) \geq \sum_{n\geq 1}\varepsilon = \infty$. Par ailleurs, pour tout $\alpha < 1$, $\lim_{n\to\infty} \frac{\alpha^n}{\mathbb{P}(\mathsf{C}_n)} \leq \lim_{n\to\infty} \frac{\alpha^n}{\varepsilon} = 0$. Donc $\mathcal{A}$ est longtemps correct et fortement résistant.
Soit $\mathcal{A}$ un SPTE fini. Observons que toute composante fortement connexe terminale (CFCT) contient soit uniquement des états corrects soit uniquement des états fautifs. On parlera donc dans la suite de CFCT correcte ou fautive. Puisque $\mathcal{A}$ est une chaîne de Markov finie, on sait que

presque sûrement une exécution infinie atteint une CFCT et que le temps moyen d'atteinte d'une CFCT est fini. En vertu de la première propriété, $\mathcal{A}$ est sûr ssi il existe une CFCT accessible et correcte.
Supposons que $\mathcal{A}$ ne soit pas sûr.

• Toutes les CFCT accessibles sont fautives ce qui implique que le temps moyen d'atteinte d'une CFCT fautive est fini. Or ce temps moyen est un majorant de la longueur observable moyenne du préfixe visible maximal correct d'une exécution. Donc $\mathcal{A}$ n'est pas longtemps correct.
• Notons $m = |Q|$. Pour tout $q \in Q_c$, il existe ρ_q un chemin issu de q composé d'un chemin élémentaire de q vers une CFCT fautive suivi d'un chemin élémentaire dans la CFCT dont uniquement le dernier événement est visible (par convergence). Ce chemin a une longueur observable inférieure ou égale à m. Notons μ_q, la probabilité de ce chemin et $\mu = \min_{q \in Q_c} \mu_q$. Considérons une exécution visible ρ de longueur observable n pour un n arbitraire et se terminant en $q \in Q_c$. D'après l'existence de ρ_q, $\mathbb{P}(\{\rho' \in \mathsf{SR}_{n+m} \cap \mathsf{C} \mid \rho \preceq \rho'\}) \leq (1-\mu)\mathbb{P}(\rho)$. Donc $\mathbb{P}(\mathsf{C}_{n+m}) \leq (1-\mu)\mathbb{P}(\mathsf{C}_n)$. Par conséquent $\mathbb{P}(\mathsf{C}_n) \in O((1-\mu)^{\frac{n}{m}})$. Notons $\alpha = (1-\mu)^{\frac{1}{m}}$, $\mathcal{A}$ n'est pas α-résistant et donc pas fortement résistant.

□

3 Contrôle et diagnostic

3.1 Spécification et rappels

L'extension du formalisme des SPTE afin d'exprimer la possibilité d'un contrôle nécessite au moins de fixer deux caractéristiques de ce formalisme : la nature du contrôle et les distributions de probabilité d'un système contrôlé. Nous avons adopté le formalisme des SCTE décrits dans [1]. Afin de spécifier le contrôle, un sous-ensemble des événements observables est considéré comme contrôlable. Au vu de la suite des observations qu'il a obtenues le contrôleur interdit un sous-ensemble d'événements contrôlables. Le contrôle est donc inchangé entre deux observations. Les transitions du système ne sont plus étiquetées par des probabilités (rationnelles) mais par des poids (entiers) qui mesurent leur probabilité relative. Ainsi étant donné un état et un contrôle courant, les poids des transitions issues de cet état et étiquetées par des événements contrôlables autorisés ou incontrôlables sont normalisés pour former une distribution de probabilité. Afin de garantir qu'un système contrôlé forme un SPTE, le contrôle ne doit pas introduire de blocage.

Définition 6 (SCTE)**.** *Un* système contrôlable de transition étiqueté *(SCTE) est un tuple* $\mathcal{C} = \langle Q, q_0, \Sigma, T \rangle$ *où :*

- Q *est un ensemble d'états avec un état initial* $q_0 \in Q$ *;*
- $\Sigma = \Sigma_o \uplus \Sigma_u$ *est un ensemble fini d'événements partitionné en événements observables* Σ_o *contenant des événements contrôlables* $\Sigma_c \subseteq \Sigma_o$ *et non observables* Σ_u *contenant la faute* $\mathbf{f}$ *;*
- $T : Q \times \Sigma \times Q \to \mathbb{N}$ *est la fonction de transition qui associe à une transition un poids entier ;*

Un SCTE a un système de transitions sous-jacent dont la relation de transition est définie par $q \xrightarrow{a} q'$ si $T(q, a, q') > 0$. La relation étendue $\Rightarrow$ est définie commme pour les SPTE. Comme précédemment, nous supposons que ce STE est convergent et vivant (i.e. $\forall q \; \exists q \xrightarrow{a} q'$).

Exemple 6. *Un SCTE* $\mathcal{C}$ *est présenté en figure 3. Les poids des transitions tous égaux à 1 ont été omis. Le seul événement contrôlable de* $\mathcal{C}$ *est b. Les transitions observables mais non contrôlables (donc ici étiquetées par a) ont été représentées en gras.*

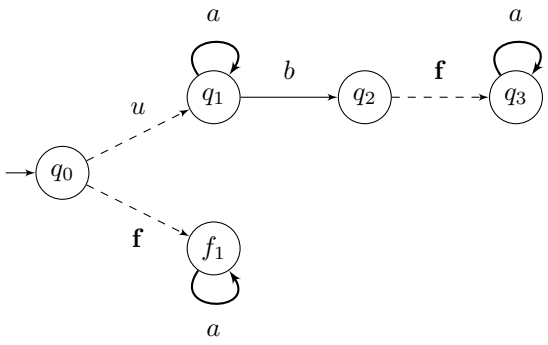

FIGURE 3 – Un exemple de SCTE.

Nous formalisons maintenant les éléments nécessaires au contrôle du SCTE. Soit $\Sigma^\bullet \subset \Sigma$ et $q \in Q$, notons $G^{\Sigma^\bullet}(q)$ la somme des poids des transitions issues de q étiquetées par un événement de $\Sigma^\bullet$. A l'aide de cette somme, nous définissons une normalisation de la relation de transition restreinte aux événements de $\Sigma^\bullet$ par :

$$T^{\Sigma^\bullet}(q,a,q') = \begin{cases} \frac{T(q,a,q')}{G^{\Sigma^\bullet}(q)} \text{ si } a \in \Sigma^\bullet \text{ et } T(q,a,q') > 0 \\ 0 \text{ sinon} \end{cases}$$

Une *stratégie* d'un SCTE $\mathcal{C}$ est une fonction $\sigma : \Sigma_o^* \to \mathsf{Dist}(2^\Sigma)$ telle que pour tout $w \in \Sigma_o^*$ et tout $\Sigma^\bullet \in \mathsf{Supp}(\sigma(w))$, $\Sigma \setminus \Sigma_c \subseteq \Sigma^\bullet$. Etant donnée une observation, une stratégie consiste à choisir aléatoirement un sous-ensemble d'événements autorisés contenant les événements incontrôlables. Soit un SCTE $\mathcal{C}$ et une stratégie σ, nous considérons des *configurations* de la forme $(w, q, \Sigma^\bullet) \in \Sigma_o^* \times Q \times 2^\Sigma$ avec w la séquence observée, q l'état courant et $\Sigma^\bullet$ est l'ensemble des événements autorisés par σ après observation de w. Nous définissons inductivement l'ensemble $\mathsf{Reach}_\sigma(\mathcal{C})$ des configurations accessibles sous σ par :

- pour tout $\Sigma^\bullet \in \mathsf{Supp}(\sigma(\varepsilon))$, $(\varepsilon, q_0, \Sigma^\bullet) \in \mathsf{Reach}_\sigma(\mathcal{C})$;
- pour tout $(w, q, \Sigma^\bullet) \in \mathsf{Reach}_\sigma(\mathcal{C})$ et tout $a \in \Sigma_u \cap \Sigma^\bullet$ tel que $q \xrightarrow{a} q'$, $(w, q', \Sigma^\bullet) \in \mathsf{Reach}_\sigma(\mathcal{C})$, noté $(w, q, \Sigma^\bullet) \xrightarrow{a}_\sigma (w, q', \Sigma^\bullet)$;
- pour tout $(w, q, \Sigma^\bullet) \in \mathsf{Reach}_\sigma(\mathcal{C})$, tout $a \in \Sigma_o \cap \Sigma^\bullet$ tel que $q \xrightarrow{a} q'$ et tout $\Sigma^{\bullet\prime} \in \mathsf{Supp}(\sigma(wa))$, $(wa, q', \Sigma^{\bullet\prime}) \in \mathsf{Reach}_\sigma(\mathcal{C})$, noté $(w, q, \Sigma^\bullet) \xrightarrow{a}_\sigma (wa, q', \Sigma^{\bullet\prime})$.

Une stratégie σ est dite *vivante* si pour toute configuration $(w, q, \Sigma^\bullet) \in \mathsf{Reach}_\sigma(\mathcal{C})$, $G^{\Sigma^\bullet}(q) \neq 0$. Seules les stratégies vivantes sont pertinentes puisque les autres stratégies introduisent des blocages. Nous sommes maintenant en mesure d'introduire la sémantique d'un SCTE contrôlé par une stratégie vivante σ en terme de SPTE. Son ensemble d'états est $\mathsf{Reach}_\sigma(\mathcal{C})$ complété par un état initial dont le but est de choisir aléatoirement conformément à $\sigma(\varepsilon)$ le contrôle initial. Les probabilités de transition sont définies par $T^{\Sigma^\bullet}$ si le contrôle courant est $\Sigma^\bullet$ sachant que lors d'une occurence d'un événement observable ces probabilités sont combinées avec le choix aléatoire (défini par σ) du contrôle suivant.

Définition 7. *Soit un SCTE $\mathcal{C}$ et une stratégie vivante σ, le SPTE $\mathcal{C}_\sigma$ induit par la stratégie σ sur $\mathcal{C}$ est défini comme $\mathcal{C}_\sigma = \langle Q_\sigma, \Sigma, q_{0\sigma}, T_\sigma, \mathbf{P}_\sigma \rangle$ où :*

- *$Q_\sigma = \{q_{0\sigma}\} \cup \mathsf{Reach}_\sigma(\mathcal{C})$;*
- *pour tout $(\varepsilon, q_0, \Sigma^\bullet) \in \mathsf{Reach}_\sigma(\mathcal{C})$, $(q_{0\sigma}, u, (\varepsilon, q_0, \Sigma^\bullet)) \in T_\sigma$;*

— *pour tout* $(w, q, \Sigma^\bullet), (w', q', \Sigma^{\bullet\prime}) \in \mathsf{Reach}_\sigma(\mathcal{C})$,
$\big((w, q, \Sigma^\bullet), a, (w', q', \Sigma^{\bullet\prime})\big) \in T_\sigma$ *ssi* $(w, q, \Sigma^\bullet) \xrightarrow{a}_\sigma (w', q', \Sigma^{\bullet\prime})$;
— *pour tout* $(\varepsilon, q_0, \Sigma^\bullet) \in \mathsf{Reach}_\sigma(\mathcal{C})$, $\mathbf{P}_\sigma(q_{0\sigma}, u, (\varepsilon, q_0, \Sigma^\bullet)) = \sigma(\varepsilon)(\Sigma^\bullet)$;
— *pour tout* $((w, q, \Sigma^\bullet), a, (w, q', \Sigma^\bullet)) \in T_\sigma$ *et tout* $a \in \Sigma_u \cap \Sigma^\bullet$,
$\mathbf{P}_\sigma\left((w, q, \Sigma^\bullet), a, (w, q', \Sigma^\bullet)\right) = T^{\Sigma^\bullet}(q, a, q')$;
— *pour tout* $\Big((w, q, \Sigma^\bullet), a, (wa, q', \Sigma^{\bullet'})\Big) \in T_\sigma$ *et tout* $a \in \Sigma_o \cap \Sigma^\bullet$,
$\mathbf{P}_\sigma\Big((w, q, \Sigma^\bullet), a, (wa, q', \Sigma^{\bullet'})\Big) = T^{\Sigma^\bullet}(q, a, q') \cdot \sigma(w.a)(\Sigma^{\bullet\prime})$.

Exemple 7. *Considérons le SCTE* $\mathcal{C}$ *présenté en figure 3. Il y a deux sous-ensembles possibles autorisés* Σ *et* $\Sigma \setminus \{b\}$ *que nous notons* Σ^-. *Définissons la stratégie* σ *par* $\sigma(a^n) = p_n \cdot \Sigma^- + r_n \cdot \Sigma$ *avec* $p_n + r_n = 1$ *pour tout* $n \in \mathbb{N}$ *et* $\sigma(w) = \mathbf{1}_\Sigma$ *pour tout autre* w. *Un extrait du SPTE* $\mathcal{C}_\sigma$ *est présenté en Figure 4. Détaillons la distribution de probabilité issue de la configuration* $(\varepsilon, q_1, \Sigma)$. *Les deux transitions sortantes de* q_1 *sont franchissables avec des probabilités relatives égales donc normalisées à 0.5. Puisque* a *et* b *sont observables le nouveau contrôle est choisi dans le cas de* a *par un choix probabiliste* $p_1 \cdot \Sigma^- + r_1 \cdot \Sigma$ *tandis que le cas de* b, *il s'agit d'un choix déterministe* $\mathbf{1}_\Sigma$. *Ceci résulte finalement en trois transitions étiquetées par* $0.5p_1$, $0.5r_1$ *et* 0.5.

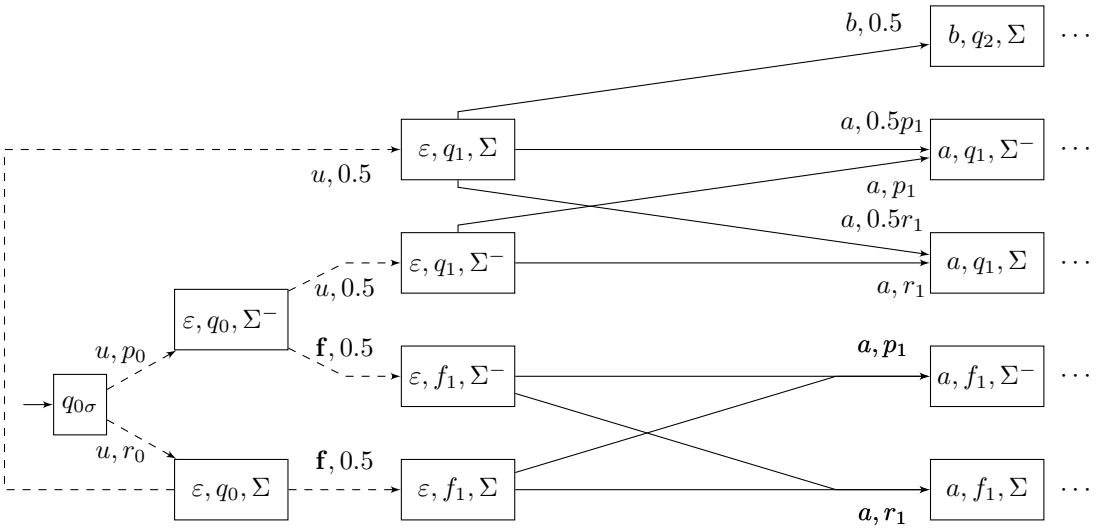

FIGURE 4 – Un exemple de SCTE contrôlé.

Nous sommes maintenant en mesure de définir les problèmes de diagnostic actif dans un contexte de contrôle de la dégradation. De manière informelle, étant donné un SCTE, il s'agit de décider s'il existe une stratégie telle que le SPTE associé soit diagnostiquable et satisfait une propriété relative à sa dégradation. Nous distinguerons comme cela se fait usuellement les problèmes quantitatifs (i.e. incluant des valeurs numériques) des problèmes qualitatifs (tels que la sûreté, la correction longue et les faible et forte résistances).

Définition 8 (Problèmes quantitatifs)**.** *Etant donné un SCTE* $\mathcal{C}$, $0 < \varepsilon, \alpha < 1$, $0 < \gamma \leq 1$ *et* $v \in [0, \infty]$ *:*

— *Le problème de* diagnostic actif ε-sûr *consiste à décider s'il existe une stratégie* σ *telle que* $\mathcal{C}_\sigma$ *est diagnostiquable et* ε*-sûr ;*
— *Le problème de* diagnostic actif (γ, v)-correct *consiste à décider s'il existe une stratégie* σ *telle que* $\mathcal{C}_\sigma$ *est diagnostiquable et* (γ, v)*-correct ;*
— *Le problème de* diagnostic actif α-résistant *consiste à décider s'il existe une stratégie* σ *telle que* $\mathcal{C}_\sigma$ *est diagnostiquable et* α*-résistant.*

Définition 9 (Problèmes qualitatifs)**.** *Etant donné un SCTE* $\mathcal{C}$ *:*
— *Le problème de* diagnostic actif sûr *consiste à décider s'il existe une stratégie* σ *telle que* $\mathcal{C}_\sigma$ *est diagnostiquable et sûr ;*
— *Le problème de* diagnostic actif longtemps correct *consiste à décider s'il existe une stratégie* σ *telle que* $\mathcal{C}_\sigma$ *est diagnostiquable et longtemps correct ;*
— *Le problème de* diagnostic actif fortement résistant *consiste à décider s'il existe une stratégie* σ *telle que* $\mathcal{C}_\sigma$ *est diagnostiquable et fortement résistant.*
— *Le problème de* diagnostic actif faiblement résistant *consiste à décider s'il existe une stratégie* σ *telle que* $\mathcal{C}_\sigma$ *est diagnostiquable et faiblement résistant.*

Rappelons les résultats obtenus pour le diagnostic actif sûr [1]. Les problèmes quantitatifs et qualitatifs du diagnostic actif sûr sont indécidables. Cependant si on se restreint à des stratégies à mémoire finie le problème qualitatif devient EXPTIME-complet. Or le SPTE obtenu par application d'une stratégie à mémoire finie est fini. En vertu des équivalences du théorème 1, nous obtenons immédiatement le théorème suivant.

Théorème 2. *Les problèmes du diagnostic actif longtemps correct et du diagnostic actif fortement résistant restreints aux stratégies à mémoire finie sont* EXPTIME*-complets.*

Exemple 8. *Afin d'illustrer l'impact de la prise en compte des stratégies à mémoire infinie, examinons le SCTE* $\mathcal{C}$ *de la figure 3. L'unique séquence observée ambiguë est* a^ω*. Une stratégie* σ *le rend donc diagnostiquable ssi la probabilité de cette séquence dans* $\mathcal{C}_\sigma$ *est nulle. Cependant l'unique exécution correcte est* $\rho = q_o u (q_1 a)^\omega$ *avec observation* a^ω*. Par conséquent* $\mathcal{C}$ *n'est pas activement diagnostiquable avec garantie de sûreté.*

Notons comme précédemment p_n*, la probabilité d'interdire b après la séquence observée* a^n *de la stratégie* σ*. Alors* $\mathbb{P}_{\mathcal{C}_\sigma}(q_o u (a q_1)^n) = \frac{1}{2}\prod_{i\leq n}\frac{1+p_i}{2}$*. Par conséquent en choisissant* $p_n = 1 - \frac{1}{n+1}$*,* $\mathcal{C}_\sigma$ *est diagnostiquable, longtemps correct et fortement résistant.*

3.2 Indécidabilité des problèmes quantitatifs

Les problèmes quantitatifs relatifs relatifs à la correction et à la résistance s'avèrent indécidables comme celui relatif à la sûreté l'était. Le schéma des preuves des propositions suivantes s'appuie sur les automates probabilistes. Un automate probabiliste est un automate fini équipé d'une distribution sur les transitions sortantes d'un état donné et étiquetées par un caractère donné. Lorsqu'on se fixe un mot fini, on obtient une distribution sur les chemins étiquetés par ce mot et la *probabilité d'acceptation* de ce mot est la probabilité du sous-ensemble de ces chemins qui conduisent à un état final. Fixons un seuil compris strictement entre 0 et 1. Etant donné un automate probabiliste, le problème de l'existence d'un mot dont la probabilité d'acceptation est supérieure ou égale (ou strictement supérieure) à ce seuil est indécidable [3].

Les preuves de ces deux propositions sont détaillées dans l'annexe. Nous donnons ici un sketch de la preuve de la proposition 1. Etant donné un automate probabiliste $\mathcal{M}$ d'alphabet Σ, on construit un SCTE $\mathcal{C}$ composé de deux parties indépendantes dans lesquelles on entre avec une probabilité $\frac{1}{2}$ de manière inobservable. On entre dans la première partie avec une

faute et dont la faute ne peut être détectée presque sûrement que si l'événement observable $\sharp \notin \Sigma$ apparaît avec probabilité 1. La deuxième partie est constituée d'une version SCTE de $\mathcal{M}$ étendue par des transitions de sortie. On sort de $\mathcal{M}$ avec probabilité $\frac{1}{2}$ à tout moment vers une sous-partie fautive excepté si l'événement $\sharp$ intervient dans un état final de $\mathcal{M}$ auquel cas la faute peut à nouveau apparaître à tout moment avec probabilité $\frac{1}{2}$. S'il existe un mot w avec probabilité $\frac{1}{2}$, la stratégie qui consiste à forcer la séquence d'observation $w\sharp$ tant qu'on reste dans $\mathcal{M}$ garantit une longueur observable (non décotée) du préfixe maximal visible correct supérieure ou égale à 1. Dans le cas contraire, on démontre qu'aucune stratégie ne parvient à atteindre ce seuil.

Proposition 1. *Le problème du diagnostic actif (γ, v)-correct est indécidable.*

Proposition 2. *Le problème du diagnostic actif α-résistant est indécidable.*

3.3 Décidabilité des problèmes qualitatifs

L'intérêt des notions de dégradation que nous avons introduites dans ce travail apparaît ici. Contrairement au problème du diagnostic actif sûr, les trois autres problèmes qualitatifs sont décidables et EXPTIME-complets. Nous développons dans cette section la preuve la plus simple et renvoyons le lecteur à l'annexe pour les preuves manquantes. Le schéma de preuve reste globalement le même : partir de la construction qui fournit une caractérisation effective du diagnostic actif [1] (qui est aussi rappelée dans la preuve ci-dessous) et établir une contrainte nécessaire et suffisante sur l'objet construit pour assurer le contrôle de dégradation étudié.

Théorème 3. *Le problème du diagnostic actif faiblement résistant est EXPTIME-complet.*

Démonstration. Afin de d'étudier la diagnostiquabilité d'un SCTE, les auteurs de [1] enrichissent les états du SCTE avec deux sous-ensembles d'état : U (resp. V) le sous-ensemble des états corrects (resp. fautifs) accessibles par une exécution visible correspondant à la séquence d'observation courante. Une paire (U, V) est appelée une *croyance*. Formellement, soit un SCTE $\mathcal{C} = \langle Q, q_0, \Sigma, T\rangle$, on définit le SCTE $\mathcal{C}^B = \langle Q^B, q_0^B, \Sigma, T^B\rangle$ par :

— $Q^B = Q \times 2^Q \times 2^Q$ et $q_0^B = (q_0, \{q_0\}, \emptyset)$;

— $T^B((q, U, V), a, (q', U', V')) = T(q, a, q')$ avec si $a \in \Sigma_o$:

1. $U' = \{q'_c \in Q_c \mid \exists q_c \in U, \exists \rho \in \mathsf{SR}_1, q_c \overset{\rho}{\Rightarrow} q'_c \wedge \pi(\rho) = a\}$
2. $V' = \{q_f \in Q_f \mid \exists q_x \in U \cup V, \exists \rho \in \mathsf{SR}_1, q_x \overset{\rho}{\Rightarrow} q_f \wedge \pi(\rho) = a\}$.

et si $a \notin \Sigma_o$, $U' = U$ et $V' = V$. T est nulle pour les autres triplets.

La taille de $\mathcal{C}^B$ est exponentielle par rapport à la taille de $\mathcal{A}$ et a le même comportement vis à vis des propriétés étudiées ici. Nous introduisons Δ, une version qualitative de T_B étendue aux séquences observées. Soit $w \in \Sigma_o^*$:

$$(q', U', V') \in \Delta((q, U, V), w) \text{ ssi } \exists \rho, \pi(\rho) = w \text{ et } (q, U, V) \overset{\rho}{\Rightarrow} (q', U', V').$$

Nous allons maintenant déterminer Win l'ensemble des croyances à partir desquelles $\mathcal{C}_B$ est activement diagnostiquable. Cet ensemble est obtenu par un calcul de plus grand point fixe.

Win est obtenu à partir d'une suite décroissante $(Win_n)_{n\in\mathbb{N}}$ définie inductivement. Lorsque $Win_{n+1} = Win_n$ la suite se stabilise et $Win = Win_n$. $Win_0 = 2^{Q_c} \times 2^{Q_f}$ et pour $n \in \mathbb{N}$, $(U, V) \in Win_{n+1}$ est l'ensemble des croyances de Win_n telles que pour tout état $q \in U \cup V$, il existe une séquence d'ensembles d'événements autorisés $(\Sigma_i^\bullet)_{1\leq i\leq k}$ et une séquence observée $w = o_1 \dots o_k$ avec $o_i \in \Sigma_i^\bullet$ vérifiant :

— il existe une exécution ρ à partir de (q, U, V) avec $\pi(\rho) = w$ atteignant (q^*, U^*, V^*) avec $q^* \in Q_c$ (i.e. l'état courant est correct) ou $U^* = 0$ (la faute est détectée) ;

— Considérons un état q_i atteint à partir d'un $q' \in (U, V)$ par une exécution de sous-séquence observée $o_1 \dots o_i$ avec $0 \leq i < k$, i.e. $(q_i, U_i, V_i) \in \Delta((q', U, V), o_1 \dots o_i)$ pour une croyance (U_i, V_i). Alors :

1. Le contrôle induit par $\Sigma_{i+1}^{\bullet}$ ne provoque pas de bloquage : $G^{\Sigma_{i+1}^{\bullet}}(q_i) \neq 0$;
2. Toute nouvelle croyance obtenue par un pas observable $o \in \Sigma_{i+1}^{\bullet}$ à partir de q_i appartient à Win_n : $\forall o \in \Sigma_{i+1}^{\bullet}, \forall (q_o, U_o, V_o) \in \Delta((q_i, U_i, V_i), o), (U_o, V_o) \in Win_n$.

Puisqu'à chaque itération non terminale une croyance est retirée, cette construction s'effectue en temps polynomial en la taille de $\mathcal{C}^B$. Dans [1], la correction de cette construction est établie et σ^* une stratégie (déterministe et à mémoire finie) assurant la diagnostiquabilité consiste étant donnée la croyance $(U, V) \in Win$ à choisir le plus grand ensemble $\Sigma^{\bullet}$ tel que toutes les croyances suivantes accessibles appartiennent à Win.

Considérons le SPTE $\mathcal{A}$ obtenu à partir de $\mathcal{C}^B$ réduit aux états de Win et contrôlé par la stratégie σ^*. Nous affirmons que $\mathcal{C}$ est activement diagnostiquable avec garantie de faible résistance ssi il existe un circuit accessible d'états dans $\mathcal{A}$ dont les premières composantes sont correctes.

• Supposons qu'un tel circuit existe et soit $\alpha > 0$ la probabilité de ce circuit, n_1 sa longueur, n_0 la longueur observée de la plus courte exécution atteignant un état de ce circuit et μ la probabilité de cette exécution. Pour tout $n \geq n_0$, $\mathbb{P}_{\mathcal{A}}(\mathsf{C}_n) \geq \mu\alpha^{\lceil \frac{n-n_0}{n_1} \rceil}$. Par conséquent $\mathcal{A}$ est α'-résistant pour tout $\alpha' < \alpha$. $\mathcal{A}$ est donc faiblement résistant. Par conséquent $\mathcal{C}_{w^*}$ qui a le même comportement probabiliste que $\mathcal{A}$ l'est aussi.

• Réciproquement, supposons qu'il n'existe aucun circuit approprié dans $\mathcal{A}$. Soit σ' une stratégie (vivante) tel que $\mathcal{C}_{\sigma'}$ soit diagnostiquable. Cette stratégie s'applique indifféremment à $\mathcal{C}^B$. Les états accessibles de $\mathcal{C}^B_{\sigma'}$ sont associés à des croyances de Win (au vu de la caractérisation rappelée ci-dessus). Puisque σ^* est la stratégie la plus permissive garantissant de rester dans Win, il n'existe pas non plus de circuit approprié dans $\mathcal{C}^B_{\sigma'}$. Par conséquent il existe n_f tel que toute exécution ρ dans $\mathcal{C}^B_{\sigma'}$ avec $|\rho| \geq n_f$ conduise à une première composante fautive. Donc $\mathbb{P}_{\mathcal{C}_{\sigma'}}(\mathsf{C}_{n_f}) = \mathbb{P}_{\mathcal{C}^B_{\sigma'}}(\mathsf{C}_{n_f}) = 0$ et ainsi $\mathcal{C}_{\sigma'}$ n'est pas faiblement résistant.

La borne inférieure de complexité s'obtient par réduction du problème du diagnostic actif. Soit un SCTE $\mathcal{C} = \langle Q, q_0, \Sigma, T \rangle$ on définit le SCTE $\mathcal{C}_S = \langle Q \cup \{q'_0, q_s\}, q'_0, \Sigma \cup \{\sharp\}, T' \rangle$ avec $\sharp \in \Sigma_o$ tel que $T'(q'_0, \sharp, q_0) = T'(q'_0, \sharp, q_s) = T'(q_s, \sharp, q_s) = 1$, pour tout $q, q' \in Q, a \in \Sigma, T'(q, a, q') = T(q, a, q')$ et pour tout autre triplet $T'(q, a, q') = 0$. Un examen immédiat démontre que $\mathcal{C}_S$ est diagnostiquable ssi $\mathcal{C}$ est diagnostiquable. Par construction $\mathcal{C}_S$ est sûr, ce qui implique que $\mathcal{C}_S$ est fortement résistant d'après le théorème 1, donc faiblement résistant. □

La preuve du théorème suivant repose aussi sur l'ensemble des croyances Win. On construit un sous-ensemble de Win, noté $WinK$. Une croyance de Win appartient à $WinK$ s'il existe une stratégie associée à la croyance telle que pour toute distribution dont la croyance est le support, elle garantit de rester dans Win et une probabilité positive que l'exécution reste indéfiniment correcte. Le SCTE est activement diagnostiquable avec garantie de forte résistance ssi de la croyance initiale, on peut atteindre une croyance de $WinK$ tout en restant dans Win. La stratégie gagnante consiste à combiner astucieusement la stratégie pour diagnostisquer et celle qui qui permet de rester dans $WinK$.

Théorème 4. *Le problème du diagnostic actif fortement résistant est EXPTIME-complet.*

Il s'avère que cette combinaison de stratégies permet aussi d'assurer le diagnostic actif longtemps correct. En fait, le théorème suivant établit que la caractérisation du diagnostic actif fortement résistant s'applique également au diagnostic actif longtemps correct.

Théorème 5. *Le problème du diagnostic actif longtemps correct est équivalent au problème du diagnostic actif fortement résistant et donc EXPTIME-complet.*

4 Conclusion

Nous avons étudié le diagnostic actif combiné avec un contrôle de la dégradation d'un système probabiliste. Plus précisément, nous avons proposé deux nouvelles notions de dégradation dans leur version quantitative et qualitative et montré leur lien avec la notion de sûreté. Puis nous avons montré que les problèmes associés aux versions quantitatives étaient indécidables. A l'inverse, les problèmes associés aux versions qualitatives sont EXPTIME-complets et ceci bien que les diagnostiqueurs correspondants peuvent nécessiter une mémoire infinie.

Nous disposons maintenant d'un ensemble de résultats algorithmiques que ce soit dans le cas passif ou actif qui justifierait le développement d'un outil logiciel. Dans un premier temps, cela supposera d'étudier et de choisir un formalisme plus approprié que les systèmes de transitions probabilistes du point de vue de la modélisation. Une autre direction consistera à reconsidérer la notion d'exécution fautive. Nous avons ici adopté le point de vue qu'une exécution est fautive dès l'occurrence d'une faute. On pourrait imaginer qu'une faute dégrade l'exécution mais que celle-ci reste quand même utile. Dans ce cadre, le diagnostic viserait à évaluer la dégradation et donc à estimer le nombre de fautes d'une exécution.

Références

[1] N. Bertrand, E. Fabre, S. Haar, S. Haddad, and L. Hélouët. Active diagnosis for probabilistic systems. In *Proceedings of FoSSaCS'14*, volume 8412 of *Lecture Notes in Computer Science*, pages 29–42. Springer, 2014.

[2] N. Bertrand, S. Haddad, and E. Lefaucheux. Foundation of diagnosis and predictability in probabilistic systems. In *Proceedings of FSTTCS'14*, volume 29 of *Leibniz International Proceedings in Informatics*, pages 417–429. Leibniz-Zentrum für Informatik, 2014.

[3] H. Gimbert and Y. Oualhadj. Probabilistic automata on finite words : Decidable and undecidable problems. In *ICALP 2010*, volume 6199 of *Lecture Notes in Computer Science*, pages 527–538. Springer, 2010.

[4] S. Haar, S. Haddad, T. Melliti, and S. Schwoon. Optimal constructions for active diagnosis. *Journal of Computer and System Sciences*, 83(1) :101–120, 2017.

[5] S. Jiang, Z. Huang, V. Chandra, and R. Kumar. A polynomial algorithm for testing diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, 46(8) :1318–1321, 2001.

[6] M. Sampath, S. Lafortune, and D. Teneketzis. Active diagnosis of discrete-event systems. *IEEE Transactions on Automatic Control*, 43(7) :908–929, 1998.

[7] D. Thorsley and D. Teneketzis. Diagnosability of stochastic discrete-event systems. *IEEE Transactions on Automatic Control*, 50(4) :476–492, 2005.

A Preuves additionnelles

Nous introduisons les automates probabilistes en vue des preuves d'indécidabilité. Un automate probabiliste $\mathcal{M} = \langle S, s_0, F, \Sigma, \mathbf{P}\rangle$ est défini par :

— S, un ensemble fini d'états dont s_0 l'état initial et F un sous-ensemble d'états finals ;
— Σ, un alphabet fini ;
— $\mathbf{P}$ une matrice $S \times \Sigma \times S$ à coefficents rationnels positifs tels pour tout $s \in S$ et tout $a \in \Sigma$, $\sum_{s' \in S} \mathbf{P}(s, a, s') = 1$.

La probabilité d'acceptation d'un mot $w = w_1 \dots w_n$, $val_{\mathcal{M}}(w)$ est définie par :

$$val_{\mathcal{M}}(w) = \sum_{s_1,\dots,s_n | s_n \in F} \prod_{i=0}^{n-1} \mathbf{P}(s_i, w_{i+1}, s_{i+1})$$

Soit $0 < \theta < 1$ un seuil arbitraire. Etant donné $\mathcal{M}$ un automate probabiliste, le problèmes de l'existence d'un mot w tel que $val_{\mathcal{M}}(w) \geq \theta$ (respectivement $val_{\mathcal{M}}(w) > \theta$) sont indécidables [3]. Dans les réductions qui suivent nous choisirons $\theta = \frac{1}{2}$.

Proposition 1. *Le problème du diagnostic actif (γ, v)-correct est indécidable.*

Démonstration. Nous procédons ici par réduction du problème de l'existence d'un mot tel que $val_{\mathcal{M}}(w) \geq \frac{1}{2}$. On considère un automate probabiliste $\mathcal{M} = \langle S, s_0, F, \Sigma, \mathbf{P}\rangle$ dont on supppose que : (1) $\Sigma \cap \{u, \mathbf{f}, \sharp, \natural\} = \emptyset$ et (2) les probabilités sont des fractions $\frac{n}{d}$ avec d fixé. On construit le SCTE $\mathcal{C} = \langle Q, q_0, \Sigma', T\rangle$ représenté en figure 5 (avec quelques abréviations par souci de lisibilité) et défini par :

— $Q = S \cup \{q_0, q_c^1, q_c^2, q_c^3, f_1, f_2\}$;
— $\Sigma' = \Sigma \cup \{\mathbf{f}, u, \sharp, \natural\}$, $\Sigma_u = \{\mathbf{f}, u\}$ and $\Sigma_c = \Sigma \cup \{\sharp\}$;
— la fonction de transition T est définie comme suit.

1. $T(q_0, \mathbf{f}, f_1) = T(q_0, u, s_0) = T(q_c^1, \sharp, q_c^3) = T(q_c^3, \sharp, q_c^3) = T(q_c^1, \mathbf{f}, f_2) = T(q_c^2, \mathbf{f}, f_2) = T(f_2, \natural, f_2) = T(f_1, \sharp, f_2)$;
2. Pour tout $a \in \Sigma$, $T(f_1, a, f_1) = 1$;
3. Pour tout $s, s' \in S$ et tout $a \in \Sigma$, $T(s, a, s') = d\mathbf{P}(s, a, s')$ et $T(s, a, f_1) = d$;
4. Pour tout $q \in F$, $T(q, \sharp, q_c^1) = 1$ et tout $q \in S \setminus F$, $T(q, \sharp, q_c^2) = 1$;
5. Pour tout autre triplet, T est nulle.

Montrons que $\mathcal{A}$ est $(1, 1)$-correct ssi il existe un mot w accepté dans $\mathcal{M}$ avec probabilité supérieure ou égale à $1/2$.

Soit σ une stratégie arbitraire, $\mathcal{C}_\sigma$ est diagnostiquable ssi $\natural$ apparaît presque sûrement dans une exécution. En effet une séquence observée $w \in \Sigma^*$ est ambiguë et toute exécution qui quitte $S \cup \{f_1\}$ atteint presque sûrement f_2 où $\natural$ apparaît indiquant que l'exécution est nécessairement fautive.

• Supposons qu'il existe $w = w_1 \dots w_k \in \Sigma^*$ tel que $val_{\mathcal{M}}(w) \geq \frac{1}{2}$. On définit la stratégie σ par :

— $\sigma(w) = \{\sharp, \natural\}$;
— pour tout $0 \leq i < k$, $\sigma(w_1 \dots w_i) = \{w_{i+1}, \natural\}$;
— σ est définie arbitrairement ailleurs.

Par le choix des poids et de la stratégie σ, une exécution visible correcte ρ telle que $\pi(\rho) = w_1 \dots w_i$ pour $i < k$ a une probabilité $\frac{1}{2}$ d'être correcte à la prochaine observation selon que l'état courant est q_c^2 ou appartient à S.

De même une exécution visible correcte ρ telle que $\pi(\rho) = w_1 \dots w_k$ a une probabilité $val_{\mathcal{M}}(w)$ d'être en q_c^1 et $1 - val_{\mathcal{M}}(w)$ en q_c^2.

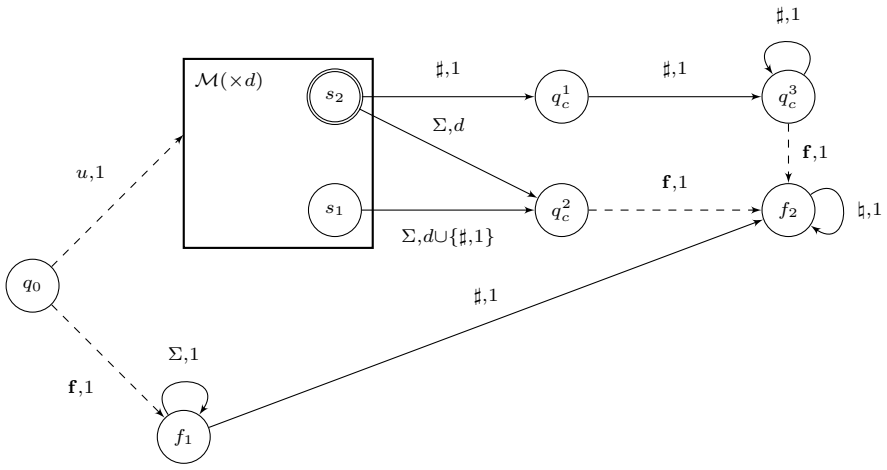

FIGURE 5 – D'un automate probabiliste à un SCTE.

Dans l'état q_c^3, une exécution correcte a une probabilité $\frac{1}{2}$ d'être encore correcte (et en q_c^3). D'où pour tout $n \leq k$, $\mathbb{P}(\mathsf{C}_n) = (\frac{1}{2})^n$ et pour tout $n > k$, $\mathbb{P}(\mathsf{C}_n) = (\frac{1}{2})^{n-1} val_{\mathcal{M}}(w) \geq (\frac{1}{2})^n$. Et finalement : $\sum_{n=1}^{\infty} \mathbb{P}(\mathsf{C}_n) \geq \sum_{n=1}^{\infty} (\frac{1}{2})^n = 1$.

• Supposons que pour tout $w \in \Sigma^*$, $val_{\mathcal{M}}(w) < \frac{1}{2}$. Soit σ une stratégie telle que $\mathcal{C}_\sigma$ soit diagnostiquable. Notons $\mathsf{last}(\rho)$ l'état courant après l'exécution ρ.
Observons que :

$$\mathbb{P}_\sigma(\mathsf{C}_n) = \sum_{w\in\Sigma^n} \mathbb{P}_\sigma(w \wedge \mathsf{C}) + \sum_{w\in\Sigma^{n-1}} \mathbb{P}_\sigma(w\sharp \wedge \mathsf{C}) + \sum_{1<k\leq n} \sum_{w\in\Sigma^{n-k}} \mathbb{P}_\sigma(w\sharp^k \wedge \mathsf{C})$$

Nous allons démontrer que $\mathbb{P}_\sigma(\mathsf{C}_{n+1}) \leq \frac{\mathbb{P}_\sigma(\mathsf{C}_n)}{2}$ avec inégalité stricte s'il existe $w \in \Sigma^{n-1}$ avec $\mathbb{P}_\sigma(w\sharp) > 0$.

$$\mathbb{P}_\sigma(\mathsf{C}_{n+1}) = \sum_{w\in\Sigma^n} \sum_{x\in\Sigma\cup\{\sharp\}} \mathbb{P}_\sigma(wx \wedge \mathsf{C}) + \sum_{w\in\Sigma^{n-1}} \mathbb{P}_\sigma(w\sharp^2 \wedge \mathsf{C}) + \sum_{1<k\leq n} \sum_{w\in\Sigma^{n-k}} \mathbb{P}_\sigma(w\sharp^{k+1} \wedge \mathsf{C})$$

Examinons chacun des termes.
◦ Une exécution correcte ρ de séquence observée w a une probabilité conditionnelle 1/2 que $\mathsf{last}(\rho) \in S$ et 1/2 que $\mathsf{last}(\rho) = q_c^2$.
Par conséquent, $\sum_{w\in\Sigma^n} \sum_{x\in\Sigma\cup\{\sharp\}} \mathbb{P}_\sigma(wx) = 1/2 \sum_{w\in\Sigma^n} \mathbb{P}_\sigma(w)$
◦ Une exécution correcte ρ de séquence observée $w\sharp^k$ avec $k > 1$ vérifie $\mathsf{last}(\rho) = q_c^3$. Par conséquent, $\sum_{1<k\leq n} \sum_{w\in\Sigma^{n-k}} \mathbb{P}_\sigma(w\sharp^{k+1} \wedge \mathsf{C}) = 1/2 \sum_{1<k\leq n} \sum_{w\in\Sigma^{n-k}} \mathbb{P}_\sigma(w\sharp^k \wedge \mathsf{C})$
◦ Une exécution correcte ρ de séquence observée $w\sharp$ a une probabilité conditionnelle $val_{\mathcal{M}}(w)$ que $\mathsf{last}(\rho) = q_c^1$ et $1 - val_{\mathcal{M}}(w)$ que $\mathsf{last}(\rho) = q_c^2$.
Par conséquent,
$\sum_{w\in\Sigma^{n-1}} \mathbb{P}_\sigma(w\sharp^2 \wedge \mathsf{C}) = \sum_{w\in\Sigma^{n-1}} val_{\mathcal{M}}(w)\mathbb{P}_\sigma(w\sharp \wedge \mathsf{C}) \leq 1/2 \sum_{w\in\Sigma^{n-1}} \mathbb{P}_\sigma(w\sharp \wedge \mathsf{C})$
avec inégalité stricte s'il existe un mot w avec $\mathbb{P}_\sigma(w\sharp) > 0$.
Or $\mathcal{C}_\sigma$ est diagnostiquable. Donc d'après notre caractérisation d'une stratégie assurant le diagnostic, il doit exister un mot w tel que $\mathbb{P}_\sigma(w\sharp) > 0$. Par conséquent, $\sum_{n=1}^{\infty} \mathbb{P}(\mathsf{C}_n) < \sum_{n=1}^{\infty} (\frac{1}{2})^n = 1$, donc $\mathcal{A}$ n'est pas $(1,1)$-correct. La même preuve peut être utilisée pour montrer que, pour

$0 < \gamma < 1$, $\mathcal{A}$ est $(\gamma, \frac{\gamma}{2-\gamma})$-correct ssi il existe un mot w accepté dans $\mathcal{M}$ avec probabilité supérieure ou égale à $1/2$.

□

Proposition 2. *Le problème du diagnostic actif α-résistant est indécidable.*

Démonstration. Il s'agit à nouveau d'une réduction depuis le problème du vide des automates probabilistes. Étant donné un automate probabiliste $\mathcal{M} = (S, s_0, \Sigma, P, F)$ on construit le SCTE $\mathcal{A} = \langle Q, s_0, \Sigma', T\rangle$ représenté en figure 6 où :

- $Q = S \cup \{f_1, f_2\}$;
- $\Sigma' = \Sigma \cup \{\mathbf{f}, u, \sharp, \natural\}$, $\Sigma_u = \{\mathbf{f}, u\}$ and $\Sigma_c = \Sigma \cup \{\sharp\}$;
- $T(f_1, \mathbf{f}, f_2) = T(f_2, \natural, f_2) = 1$. Comme les probabilités de $\mathcal{M}$ sont rationnelles, soit d leur plus petit dénominateur commun, pour $s, s' \in S, a \in \Sigma, T(s, a, s') = d \times P(s, a, s')$ et $T(s, a, f_1) = d$. For $q \in F$, $T(q, \sharp, s_0) = 1$ and for $q \in S \setminus F$, $T(q, \sharp, f_1) = 1$.

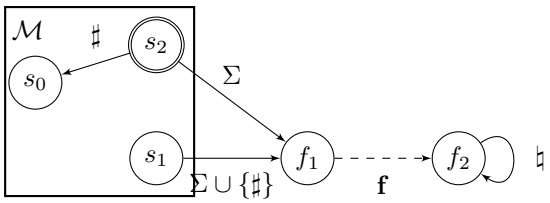

FIGURE 6 – Réduction vers la α-résistance.

Montrons qu'il existe un contrôleur σ tel que $\mathcal{A}_\sigma$ est $1/2$-résistant ssi il existe un mot $w \in \Sigma^*$ accepté dans $\mathcal{M}$ avec probabilité strictement supérieure à $1/2$.

Soit $w \in \Sigma^*$ accepté dans $\mathcal{M}$ avec probabilité strictement supérieure à $1/2$. On définit le contrôleur σ pour $\mathcal{A}$ tel que $\sigma((w\sharp)^*w) = \sharp$ et pour tout $0 \leq i < |w|$, $\sigma((w\sharp)^*w_{\downarrow i}) = w_{i+1}$ où $w_{\downarrow i}$ est le préfixe de longueur i de w et w_i est la i-ème lettre de w. Alors pour tout $n \in \mathbb{N}$, $\mathbb{P}_\sigma(\mathsf{C}_n) = (\frac{1}{2})^{n - \lfloor \frac{n}{|w|+1} \rfloor} \times \mathbb{P}_{\mathcal{M}}(w)^{\lfloor \frac{n}{|w|+1} \rfloor}$. Par conséquent, comme $\mathbb{P}_{\mathcal{M}}(w) > 1/2$, $\limsup_{n\to\infty} \frac{\frac{1}{2^n}}{\mathbb{P}_\sigma(\mathsf{C}_n)} = \limsup_{n\to\infty} \frac{(\frac{1}{2})^{\lfloor \frac{n}{|w|+1} \rfloor}}{\mathbb{P}_{\mathcal{M}}(w)^{\lfloor \frac{n}{|w|+1} \rfloor}} = 0$. Par conséquent, $\mathcal{A}_\sigma$ est $1/2$-résistant.

Supposons maintenant que pour tout mot $w \in \Sigma^*$, $\mathbb{P}_{\mathcal{M}}(w) \leq \frac{1}{2}$. Soit σ un contrôleur. Pour tout $n \in \mathbb{N}$, $\mathbb{P}_\sigma(\mathsf{C}_n) \leq \frac{1}{2^n}$. En effet, lorsqu'une lettre de Σ est observée l'exécution devient fautive avec probabilité $1/2$ et quand un $\sharp$ est déclenché l'exécution devient fautive avec une probabilité supérieure ou égale à deux, par hypothèse. Par conséquent $\limsup_{n\to\infty} \frac{\frac{1}{2^n}}{\mathbb{P}(\mathsf{C}_n)} \geq \limsup_{n\to\infty} \frac{\frac{1}{2^n}}{\frac{1}{2^n}} = 1$. □

Théorème 4. *Le problème du diagnostic actif fortement résistant est EXPTIME-complet.*

Démonstration. Soit $\mathcal{C}$ un SCTE. Nous construisons comme dans la preuve du théorème 3, $\mathcal{C}^B$, Win et σ^*. Nous définissons ensuite $WinK_U \subseteq 2^Q \times Win$ par un calcul de plus grand point fixe. Pour $(U', (U, V)) \in WinK_U$, (U, V) est une croyance pour laquelle il existe une stratégie permettant à un ensemble d'exécutions démarrant en U' de rester dans des états de $\mathcal{C}^B$ associés à une croyance de Win tout en restant correctes. $WinK_U$ est obtenue comme limite de la suite décroissante $(WinK_n)_{n\in\mathbb{N}}$ définie inductivement par $WinK_0 = \{(U', (U, V)) \mid (U, V) \in Win \wedge \emptyset \neq U' \subseteq U\}$ et pour $n \in \mathbb{N}$, $(U', (U, V)) \in WinK_{n+1}$ est un élément de $WinK_n$ tel qu'il existe un ensemble d'événements autorisés $\Sigma^\bullet$ vérifiant :

— $\Sigma^\bullet$ ne provoque pas de bloquage : $\forall q \in U \cup V, G^{\Sigma^\bullet}(q) \neq 0$;
— sous le contrôle $\Sigma^\bullet$ aucune exécution démarrant dans un état de U' ne réalisera de faute avant la prochaine observation : $\forall q_c \in U', \forall \rho \in \mathsf{SR}_1, q_c \stackrel{\rho}{\Rightarrow} q_c \wedge \pi(\rho) \in \Sigma^\bullet \Rightarrow q \in Q_c$;
— tout triplet atteint par un pas observable de $o \in \Sigma^\bullet$ appartient à $WinK_n$: $(\tilde{U}', (\tilde{U}, \tilde{V})) \in WinK_n$ avec :

1. $\tilde{U}' = \{q'_c \in Q_c \mid \exists q_c \in U'_1, \exists \rho \in \mathsf{SR}_1, q_c \stackrel{\rho}{\Rightarrow} q'_c \wedge \pi(\rho) = a\}$;
2. $(\tilde{U}, \tilde{V})$ obtenue par la mise à jour de la croyance (U, V) suite à l'observation o.

A partir de $WinK_U$, nous définissons l'ensemble $WinK \subseteq Win$ en conservant uniquement la seconde composante de $WinK_U$: $WinK = \{(U, V) \in Win_\infty \mid \exists U', (U', (U, V)) \in WinK_U\}$. Observons certaines propriétés de cette construction.

— Par induction, si $(U', (U, V)) \notin WinK_n$ alors pour toute stratégie (vivante), il existe une exécution fautive démarrant en U' de longueur observable n ;
— Si $\emptyset \neq U'' \subseteq U'$ alors $(U', (U, V)) \in WinK_U$ implique $(U'', (U, V)) \in WinK_U$. Par conséquent, si $(U, V) \notin WinK$, pour tout $q \in U$, $(\{q\}, (U, V)) \notin WinK_U$.

On définit également $PreWin$ l'ensemble des états de $\mathcal{C}^B$ de la forme $Q \times Win$ depuis lequel un état (q, U, V) avec $(U, V) \in WinK$ est accessible. Montrons que $\mathcal{C}$ est diagnostiquable et fortement résistant ssi l'état initial de $\mathcal{C}^B$ appartient à $PreWin$.

• Supposons que l'état initial appartienne à $PreWin$. Soit $(U', (U, V))$ un élément de $WinK_U$. On définit $\sigma_{(U',(U,V))}$ dont la mémoire est un triplet $(\tilde{U}', (\tilde{U}, \tilde{V}))$ et qui, en partant de $(U', (U, V))$, reste dans $WinK_U$. Cette stratégie se déduit immédiatement de la construction de $WinK_U$.

Soit $(U, V) \in WinK$.
On définit $\sigma_{(U,V)} = \sigma_{(U',(U,V))}$ pour un U' arbitraire tel que $(U', (U, V)) \in WinK_U$.

Enfin on définit la stratégie σ_0 qui fonctionne en trois phases dont chaque phase successive peut n'être jamais déclenchée.

1. Initialement σ_0 se comporte comme σ^* jusqu'à ce que la croyance (U, V) rencontrée appartienne à $WinK$;
2. Puis durant la deuxième phase à chaque nouvelle séquence observée w, σ_0 choisit avec probabilité $p_w = \frac{|w|}{|w|+1}$ d'appliquer $\sigma_{(U,V)}$ et avec probabilité $1 - p_w$ de passer à la troisième phase ;
3. σ_0 se comporte indéfiniment comme σ^*.

$\mathcal{C}_{\sigma_0}$ est diagnostiquable. En effet, comme les ensembles d'événements autorisés par σ_0 sont des sous-ensembles de ceux autorisés par σ^*, et que (au vu du choix de p_w) avec probabilité 1, σ^* sera appliqué ultimement, toute faute sera presque sûrement détectée.
De plus, il est fortement résistant. En effet, par définition de $PreWin$, il existe une exécution ρ depuis l'état initial atteignant un état (q, U, V) tel que (U, V) appartienne à $WinK$. Notons $U' \subseteq U$ celui choisi arbitrairement pour définir $\sigma_{(U,V)}$. Sans perte de généralité, on suppose que ρ atteint un état de U'. Comme une faute ne peut être provoquée après ρ que si σ_0 passe en troisième phase, pour $n \geq |\rho|_o$ on a $\mathbb{P}(\tilde{\rho} \in \mathsf{C}_n \mid \rho \preceq \tilde{\rho}) \geq \mathbb{P}(\rho) \prod_{i=|\rho|}^{n} \frac{i}{i+1} = \mathbb{P}(\rho) \frac{|\rho|}{n+1}$ et pour tout $\alpha < 1$, $n\alpha^n$ tend vers 0.

• Réciproquement, supposons que l'état initial n'appartienne pas à $PreWin$. Soit σ une stratégie assurant la diagnostiquabilité. Pour tout état (q, U, V) avec $q \in U$ accessible par une exécution ρ_0 avec σ, $(U, V) \notin WinK$ et en vertu d'une de nos observations $(\{q\}, (U, V)) \notin WinK_U$. Soit K le nombre d'itérations du calcul du point fixe dans la création de $WinK$. En vertu de l'autre observation, pour toute suite de K choix aléatoires effectués par σ, il existe une exécution $\rho \in \mathsf{F}$ compatible avec ces choix démarrant en (q, U, V) de longueur observable

inférieure à K. En sommant les exécutions correspondant à chaque suite de choix de σ on obtient $\mathbb{P}_\sigma(\rho \in \mathsf{F}_{|\rho_0|_o+K} \mid \rho_0 \preceq \rho) \geq \mathbb{P}_\sigma(\rho_0)\lambda^{K|Q|})$ où $\lambda = \min_{q\in Q} \frac{1}{G^\Sigma(q)}$. Par conséquent pour tout $n \in \mathbb{N}, \mathbb{P}_\sigma(\mathsf{C}_{n+K}) \leq \mathbb{P}_\sigma(\mathsf{C}_n)(1-\lambda^{K|Q|})$. En posant $\alpha = (1-\lambda^{K.|Q|})^{\frac{1}{K}}$, on a $\lim_{n\to\infty} \frac{\alpha^n}{\mathbb{P}_\sigma(\mathsf{C}_n)} > 0$. La EXPTIME-difficulté s'obtient par la même réduction que celle du théorème 3.

□

Théorème 5. *Le problème du diagnostic actif longtemps correct est équivalent au problème du diagnostic actif fortement résistant et donc EXPTIME-complet.*

Démonstration. Nous allons montrer ici que la caractérisation fournie dans le théorème 4 qu'un SCTE soit activement diagnostiquable et fortement résistant permet également de caractériser si le SCTE est activement diagnostiquable et longtemps correct. Ceci montrera l'équivalence des deux notions dans le cadre actif ainsi que la EXPTIME-complétude du problème de décision. Etant donné un SCTE, on effectue les mêmes constructions que dans la preuve du théorème 4 et réutilisons les notations introduites. Montrons que $\mathcal{C}$ est diagnostiquable et fortement résistant ssi l'état initial de $\mathcal{C}^B$ appartient à $PreWin$.

• Supposons que l'état initial appartienne à $PreWin$. Alors, comme vu dans la preuve du théorème 4, $\mathcal{C}_{\sigma_0}$ est diagnostiquable et il existe une exécution finie ρ telle que $\mathbb{P}(\tilde{\rho} \in \mathsf{C}_n \mid \rho \preceq \tilde{\rho}) \geq \mathbb{P}(\rho)\frac{|\rho|}{n+1}$. Par conséquent :

$$\sum_{n=1}^{\infty} \mathbb{P}(\mathsf{C}_n) \geq \sum_{n=|\rho|}^{\infty} \mathbb{P}(\tilde{\rho} \in \mathsf{C}_n \mid \rho \preceq \tilde{\rho}) \geq \mathbb{P}(\rho)|\rho| \sum_{n=|\rho|}^{\infty} \frac{1}{n+1} = \infty.$$

• Réciproquement, si l'état initial n'appartient pas à $PreWin$. Soit σ une stratégie assurant la diagnostiquabilité. En reprenant les notations du théorème 4, on a pour tout $n \in \mathbb{N}, \mathbb{P}(\mathsf{C}_{n+K}) \leq \mathbb{P}(\mathsf{C}_n)(1-\lambda^{K.|Q|})$. Par conséquent :

$$\sum_{n=1}^{\infty} \mathbb{P}(\mathsf{C}_n) \leq K \sum_{n=1}^{\infty} (1-\lambda^{K.|Q|})^n \leq K.|Q_B|.\frac{1}{\lambda^{K.|Q|}} < \infty.$$

□