Rapport de stage
DEA Algorithmique 2001/2002

Vérification de canaux à pertes stochastiques

Nathalie BERTRAND

Sous la direction de Philippe Schnoebelen

Laboratoire Spécification et Vérification, ENS Cachan

Table des matières

Chapitre 1

Introduction, motivation

1.1 Systèmes stochastiques

De nombreux systèmes réels peuvent être modélisés par des systèmes stochastiques et cela pour différentes raisons. Dans tous les cas cette modélisation est sensée quand on considère que le comportement est régi par une loi de probabilité.

Algorithmes randomisés. Les algorithmes randomisés par exemple utilisent des tirages aléatoires (pile ou face, dé, génération aléatoire de nombre). Si ces tirages ne sont pas biaisés, on peut naturellement les modéliser par une loi uniforme sur l'ensemble des évènements possibles.

La figure 1.1 représente un algorithme randomisé très simple pour illustrer notre modélisation. Lorsque plusieurs transition sont possibles dans un état donné, le réel compris entre 0 et 1 qui étiquette une transition représente la probabilité avec laquelle cette transition sera parcourue. Lorsqu'aucune indication ne figure sur une transition, celle-ci sera franchie avec probabilité 1 (c'est donc le cas quand une unique transition est possible). Dans l'état initial I on tire à pile ou face pour savoir quel état sera le successeur. Avec probabilité $\frac{1}{2}$ on passe dans l'état 1 et avec probabilité $\frac{1}{2}$ on atteint l'état 0.

La randomisation permet dans certains cas d'améliorer la complexité des algorithmes et même parfois de trouver des solutions à des problèmes qui n'acceptent aucune solution déterministe.

Le système de transition modélisant l'algorithme randomisé est une chaîne de Markov (les définitions formelles sont données au chapitre 4). Il a pour principale propriété que la somme des probabilités figurant sur l'ensemble des arêtes sortantes d'un état vaut 1.

Dans l'exemple ci-dessus, il est aisé de démontrer que « presque toutes » les exécutions du systèmes visitent infiniment souvent l'état acceptant 1. En revanche si on considère le système non déterministe obtenu en ignorant les probabilités, il est faux que toutes les exécutions visitent – ne serait-ce qu'une fois – l'état 1.

Modélisation de pannes. Grâce aux probabilités, on peut aussi modéliser des pannes ou des comportements défaillants en tenant compte du temps

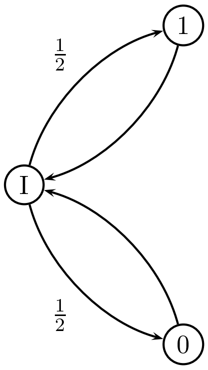


FIG. 1.1 – Système de transition pour un exemple d'algorithme randomisé.

moyen qui s'écoule entre une mise en service et une panne ou compte tenu de l'expérience, en estimant la probabilité qu'à chaque instant une défaillance apparaisse.

À titre d'exemple on considère un local éclairé par 2 ampoules, une à incandescence et une à halogène de durées de vie moyennes respectives 1200 et 2000 heures. On estime que le temps moyen nécessaire au changement d'une ampoule est de 5 minutes. Cette situation peut être modélisée par le système de transition de la figure 1.2.

Lorsque les deux ampoules fonctionnent correctement, on se trouve dans l'état initial `ok`. Au moment ou l'ampoule halogène (resp. à incandescence) cesse de fonctionner on passe dans l'état 1 (resp. 2). L'état 1&2 correspond à la situation où les deux ampoules ne fonctionnent pas. La durée qui étiquette une transition correspond au temps moyen de franchissement de cette transition. On modélise la loi de probabilité du franchissement d'une transition par une loi de Poisson du type $1 - \exp(-\frac{t}{\lambda})$ où λ est la durée moyenne et t le temps écoulé dans l'état courant. À chaque instant t, la probabilité que la transition ait été franchie avant est $1 - \exp(-\frac{t}{\lambda})$.

À l'aide de cette modélisation, on peut chercher à calculer le temps moyen passé dans l'état défaillant 1&2 où les deux ampoules sont en panne. On peut également calculer la probabilité que l'ampoule à halogène tombe en panne avant l'ampoule à incandescence lorsqu'on se trouve dans l'état initial `ok`.

Modélisation du non-déterminisme. On peut encore modéliser le comportement de l'utilisateur du système ou de l'environnement quand il n'est pas déterministe. On utilise pour cela des systèmes de transition ayant deux types d'états, des états probabilistes (représentés par des ronds) et des états non-déterministes (entourés de carrés). Ce type de système de transition est appelé processus de décision markovien (voir le chapitre 3) pour une définition formelle).

La figure 1.3 représente un gestionnaire de ressource partagée par deux

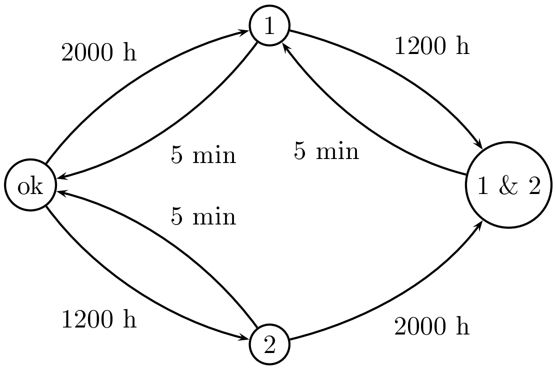


Fig. 1.2 – Exemple de modélisation de pannes

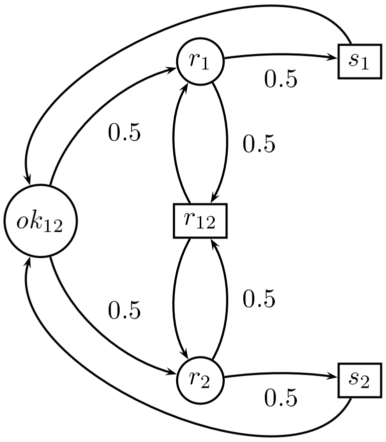


Fig. 1.3 – Exemple de système probabiliste et non-déterministe

utilisateurs appelés 1 et 2. Dans l'état ok_{12} aucun des utilisateurs n'a demandé accès à la ressource commune. Dans l'état probabiliste r_1 (resp. r_2), l'élément 1 (resp. 2) a fait une requête pour utiliser la ressource. Ces requêtes doivent être prises en compte par un environnement extérieur à 1 et2. Dans l'état r_{12} où les deux participants ont fait une requête, il doit choisir lequel de 1 ou 2 il satisfera. Les états non-déterministes s_1 et s_2 pourraient aussi bien être probabilistes car il n'y a pas de choix possible pour l'environnement. On a pourtant choisi de les considérer non-déterministes puisqu'ils représentent un état dans lequel l'environnement doit agir. Dans cet exemple, quels que soient les choix de l'extérieur, les requêtes seront satisfaites « un jour » (au sens de "eventually"). Ceci n'étant pas vrai si on retire l'aspect probabiliste.

Ces nombreuses situations d'application justifient l'étude des systèmes stochastiques.

1.2 Systèmes communicant par des canaux non fiables

1.2.1 Présentation

Un système à canaux non fiables est constitué de processus communicants par des canaux FIFO sur lesquels ils écrivent et lisent des messages. Si les canaux ne sont pas parfaits et peuvent perdre des messages, on parle de canaux non fiables. Les pertes de messages s'effectuent de façon non-déterministe. Ces systèmes permettent de modéliser des protocoles de communication asynchrones sensés fonctionner même en cas de pertes de messages tels que le protocole du bit alterné ou le protocole BRP, etc... Les processus considérés sont à espace d'états fini. La taille des canaux étant non bornée, on obtient pourtant un système global à espace d'états infini ce qui rend la vérification moins aisée.

1.2.2 Vérification des systèmes à canaux non fiables

La vérification de systèmes infinis demande plus d'efforts que celle des systèmes finis car la plupart des problèmes intéressants de vérification sont alors indécidables. C'est le cas pour la classe des systèmes communicants par des canaux parfaits [BZ83], ce modèle pouvant simuler une machine de Turing. Des méthodes de vérification ont cependant été établies pour cette classe de systèmes mais l'indécidabilité des problèmes empêche toute méthode automatique et générale. Dans le cas de systèmes communicants par des canaux non fiables, plusieurs problèmes intéressants de vérification sont décidables [CFI96] [AJ96b]. Plus précisément, des algorithmes sont établis pour vérifier les propriétés suivantes :

- Le problème d'accessibilité : Un ensemble d'états est-il accessible depuis un autre état du système ?
- Des propriétés de sûreté : Un système vérifie-t-il une propriété de sûreté sur les traces ?

D'autres problèmes ont été prouvés indécidables [AJ96a]. C'est le cas du problème de model-checking vis-à-vis des logiques temporelles telles que LTL ou

CTL et de la vérification de propriétés de vivacité lorsque le comportement satisfait des hypothèses d'équité.

1.2.3 Pertes stochastiques

Nous l'avons vu, plusieurs problèmes intéressants sont indécidables pour les systèmes communicants par des canaux à pertes non déterministes. De plus, une modélisation des pertes par une loi de probabilité permettrait de se rapprocher de la réalité. Le modèle probabiliste décrit bien les pannes : il est plus précis que le non-déterminisme ; de plus la notion d'indépendance des pannes entre elles est conservée. En outre, sous des hypothèses probabilistes, on retrouve l'espoir de décider la vivacité, et on peut se contenter de prouver la vivacité avec probabilité 1.

La notion de système à canaux à pertes stochastiques a été introduite dans [PN97] puis reprise dans [BE99] et [ABPJ00]. Dans ces articles, la probabilité de perte est une constante $\mathcal{P}$: dans chaque état global du système la probabilité qu'un message soit perdu dans un canal est $\mathcal{P}$. Les autres actions (écriture ou lecture sur un canal, action interne) sont munies d'un poids qui induit une loi de probabilité et engendre une chaîne de Markov sur les états globaux du système. Cette chaîne de Markov sera très souvent infinie. Iyer et Narasimha s'intéressèrent à la satisfaction d'une formule de LTL avec probabilité supérieure à p et une tolérance ϵ [PN97]. Dans [BE99], Baier et Engelen ont considéré le problème suivant : Étant donné un système à canaux à pertes stochastiques $\mathcal{L}$ et une formule de LTL Φ, l'ensemble des exécutions dans $\mathcal{L}$ qui satisfont Φ est-il de mesure 1 ? Lorsque la probabilité de perte est « suffisamment grande », le problème de model-checking peut se réduire à un problème d'accessibilité dans le système à canaux parfaits sous-jacent, lui même décidable [AJ96a]. Malheureusement, la restriction « suffisamment grande » signifie à peu près supérieure à $\frac{1}{2}$ [1]. Plus tard, Abdulla, Baier, Iyer et Jonsson montrent que sans l'hypothèse de probabilité de perte suffisamment grande, le model-checking de propriétés de vivacité avec probabilité 1 est indécidable [ABPJ00].

Notre contribution. Le résultat de [BE99] est difficilement appliquable en pratique car les pertes de messages lors d'un protocole de communication par exemple ont une probabilité bien inférieure à $\frac{1}{2}$. En outre, le fait que la probabilité de perte ne dépende pas du nombre de messages présents dans les canaux nous semble éloigné de la réalité. En effet, on constate en pratique que les pertes de messages sont plus fréquentes lorsque les canaux sont chargés plutôt que lorsqu'ils sont presque vides. Il apparaît donc intéressant de chercher une nouvelle définition des pertes reflétant mieux la réalité. On a ainsi l'espoir de démontrer la décidabilité du model-checking indépendamment de la probabilité de perte.

Notre contribution sera donc de donner un nouveau modèle pour les pertes stochastiques dans les canaux de communications. Ce modèle attache à chaque message un taux de perte constant. Lorsque plusieurs messages sont dans le canal, les taux s'additionnent et ainsi la probabilité de perte augmente avec le nombre de messages. Cette définition implique également que la probabilité de perte d'un message particulier augmente avec le temps qu'il passe dans le canal.

[1] En réalité la borne dépend des poids affectés dans chaque état aux différentes actions possibles mais elle peut être majorée dans tous les cas par $\frac{1}{2}$.

Notre but est de donner avec cette définition des résultats indépendants du taux de perte, voire même valables lorsque ce taux est inconnu.

1.3 Vérification des processus stochastiques : des rappels

Pour le model-checking classique, si ϕ est une formule de logique temporelle et M une structure de Kripke, on cherche à savoir si M vérifie ϕ (noté $M \vDash \phi$) c'est-à-dire si toutes les exécutions possibles dans M vérifient ϕ. Dans le cas des chaînes de Markov et des processus de décision markoviens, cette question ne fait pas intervenir les probabilités. On se demandera donc plutôt si l'ensemble des chemins vérifiant ϕ est de mesure 1 ou non. On cherche à savoir si la propriété exprimée par ϕ est vraie pour presque toutes les exécutions dans la chaîne de Markov ou dans le processus de décision markovien. On notera $M \vDash_{p=1} \phi$ pour signifier que la chaîne de Markov M vérifie ϕ avec probabilité 1.

Pour les processus de décision markoviens on spécifie les choix faits aux états non-déterministes par une fonction associant un successeur à chaque séquence finie aboutissant dans un état non-déterministe. Cette fonction est appelée *adversaire*. Lorsqu'il y a à la fois des états probabilistes et des états non-déterministes, la notion de $M \vDash_{p=1} \phi$ dépend des choix non-déterministes, c'est-à-dire de l'adversaire. On cherchera alors à démontrer que ϕ est vérifiée avec probabilité 1 et ce, quel que soit l'adversaire. Ainsi, même dans le cas d'un adversaire « pire », la propriété sera vraie presque sûrement. Ce dernier problème est plus compliqué que le précédent et non trivial [Var85] [CY95]. Il est très interessant car on peut modéliser de nombreux systèmes réels par des processus de décision markoviens : l'environnement est probabiliste et le comportement du système non-déterministe. Des variantes de ce problème consistent par exemple à se restreindre à des adversaires « déterministes » [2]. On peut également s'intéresser à *l'existence* d'un adversaire pour lequel ϕ est vérifiée presque partout.

L'approche que nous avons considérée à l'instant est *qualitative* car on ne cherche pas à calculer la valeur exacte de la probabilité avec laquelle une formule est vérifiée mais on veut seulement savoir si cette probabilité est 1 ou non. Une autre approche, *quantitative*, cherche à calculer exactement la probabilité. Étant données une chaîne de Markov M et une formule de LTL ϕ, il peut être intéressant de calculer la mesure de l'ensemble des exécutions de M qui vérifient ϕ. Pour les processus de décision markoviens, il est nécessaire de fixer l'adversaire pour calculer la mesure de l'ensemble qui vérifie ϕ. On peut alors rechercher les adversaires qui donnent respectivement la plus petite et la plus grande probabilité pour déterminer l'intervalle de probabilité $[p_{min}, p_{max}]$, p_{min} correspondant à l'adversaire le pire et p_{max} au meilleur adversaire possible.

1.4 Plan

Dans une première partie, nous introduirons les chaînes de Markov en rappelant les notions nécessaires de théorie des probabilités. La deuxième partie sera consacrée aux processus de décision markovien, généralisation des chaînes

[2] ou plus exactement ne dépendant que de l'état de contrôle et aucunement de l'historique des états visités

de Markov dans le cas de non-déterminisme mêlé au côté stochastique. Nous exposerons ensuite les résultats obtenus pour les systèmes à canaux à pertes stochastiques (avec notre définition de perte) dans le cas des chaînes de Markov. La quatrième et dernière partie relatera les résultats concernant les processus de décision markoviens.

Après avoir donné notre nouvelle définition nous montrons la décidabilité du model-checking pour les systèmes à canaux à pertes stochastiques ayant un nombre fini ou dénombrable d'états de contrôle. Ce résultat est comme on l'espérait indépendant du taux de perte et ne nécessite pas la connaissance de ce dernier. Nous considérons ensuite le problème des systèmes à la fois stochastiques et non-déterministes. Dans ce cas, le problème «Une propriété Φ est elle vérifiée avec probabilité 1 quelque soit l'adversaire» est indécidable. Nous le montrerons par une réduction du problème : un système à canal non fiable est-il borné ou non ?

Chapitre 2

Chaînes de Markov

Dans cette section, nous allons introduire formellement la notion de chaîne de Markov en rappelant quelques bases de la théorie de la mesure. Nous nous appuyons pour cela sur le travail de Panangaden [Pan01] et également sur des ouvrages de probabilités [Nor98] [Bré99].

Nous montrerons ensuite comment appliquer ces définitions aux systèmes stochastiques.

2.1 Définitions

Nous commençons par introduire la notion d'espace mesurable. Intuitivement, une mesure permet de définir la taille d'un objet dans un ensemble donné. Les principales difficultés rencontrées -et qui semblent aller contre l'entendement- sont qu'il existe des ensembles non mesurables (une mesure étant fixée) et que certains ensembles mesurables non vides sont pourtant de mesure nulle. Le cas discret n'offre pas ces "bizarreries" mais dès qu'on s'intéresse aux ensembles infinis, les exemples sont nombreux. Le cas discret ne suffit pas pour étudier les systèmes stochastiques. En effet, même dans un graphe fini, l'ensemble des chemins est non dénombrable. Nous devons donc nous plonger dans le domaine des ensembles infinis non dénombrables.

2.1.1 Mesure

Définition 2.1 *Soit E un ensemble et Σ une famille de sous-ensembles de E. Σ est une* σ-algèbre *sur E si les trois axiomes suivants sont vérifiés :*

1. $\emptyset \in \Sigma$,
2. $A \in \Sigma \Rightarrow A^c (= E \setminus A) \in \Sigma$,
3. *Si I est un ensemble dénombrable d'indices et si $\forall i \in I,\ A_i \in \Sigma$ alors,* $\bigcup_{i \in I} A_i \in \Sigma$.

Dans ce cas, (E, Σ) sera appelé espace mesurable.

Exemples Soit E un ensemble fixé.

– $\{\emptyset,\ E\}$ est trivialement une σ-algèbre sur E.

- $\mathcal{P}(E)$, la collection des parties de E est également une σ-algèbre. Entre ces deux cas extrémaux, il existe une variété immense de σ-algèbres.
- Si E est non-dénombrable, la collection de tous ses sous-ensembles dénombrables ou de complémentaire dénombrable forme une σ-algèbre sur E.
- Si E est un espace topologique, c'est-à-dire muni d'une topologie $\mathcal{T}$, la σ-algèbre borélienne $\mathcal{B}(E)$ est engendré par les ouverts de $\mathcal{T}$: c'est la plus petite σ-algèbre contenant tous les ouverts de $\mathcal{T}$.

À présent que les espaces mesurables sont définis, nous pouvons définir les fonctions mesurables en utilisant des images inverses comme c'est le cas pour la continuité.

Définition 2.2 *Soient (E, Σ_E) et (F, Σ_F) deux espaces mesurables et $f : (E, \Sigma_E) \to (F, \Sigma_F)$ une fonction. f est dite* mesurable *si $\forall B \in \Sigma_F,\ f^{-1}(B) \in \Sigma_E$.*

Nous l'avons dit, la définition de la mesurabilité des fonctions ressemble à celle de la continuité puisqu'elles se basent toutes les deux sur la notion d'image inverse. Cependant, contrairement à ce qui se passe pour la continuité, la limite point à point d'une suite de fonctions mesurables est elle-même mesurable. Ceci tient au fait que les ouverts ne sont pas stables par intersection dénombrable alors que les ensembles mesurables le sont.

Nous allons maintenant introduire la notion fondamentale de "mesure". Comme nous l'avons dit précédemment, la mesure est intuitivement l'attribution d'un réel à des ensembles, reflétant leur taille. Plus précisément, nous allons définir une mesure sur les éléments d'une σ-algèbre.

Définition 2.3
1. *Une* mesure*, μ sur un espace mesurable (E, Σ) est une fonction de Σ dans $[0, +\infty]$ vérifiant la propriété de* σ-additivité *c'est-à-dire telle que pour toute famille dénombrable $\{A_i,\ i \in I\}$ d'ensembles deux à deux disjoints, $\mu(\bigcup_{i \in I} A_i) = \sum_{i \in I} \mu(A_i)$.*
2. *Une* mesure de probabilité *est une mesure de Σ dans $[0, 1]$.*

Remarque 2.4
- *On note fréquemment les mesures de probabilité $\mathbb{P}$ à la place du μ général.*
- *Puisque $\emptyset = \emptyset \cup \emptyset$, la mesure de probabilité de l'ensemble vide est nulle, et ce quelle que soit $\mathbb{P}$.*
- *On remarque aussi que pour toute mesure de probabilité $\mathbb{P}$ sur (E, Σ), si on suppose qu'elle est surjective sur $[0, 1]$, alors $\mathbb{P}(E) = 1$.*

Un ensemble de mesure nulle est appelé *ensemble négligeable.* Lorsque $\mathbb{R}$ est muni de la σ-algèbre borélienne $\mathcal{B}(\mathbb{R})$, tous ses ensembles dénombrables sont négligeables. Ce sera également le cas pour nos ensembles de chemins. En effet, l'ensemble des mots infinis sur un alphabet fixé (de deux lettres au moins) est en bijection avec $\mathbb{R}$ et les ensembles de mots ayant un préfixe commun correspondent aux ouverts de base.

Tout d'abord, tout alphabet de cardinal strictement supérieur à 2 peut être remplacé par l'alphabet $[0, 1]$ en codant les différentes lettres de l'alphabet de départ par une suite de 0 et en séparant les différentes lettres d'un mot par un 1. Ensuite, l'ensemble des mots infinis sur $\{0, 1\}$ est de même cardinal que le fermé $[0, 1]$ qui est lui même du cardinal de $\mathbb{R}$ c'est-à-dire $\aleph_1$. L'intervalle $[0, 1]$

s'injecte trivialement dans $\mathbb{R}$ et on peut construire une injection de $\mathbb{R}$ dans $[0,1]$ comme suit. Si x est un réel de partie entière $n = n_1 \cdots n_k$ et de décimales $x_1,\ x_2, \cdots$ alors on lui associe $0, n_1 x_1 \cdots n_k x_k 0 x_{k+1} \cdots$ qui est un réel de $[0,1]$. Ainsi, $[0,1]$ est de cardinal $\aleph_1$

On considérera des cônes, c'est-à-dire les mots ayant un préfixe fini commun. Ces cônes correspondent à des ouverts de $[0,1]$ car les décompositions des réels qui sont dans un même ouvert de $[0,1]$ sont identiques au début, et ce préfixe commun est plus long lorsque la taille de l'ouvert diminue.

Ainsi on peut faire une analogie entre $\mathbb{R}$ est l'ensemble des mots sur un alphabet de cardinal au moins 2 tant sur le cardinal que sur les σ-algèbres dont on les dote. Alors, nous aurons comme dans le cas de $\mathbb{R}$ muni de sa σ-algèbre borélienne de nombreux ensembles non vides négligeables.

On dira que l'événement A est vrai "*presque partout*" ou "*presque sûrement*" s'il existe un ensemble négligeable N tel que A soit vrai sur $E \setminus N$.

Dans la suite, sauf mention du contraire, les ensembles considérés seront toujours mesurables.

Enfin, nous allons énoncer une propriété utile par la suite pour déterminer la mesure de la limite d'une suite croissante d'ensembles mesurables.

Proposition 2.5 *Monotonie et Continuité : Soit* (E, Σ) *un espace mesurable.*

1. *Si* $A \subset B$*, alors* $\mu(A) \leq \mu(B)$
2. *Si* $(A_i)_{i\in\mathbb{N}}$ *est une suite croissante d'ensembles, c'est-à-dire* $A_1 \subset A_2 \subset \cdots \subset A_n \subset A_{n+1} \cdots$*, alors* $\lim_{i\to\infty} \mu(A_i) = \mu(\bigcup_{i\in\mathbb{N}} A_i)$.
3. *Symétriquement, si* $(A_i)_{i\in\mathbb{N}}$ *est une suite décroissante d'ensembles, c'est-à-dire* $A_1 \supset A_2 \supset \cdots \supset A_n \supset A_{n+1} \cdots$*, alors* $\lim_{i\to\infty} \mu(A_i) = \mu(\bigcap_{i\in\mathbb{N}} A_i)$.

Cette propriété est utile pour déterminer la mesure d'un ensemble qu'on approxime par suite croissante ou décroissante.

Probabilités conditionnelles Dans le cas discret, les probabilités conditionnelles se définissent aisément de la façon suivante : si $\mathbb{P}$ est une mesure de probabilité et A et B deux événements de l'univers, alors la probabilité de "A sachant B" [1], notée $\mathbb{P}(A|B)$ est donnée par

$$\mathbb{P}(A|B) = \frac{\mathbb{P}(A)}{\mathbb{P}(B)}.$$

Cette définition n'a de sens que si $\mathbb{P}(B)$ est non nulle.

Lorsqu'on sort du cas discret, tout devient plus compliqué, en partie du fait que cette fois-ci, "beaucoup d'ensembles" sont de mesure nulle. Alors, la définition donnée plus haut doit être plus subtile.

L'idée intuitive permettant de définir une probabilité conditionnelle lorsque B est un ensemble négligeable est de l'approcher par une suite décroissante d'ensembles de mesure non nulle. Si $(B_i)_{i\in\mathbb{N}}$ est une suite décroissante d'ensembles - c'est-à-dire $B_1 \supset B_2 \supset \cdots \supset B_n \cdots$ - vérifiant $\bigcap_{i\in\mathbb{N}} B_i = B$ et telle que $\forall i \in \mathbb{N},\ \mathbb{P}(A|B_i)$ est définie alors on pose $\mathbb{P}(A|B) = \lim_{i\to\infty}\ \mathbb{P}(A|B_i)$.

Nous ne donnons pas la définition formelle des probabilités conditionnelles dans le cas continu car elle ne sera pas utile par la suite.

[1] Plus précisément, la probabilité que A soit vrai sachant que B est vrai.

On note $(\Omega,\ \mathcal{F},\ \mathbb{P})$ un espace de probabilité. Ω est un ensemble appelé univers muni d'une σ-algèbre $\mathcal{F}$ et d'une mesure de probabilité $\mathbb{P}$.

2.1.2 Chaînes de Markov

Les notions de variable aléatoire et probabilités conditionnelles sont nécessaires pour définir les chaînes de Markov.

Définition 2.6 *Une* variable aléatoire *E sur un espace de probabilité $(\Omega,\ \mathcal{F},\ \mathbb{P})$, est une fonction mesurable de Ω dans $\mathbb{R}$ muni de la σ-algèbre borélienne.*

Nous voici à présent prêts à introduire les chaînes de Markov qui sont un cas particulier de processus stochastiques.

Définition 2.7 *Soit $(\Omega,\ \mathcal{F},\ \mathbb{P})$ un espace de probabilité. Un* processus stochastique à temps discret *à valeurs dans l'espace d'état E, est une famille de variables aléatoires indexée par $\mathbb{N}$: $\forall n \in \mathbb{N},\ X_n :\ \Omega \to E$*

Définition 2.8 *Un processus stochastique $(X_n)_{n\in\mathbb{N}}$ à temps discret et à espace d'états dénombrable E est une* chaîne de Markov *si pour tout entier $n \geq 0$ et tous états $i_0, i_1,\ ..., i_{n-1}, i, j$,*

$$\mathbb{P}(X_{n+1} = j | X_n = i,\ X_{n-1} = i_{n-1},\ ...,\ X_0 = i_0) = \mathbb{P}(X_{n+1} = j | X_n = i) \quad (2.1)$$

à chaque fois que les deux membres sont bien définis.

La propriété (2.1) est appelée *propriété de Markov*.

On dit qu'une chaîne de Markov est *homogène* et on parle alors de HMC lorsque pour tous états $i,\ j \in E$, $\mathbb{P}(X_{n+1} = j | X_n = i)$ est indépendant de n.

Remarque 2.9 *Une chaîne de Markov est donc un processus stochastique qui évolue uniquement en fonction du dernier état visité et non pas en considérant tout l'historique. On peut donc comparer le cas particulier des chaînes de Markov dans les processus stochastiques à celui des jeux à stratégies gagnantes sans mémoire dans les stratégies gagnantes des jeux déterminés.*

Lorsqu'une chaîne de Markov est homogène, ce qui sera le cas dans la suite, on appelle *matrice de transition* la matrice $\mathbf{P} = (p_{ij})_{i,j\in E}$ où $p_{ij} = \mathbb{P}(X_{n+1} = j | X_n = i)$.

On peut alors facilement passer de la matrice de transition à un système de transition la représentant. Il suffit de prendre comme états les états de E et d'étiqueter l'arête de i à j par p_{ij}. Chaque étiquette est donc un réel compris entre 0 et 1 et pour tout état $i \in E$, la somme des étiquettes sortantes est 1.

Inversement, si on se donne un graphe orienté d'ensemble de sommets E, dont les arêtes sont étiquetées dans $[0, 1]$ et qui vérifie que pour tout sommet, la somme des étiquettes sortantes est 1, on peut construire une chaîne de Markov homogène de matrice de transition $\mathbf{P} = (p_{ij})_{i,j\in E}$ où p_{ij} est l'étiquette de l'arête partant de i et pointant vers j. La distribution initiale X_0 de la chaîne de Markov est déterminée grâce aux états initiaux.

Dans le cas homogène, voici donc une définition équivalente :

Définition 2.10 *Une* chaîne de Markov *est un triplet* $M = (X, P, P_0)$ *où* X *est un ensemble dénombrable* [2] *d'états ;* $P : X \times X \to [0,1]$, *une fonction de probabilité de transition vérifiant* $\forall x \in X,\ \sum_{y \in X} P(x,y) = 1$ *;* $P_0 : X \to [0,1]$ *une distribution de probabilité initiale telle que* $\sum_{x \in X} P_0(x) = 1$.

Remarque 2.11 *Cette définition implique en particulier que tout état possède au moins un successeur. Si dans le système à modéliser ce n'est pas le cas, on augmente les états sans successeurs d'une boucle de probabilité* 1.

2.2 Vérification

Une chaîne de Markov n'est donc rien d'autre pour nous qu'un graphe orienté dont les arêtes sont étiquetées par des règles précises : la somme des étiquettes sortantes est 1 pour chaque état du système.

Soit $M = (X, P, P_0)$ une chaîne de Markov.

On dit que $x_0 \in X$ est un état initial de M lorsque $P_0(x) > 0$.

De $\forall x \in X,\ \sum\limits_{y \in X} P(x,y) = 1$ on déduit que tout état de X admet au moins un successeur. Ainsi, tout chemin fini dans M peut être prolongé.

Une exécution du système est un chemin infini dans le système de transition qui le représente.

Définition 2.12 *Un mot infini* $U = q_0 \cdot q_1 \cdots q_n \cdots$ *sur* X *est une* exécution [3] *si* $\forall i \in \mathbb{N},\ P(q_n, q_{n+1}) > 0$ *et* $P_0(q_0) > 0$.

Pour vérifier les chaînes de Markov nous avons besoin d'introduire une mesure sur l'ensemble des chemins d'un système de transition stochastique. Cette mesure est définie sur des cônes, c'est-à-dire des ensembles de chemins qui ont un préfixe fini commun. Si w est un mot fini sur X, $[w] = \{U \text{ run} \mid w \text{ préfixe de } U\}$ est le cône élémentaire engendré par w. La mesure de $[w]$ est donnée par $P_0(w_0) \cdot P(w_0, w_1) \cdots P(w_{n-1}, w_n)$ si $w = w_0 \cdot w_1 \cdots w_{n-1} \cdot w_n$. Cette mesure est alors prolongée de façon unique à une mesure sur la σ-algèbre engendrée par les cônes élémentaires, qui définit donc les ensembles mesurables d'exécutions. Soit $U = q_0 \cdot q_1 \cdots q_n \cdots$ une exécution dans une chaîne de Markov M. On appelle *suite des probabilités de* U la suite de premier terme $a_0 = P_0(q_0)$ et de terme général $a_n = P(q_{n-1}, q_n)$. Lorsque la suite des probabilités d'une exécution n'est pas de la forme $f_0 \cdot 1^\omega$, c'est-à-dire constituée uniquement de 1 après une suite finie f_0, la mesure du singleton associé à ce chemin est nulle. Toute union dénombrable d'ensembles de mesure nulle est mesurable et de mesure nulle. Il existe donc souvent des ensembles non vides de mesure nulle.

Avant même de se poser la question de la mesure d'un ensemble de runs, il faudra se demander s'il est mesurable. Comme les cônes sont les seuls ensembles que nous savons être mesurables, il faudra partir d'eux et à l'aide de complémentaires et d'unions dénombrables atteindre l'ensemble à étudier pour montrer qu'il est bien dans la σ-algèbre.

Remarque 2.13 *Parfois, on ajoute une composante à la définition de la chaîne de Markov pour étiqueter les états. Une fonction* $L : X \to 2^{AP}$ *est définie, où*

[2] C'est-à-dire fini ou infini dénombrable.
[3] ou un “run”

AP est un ensemble de propositions atomiques. On parle dans ce cas de chaîne de Markov « étiquetée ». Nous n'avons pas mentionné la fonction d'étiquetage dans la définition 2.10 car il est possible de coder dans le nom des états les propositions atomiques qui y sont vraies.

Notations Soit M une chaîne de Markov d'ensemble d'états X et $x \in X$. On note $Path(x)$ l'ensemble des exécutions dans M partant de x.

Définition 2.14 *Soit Φ une formule de LTL et M une formule de LTL. On suppose que l'ensemble des propositions atomiques présentes dans Φ est inclus dans l'ensemble des propositions atomiques qui étiquette M.*

On dit qu'une exécution $U = x_0 \cdot x_1 \cdots$ dans M vérifie Φ si $L(x_0) \cdot L(x_1) \cdots \models \Phi$.

On dit que M vérifie Φ avec probabilité $p \in [0,1]$ si l'ensemble des chemins infinis dans M commençant dans un état initial et vérifiant la formule Φ est de mesure p.

On dit que M vérifie Φ (sans préciser la probabilité) et on note $M \models \Phi$ si M vérifie Φ avec probabilité 1.

Nous présentons maintenant un résultat classique de mesurabilité exposé par Vardi dans [Var85].

Théorème 2.15 *Soit $M = (X, P, P_0)$ une chaîne de Markov et L une fonction d'étiquetage des états de M dans 2^{AP}. Soit $\mathcal{A}$ un automate de Büchi sur 2^{AP}. $L_\omega(\mathcal{A})$ désigne l'ensemble des mots infinis acceptés par $\mathcal{A}$. Alors l'ensemble $\Delta(\mathcal{A}) = \{U \in Path(M) | L(U) \in L_\omega(\mathcal{A})\}$ est mesurable.*

Démonstration Les automates de Büchi n'ont pas toujours d'équivalent déterministe. Nous allons donc passer par les automates de Rabin dont le pouvoir d'expression est le même que celui des automates de Büchi et qui peuvent être déterminisés.

Soit donc $\mathcal{R}$ un automate de Rabin déterministe qui accepte le même langage que $\mathcal{A}$: $L_\omega(\mathcal{A}) = L_\omega(\mathcal{R})$.

La condition d'acceptation de $\mathcal{R}$ peut être exprimée à l'aide de d'une disjonction $\bigvee_{i=1}^{n} \Box\Diamond a_i \wedge \Diamond\Box b_i$ où les a_i et b_i sont des sous-ensembles de 2^{AP}. Dans la démonstration on vérifiera la mesurabilité pour une de ces disjonctions c'est-à-dire avec la formule $f = \Box\Diamond a \wedge \Diamond\Box b$.

Nous allons maintenant montrer que chacun des ensembles de chemins vérifiant une formule de la conjonction f est mesurable.

On note A l'ensemble des états x de M tels que $a \in L(x)$: $A = \{x \in X | a \in L(x)\}$. Symétriquement, $B = \{x \in X | b \in L(x)\}$.

Soit Ω_n pour $n \in \mathbb{N}$ l'ensemble des exécutions dans M qui visitent au moins n fois A. L'ensemble des chemins le long desquels a est vraie infiniment souvent est l'intersection dénombrable Ω_∞ de tous les ensembles Ω_n. Si pour tout $n \in \mathbb{N}$ on montre que Ω_n est mesurable, la stabilité par intersection dénombrable de la σ-algèbre impliquera que Ω_∞ est aussi mesurable.

Soit $n \in \mathbb{N}$ et x_0 un état initial de M. On peut construire une suite dénombrable $(w_j)_{j \in \mathbb{N}}$ de chemins finis dans M de longueurs croissantes tels que pour tout j, w_j commence en x_0 et visite exactement n fois A et s'arrête en un état de A. Le cône engendré par w_j est un ensemble mesurable, c'est un ouvert élémentaire de la σ-algèbre. Puis, comme $\Omega_{n,x_0} = \bigcup_{j\in\mathbb{N}}[w_j]$, Ω_{n,x_0} est mesurable comme union dénombrable d'ensembles mesurables.

S'il y a plusieurs états initiaux dans M, on fait l'union (finie ou infinie dénombrable) des Ω_{n,x_0} sur l'ensemble des états initiaux pour obtenir que Ω_n est mesurable.

Enfin, la stabilité des σ-algèbres par intersection dénombrable nous permet d'affirmer que $\Omega_\infty = \bigcap_{n\in\mathbb{N}} \Omega_n$ est mesurable. $\square$

Puisque l'ensemble des mots acceptés par $\mathcal{A}$ est identique à celui de $\mathcal{B}$, on a donc prouvé le théorème, à savoir qu'un ensemble d'exécutions accepté par Büchi est mesurable.

2.3 Premiers résultats

Nous allons démontrer ici des résultats généraux sur les chaînes de Markov qui nous seront utiles dans les chapitres suivants.

Soit $M =< W, P, P_0, L >$ une chaîne de Markov étiquetée, d'ensemble d'états W, de fonction de probabilité de transition P, de distribution initiale P_0 et ayant pour fonction d'étiquetage L.

On suppose qu'un état $q_0 \in W$ est visité infiniment souvent avec probabilité 1. On suppose également qu'il existe une portion de trajectoire $q_{0,n} = q_0 \to q_1 \cdots \to q_n$ dans M, vérifiant $\forall j,\ 0 \leq j \leq n-1,\ P(q_i, q_{i-1}) > 0$. On notera $\pi \vDash q_{0,n}$ si l'exécution π parcourt le chemin $q_{0,n}$.

Lemme 2.16 $Prob(\Box\Diamond q_{0,n} | \Box\Diamond q_0) = 1$

Démonstration On cherche à montrer que presque toutes les exécutions empruntent une infinité de fois le chemin $q_{0,n}$.

On pose $p = \prod_{j=0}^{n-1} P(q_i, q_{i-1})$. Partant de q_0, avec probabilité $1-p$, on réatteint pour la première fois q_0 sans avoir emprunté la branche $q_0\ q_1 \cdots\ q_n$. En effet, partant de q_0 comme de q_n, la probabilité d'atteindre q_0 est 1.

$$Prob(\{\pi \in Path(q_0),\ \pi \vDash q_{0,n} | \pi \vDash \bigcirc\Diamond q_0\}) = Prob(\{\pi \in Path(q_0),\ \pi \vDash q_{0,n}\}) = 1-p$$

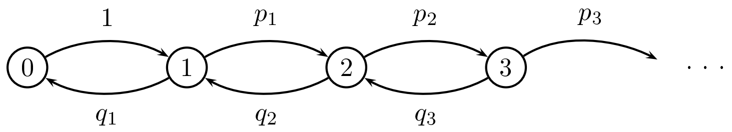
Pour emprunter un nombre fini de fois le chemin $q_{0,n}$, il faut l'éviter un nombre infini de fois. L'ensemble des chemins qui évite une fois $q_{0,n}$ est de mesure $1-p$. En itérant ce résultat, l'ensemble des chemins qui évitent k fois $q_{0,n}$ est de mesure $(1-p)^k$. Puisque p non nul, $1-p$ est strictement inférieur à 1. Alors, lorsque k tend vers l'infini, la mesure des chemins qui évitent k fois $q_{0,n}$ tend vers 0. On a donc établi le fait que la mesure des chemins qui visitent infiniment souvent q_0 et seulement finiment souvent le chemin $q_{0,n}$ est négligeable. $\square$

On utilisera fréquemment ce lemme qui peut se traduire par : on ne peut pas éviter infiniment souvent une série de transitions infiniment souvent possible.

Voici à présent un autre résultat sur un certain type de chaînes de Markov, les marches aléatoires sur $\mathbb{N}$.

Notations et hypothèses

On considère un ensemble dénombrable d'états I. À chaque état indexé par un entier i, on associe une probabilité p_i de passer à l'état $i+1$ (écriture d'un message dans un des canaux) et une probabilité q_i d'aller dans l'état $i-1$ (lecture d'un message ou perte).



On suppose qu'il existe un entier k tel que :

$$\forall n \geq k, q_n \geq \frac{1}{2} \ et \ p_n \leq \frac{1}{2}.$$

Soit i un entier fixé. Nous allons montrer que l'ensemble des chemins [4] issus de i qui visitent infiniment souvent 0 est de mesure 1. On est donc toujours forcé de revenir dans l'état 0.

Lemme 2.17 $\mathbb{P}(\{\pi \in \mathrm{Path}(i),\ \pi \vDash \Box\Diamond 0\}) = 1$

Démonstration Nous allons effectuer cette démonstration en plusieurs temps. Tout d'abord, nous allons prouver la mesurabilité de l'ensemble des chemins issus de i qui visite infiniment souvent 0. Nous calculerons ensuite la mesure de cet ensemble pour montrer qu'elle vaut 1.

Mesurabilité Commençons par montrer qu'il est mesurable pour la mesure de chemins que l'on s'est fixée. Il suffit pour cela d'utiliser le théorème 2.15.

Calcul de la mesure Nous pouvons à présent calculer la mesure de $\Omega_\infty(i)$. Pour cela, nous nous appuierons sur la démarche utilisée par Norris dans [Nor98].

Pour montrer que partant d'un état i quelconque, on passera sûrement infiniment souvent en 0, nous allons prouver que 0 est atteint avec probabilité 1, ceci à partir de n'importe quel état.

Soit i un entier. Montrons donc que $Prob\{\pi \in Path(i),\ \pi \vDash \Diamond 0\} = 1$. Pour alléger l'écriture, on dénotera par $\mathbb{P}_i$ la mesure de l'ensemble des chemins partant de i qui atteignent 0. Avec les notations introduites plus haut, on obtient les équations suivantes :

$$\mathbb{P}_0 = 1 \ et \ \forall i \in \mathbb{N} \setminus \{0\},\ \mathbb{P}_i = p_i \mathbb{P}_{i+1} + q_i \mathbb{P}_{i-1}$$

On définit alors pour i entier naturel non nul une nouvelle variable : $u_i = \mathbb{P}_{i-1} - \mathbb{P}_i$. Comme $p_i + q_i = 1$, on a $p_i u_{i+1} = q_i u_i$. On peut alors exprimer u_i en fonction de u_1 :

$$u_i = \frac{q_{i-1} q_{i-2} \cdots q_1}{p_{i-1} p_{i-2} \cdots p_1} u_1 =: \gamma_{i-1} u_1$$

[4] Cet ensemble est noté $\{\pi \in Path(i),\ \pi \vDash \Box\Diamond 0\}$

Enfin, puisque $\sum_{j=0}^{i} u_j = \mathbb{P}_0 - \mathbb{P}_i$, on obtient :

$$\mathbb{P}_i = 1 - u_1 \sum_{j=0}^{i-1} \gamma_j$$

Si on détermine u_1, on pourra calculer toutes les probabilités. Dans notre cas, l'hypothèse $(H1)$ implique que $\sum_{j=0}^{\infty} \gamma_i = \infty$. En effet, considérons le terme général de la série : pour $i \leq k$, $\gamma_i = \frac{q_i ... q_k}{p_i ... p_k} \cdot \frac{q_{k-1} ... q_1}{p_{k-1} ... p_1}$. Notre hypothèse permet d'affirmer que $\forall i \geq k$, $\frac{q_i ... q_k}{p_i ... p_k} \geq 1$. Ainsi, il existe une constante C positive telle que, quelque soit $i \geq k$, $\gamma_i \geq C$. De plus, C est *strictement* positive dès que $q_{k-1} ... q_1 > 0$ ce qui est le cas sous nos hypothèses. Le terme général de la série ne tend pas vers 0, donc la série diverge. On a $\sum_{j=0}^{\infty} \gamma_i = \infty$.

Rappelons que $\mathbb{P}_i$ est une probabilité, et ce quelque soit i. Alors, on a toujours $0 \leq \mathbb{P}_i \leq 1$. Pour que $\mathbb{P}_i$ soit compris entre 0 et 1 même lorsque i croît, il faut nécessairement $u_1 = 0$ (puisque la série de terme général γ_i diverge). Par suite, pour tout i entier naturel, $\mathbb{P}_i = 1$.

Ainsi, nous avons prouvé qu'à partir de n'importe quel état, on atteint l'état 0 avec probabilité 1 : $\forall i \in \mathbb{N},\ \mathit{Prob}(\Omega_1(i)) = 1$. Puisque de l'état 0 on passe en un coup avec probabilité 1 dans l'état 1, on a $\mathit{Prob}(\Omega_{n+1}(i)) = \mathit{Prob}(\Omega_n(i))\ \mathit{Prob}(\Omega_1(1))$. Et donc, $\forall n \in \mathbb{N},\ \forall i \in \mathbb{N},\ \mathit{Prob}(\Omega_n(i)) = 1$. Comme $\Omega_\infty(i) = \lim_{n\to\infty} \Omega_n(i)$ et par la continuité de la mesure, on conclut que $\forall i \in \mathbb{N},\ \mathit{Prob}(\Omega_\infty(i)) = 1$, c'est-à-dire que les chemins visitent infiniment souvent l'état 0 presque sûrement.

$$\forall i \in \mathbb{N},\ \mathit{Prob}\{\pi \in \mathit{Path}(i),\ \pi \vDash \Box\Diamond 0\} = 1$$

Chapitre 3

Processus de décision markoviens

3.1 Définitions

Jusqu'ici nous avons modélisé les systèmes stochastiques par des chaînes de Markov. Ce modèle est adapté lorsque toutes les transitions du systèmes sont probabilistes et convient donc particulièrement aux systèmes pour lesquels les actions ne dépendent pas de l'environnement extérieur et que Vardi appelle systèmes *fermés* [Var85]. Si on s'intéresse maintenant aux systèmes qui réagissent à leur environnement extérieur, il faut aussi considérer des transitions non-déterministes. Le modèle correspondant est appelé processus de décision markovien (PDM). Les processus de décision markoviens ont donc deux types d'états, les états probabilistes et les états non-déterministes. Lorsqu'une exécution atteint un état probabiliste, un successeur est choisi en suivant la loi de probabilité donnée. Lorsque au contraire une exécution visite un état non-déterministe, un successeur est choisi de façon non-déterministe parmi les successeurs possibles. Voici maintenant une définition plus formelle des processus de décision markoviens.

Définition 3.1 *Un* processus de décision markovien *est un quadruplet* (X, N, P, P_0) *où* (X, P, P_0) *est une chaîne de Markov et* $N \subset X$ *est l'ensemble des états non-déterministes (*$X \setminus N$ *est l'ensemble des états probabilistes).*

Les ensembles N (resp. $X \setminus N$) sont donc respectivement les ensembles d'états pour lesquels une transition non-déterministe (resp. probabiliste) s'opère. Si x est un état non-déterministe, on interprète alors $P(x, y)$ par : $P(x, y) > 0$ si, et seulement si il existe une transition de x à y.

Cette définition des processus de décision markoviens a été introduite dans [Var85] sous le nom de *chaîne de Markov concurrente*. Il s'avère qu'elle est équivalente à la notion de processus de décision markovien de Derman [Der70].

Remarque Comme pour les chaîne de Markovs, on peut ajouter à la définition des processus de décision markoviens une composante L, fonction d'étiquetage des états par des propositions atomiques de AP.

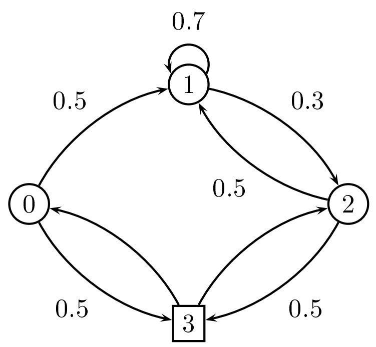


FIG. 3.1 – Exemple de processus de décision markovien...

On a alors besoin de la notion d'*adversaire* pour définir les choix faits dans les états non-déterministes et donc les trajectoires possibles. Cet adversaire, aussi appelé *scheduler* fait tous les choix non-déterministes, en tenant compte de l'historique des états précédemment visités.

Formellement, un adversaire pour une chaîne de Markov concurrente $M = (X, N, P, P_0)$ est une fonction $\sigma : X^* \times N \to X$ qui associe un état à chaque suite finie d'états terminant par un état non-déterministe. De plus σ vérifie : $\sigma(x_1, x_2, \cdots, x_n) = x$ seulement si $P(x_n, x) > 0$, c'est-à-dire que x est un successeur de x_n.

Si M est un processus de Markov et σ un adversaire pour M, alors on peut construire une chaîne de Markov $M^\sigma = (X^+, P^\sigma, {P_0}^\sigma)$ qui décrit le comportement de M face à l'adversaire $\sigma.X^+$ dénotant l'ensemble des mots non vides sur l'alphabet X. La chaîne de Markov M^σ est définit comme suit :

- ${P_0}^\sigma(x) : X^+ \to [0, 1]$ vérifie ${P_0}^\sigma(x) = P_0(x)$ si $x \in X$ et ${P_0}^\sigma(w) = 0$ si $w \in X^+ \setminus X$,
- $P^\sigma : X^+ \times X^+ \to [0, 1]$ est défini pour tout $(x, y) \in X^+ \times X^+$ par
  - $P^\sigma(xu, xuv) = P(u, v)$ si $u \in X \setminus N$,
  - $P^\sigma(xu, xuv) = 1$ si $u \in N$ et $\sigma(xu) = v$, et
  - $P^\sigma(x, y) = 0$ sinon.

La chaîne de Markov M^σ est en fait un dépliage du graphe de M en arbre.

Exemple Voici un exemple illustrant le passage d'un processus de décision markovien et d'un scheduler associé à la chaîne de Markov correspondante. Les états représentés par des ronds (0, 1 et 2) sont des états probabilistes et l'état représenté par un carré (3) est un état non-déterministe.

Le but de l'adversaire ici peut être d'emprunter infiniment souvent chaque transition partant de l'état 3.

On considère un adversaire ne tenant compte que de l'état précédant 3. Si ce dernier est 0, il exécute la transition vers 2 et vice et versa. Formellement, σ se définit par :

- $\sigma(w \cdot 0 \cdot 3) = 2$, et
- $\sigma(w \cdot 2 \cdot 3) = 0$.

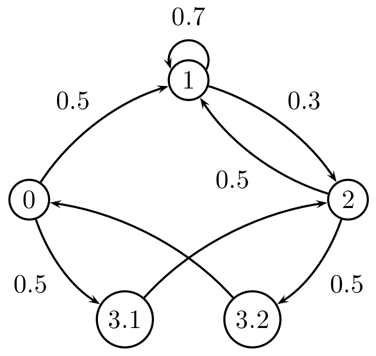


FIG. 3.2 – ... et une chaîne de Markov équivalente à adversaire fixé

La chaîne de Markov résultante est représentée 3.2.

Si au lieu de choisir cet adversaire, on définit :

- $\sigma(w \cdot 3) = 0$ si, et seulement si $|w|_2$ premier [1],
- $\sigma(w \cdot 3) = 2$ sinon.

la chaîne de Markov résultante possède un nombre infini dénombrable d'états et on ne peut trouver de chaîne de Markov équivalente ayant un nombre fini d'états.

3.2 Vérification

Nous allons maintenant nous intéresser à la vérification des processus de décision markoviens. Nous l'avons vu dans le paragraphe précédent, en munissant un processus de décision markovien d'un adversaire, on obtient une chaîne de Markov (à espace d'états infini). Si on fixe un adversaire, on peut donc munir l'ensemble des exécutions d'une mesure de probabilité définie sur les préfixes finis des runs comme on le fait pour les chaînes de Markov.

Un mot infini $U = q_0 \cdot q_1 \cdots q_n \cdots$ sur X est une exécution du processus de décision markovien M conforme à l'adversaire σ si, et seulement si

- $\forall i \in \mathbb{N},\ q_i \in X \setminus N \Rightarrow \sigma(q_0 \cdot q_1 \cdots q_i) = q_{i+1}$,
- $\forall i \in \mathbb{N},\ q_i \in N \Rightarrow P(q_i, q_{i+1}) > 0$, et
- $P_0(q_0) > 0$.

Notations Soit Φ une formule de LTL. On dit que l'exécution $U = x_0 \cdot x_1 \cdots$ de M vérifie Φ si $L(x_0) \cdot L(x_1) \cdots \models \Phi$.

On dit que $\langle M, \sigma \rangle$ vérifie Φ avec probabilité $p \in [0, 1]$ – et on note $\langle M, \sigma \rangle \models_p \Phi$ – si l'ensemble des exécutions de M conformes à σ qui vérifient la formule Φ est de mesure p.

[1] où $|w|_2$ représente le nombre de 2 dans w

On dit que l'adversaire σ est sans mémoire si les choix faits par l'adversaire ne dépendent que de l'état de contrôle courant, ce qui s'exprime plus formellement ainsi : $\forall x \in N,\ \forall (w, w') \in X^* \times X^*,\ \sigma(w \cdot x) = \sigma(w' \cdot x)$.

Voici à présent quelques problèmes qu'il nous semblent intéressant de traiter au sujet des processus de décision markoviens.

P_1 **: Universalité** Étant donnés une formule de LTL Φ et un processus de décision markovien M a-t-on : $\forall \sigma,\ \langle M, \sigma\rangle \vDash_{p=1} \Phi$?

P_2 **: Existence** Étant donnés une formule de LTL Φ et un processus de décision markovien M a-t-on : $\exists \sigma,\ \langle M, \sigma\rangle \vDash_{p=1} \Phi$?

P_3 **: Universalité sans mémoire** Étant donnés une formule de LTL Φ et un processus de décision markovien M a-t-on : $\forall \sigma$ sans mémoire, $\langle M, \sigma\rangle \vDash_{p=1} \Phi$?

Il est clair que les problèmes P_2 et P_3 sont moins difficiles que le problème P_1. Cependant, un lien entre P_2 et P_3 est encore insoupconné.

Pour le problème d'universalité de l'adversaire «satisfaisant», nous ne traitons que le cas particulier où Φ est de la forme $\Box\Diamond f$ si f est une proposition atomique. Nous ne considérerons d'autre part que des systèmes de décision markoviens particuliers à savoir des systèmes à canaux pour lesquels seules les pertes sont probabilistes, les autres actions étant non-déterministes.

Cette variante restrictive du problème P_1 est prouvée **indécidable** dans le chapitre 5. Le problème *d'existence* est lui **décidable** et nous donnerons l'algorithme également au chapitre 5. Le troisième problème est également **décidable**, ce résultat utilisant la décidabilité de P_2.

Chapitre 4

Systèmes communicants par des canaux à pertes stochastiques

4.1 Systèmes communicants par des canaux non fiables

Lorsqu'on prouve des bornes inférieures, comme par exemple des résultats d'indécidabilité, l'étude des systèmes communicants par des canaux non fiables peut se restreindre sans perte de généralité à un unique système «communicant avec lui-même» par un seul canal non fiable. Ce sera en particulier le cas dans notre étude et nous nous restreindrons souvent à un seul processus et un seul canal. Néanmoins les définitions sont données dans un cadre plus général.

4.1.1 Les *Lossy*

Par LCS (pour *Lossy Channel Systems*) nous désignons un système à canaux non fiables.

Définition 4.1 *Un LCS est un sextuplet $\mathcal{L} = (S_{control}, s_0, L, Ch, M, \hookrightarrow)$ où*
- *$S_{control}$ est un ensemble fini d'états de contrôle ;*
- *s_0 est un état de contrôle initial ;*
- *$L : S_{control} \to 2^{AP}$ est une fonction d'étiquetage ;*
- *Ch est un ensemble fini de canaux ;*
- *M est un ensemble fini de messages ;*
- *$\hookrightarrow \subseteq S_{control} \times Act \times S_{control}$ une relation de transition*

où $SendAct = \{c!m : c \in Ch,\ m \in M\}$, $RecAct = \{c?m : c \in Ch,\ m \in M\}$, τ représente les actions internes du système et $Act = SendAct \cup RecAct \cup \{\tau\}$.

À un LCS $\mathcal{L}$ on associe un système de transition $TS(\mathcal{L})$. Les états globaux de ce système sont des couples $\mathbf{s} = \langle s, w \rangle$ où s est un état de $S_{control}$ et w représente le contenu des canaux. Formellement, w est une fonction de Ch dans M^*. On note $\mathbf{S}_{global}$ l'ensemble des états globaux du système. L'état initial du système de transition est $s_0 = \langle s_0, \emptyset \rangle$ où $\emptyset$ désigne la fonction de Ch dans

M^* qui associe à chaque canal le mot vide. On note $|\mathbf{s}|$ le nombre total de messages qu'il y a dans les canaux à l'état $\mathbf{s}$ et $\mathbf{s} \cdot c$ le contenu $m_1 m_2 ... m_k$ du canal $c \in Ch$ dans l'état global $\mathbf{s}$. La fonction d'étiquetage est encore notée L et définie par : $L(\langle s, w\rangle) := L(s)$. On utilise l'ensemble d'actions $Act_{\mathfrak{l}} = Act \cup \{\mathfrak{l}_{c,i} : c \in Ch,\ i \in \mathbb{N}\}$ où $\mathfrak{l}_{c,i}$ signifie que le $i$ème message du canal c se perd. La relation de transition $\rightarrow \subseteq \mathbf{S}_{global} \times \mathbf{Act}_{\mathfrak{l}} \times \mathbf{S}_{global}$ est la plus petite relation telle que, pour $w(c) = m_1 m_2 ... m_k$:

- Si $s \hookrightarrow^{c!m} t$ alors $\langle s, w\rangle \xrightarrow{c!m} \langle t, w[c := w(c)m]\rangle$
- Si $s \hookrightarrow^{c?m} t$ et $k \geq 1$ alors $\langle s, w[c := mw(c)\rangle \xrightarrow{c?m} \langle t, w\rangle$.
- Si $k \geq 1$ et $i \in \{1, ..., k\}$ alors $\langle s, w\rangle \xrightarrow{\mathfrak{l}_{c,i}} \langle s, w[c := m_1 ... m_{i-1} m_{i+1} ... m_k]\rangle$.
- Si $s \hookrightarrow^{\tau} t$ alors $\langle s, w\rangle \xrightarrow{\tau} \langle t, w\rangle$.

4.1.2 Pertes stochastiques

Dans la littérature, on trouve une définition pour les systèmes à canaux à pertes stochastiques qui attribue au système une probabilité constante de perte quelle que soit la taille et le contenu du canal de communication [BE99] [ABPJ00] [PN97].

Cette définition semble peu réaliste car en pratique, la probabilité de perte dépend fortement du contenu du canal et en particulier du nombre de messages. En effet, plus le nombre de messages est grand, plus il y a de chances qu'un message se perde.

D'autre part, les résultats obtenus avec ce modèle dépendent fortement de la probabilité de perte $\mathcal{P}$: la décidabilité de la vérification est prouvée pour $\mathcal{P} > \frac{1}{2}$ et en deça de cette valeur, $\mathcal{P}$ doit être connu et relativement grand par rapport aux autres probabilités de transitions (action interne du système, écriture ou lecture sur le canal) pour que la vérification soit décidable. Compte tenu qu'en pratique la probabilité de perte est souvent bien inférieure à $\frac{1}{2}$, les résultats obtenus avec cette définition des pertes stochastiques font que cette dernière semble là aussi inadaptée.

Nous allons donc introduire une nouvelle définition des systèmes communicants par des canaux à pertes stochastiques. Cette définition nous semble plus réaliste car la probabilité de perte dépend du nombre de messages qu'il y a dans le canal et tend vers 1 quand le nombre de messages tend vers l'infini. Notre but est également de donner des résultats indépendants du taux de perte attribué à chaque message et même des résultats lorsque la valeur du taux de perte est inconnue.

Dans toute la suite nous appellerons $PLCS$ un système à canaux à pertes stochastiques (Probabilistic Lossy Channel Systems).

Définition 4.2 *Un $PLCS$ est un triplet $\mathcal{PL} = (\mathcal{L}, P_{control}, \tau)$ où $\mathcal{L}$ est un LCS, $\tau \in]0, \infty[$ le taux de perte et $P_{control} : S_{control} \times Act \times P_{control} \rightarrow [0,1]$ une fonction vérifiant $P_{control}(s, \alpha, t) > 0$ si, et seulement sis $\hookrightarrow \alpha t$.*

À un $PLCS$ $\mathcal{PL} = (\mathcal{L}, P_{control}, \tau)$ on associe une chaîne de Markov en augmentant les transitions du système de transitions $TS(\mathcal{L})$ par des probabilités. À chaque pas du système, tous les messages du canal ont le même taux de perte τ. Aux autres actions $\alpha \in Act$, on donne un poids par l'intermédiaire de $P_{control}$. Pour obtenir des probabilités, nous devons introduire une fonction de normalisation $\nu : S_{global} \to]0,\infty[$ définie par :

$$\nu(\langle s,w\rangle) = |w| \cdot \tau + \sum_{\alpha \in Act(\langle s,w\rangle)} P_{control}(s,\alpha)$$

où $P_{control}(s,\alpha) = \sum_{t \in S_{control}} P_{control}(s,\alpha,t)$. Ce facteur de normalisation est toujours non nul car on suppose que dans tout état s, il existe une action α et un état t tel que $s \hookrightarrow^{\alpha} t$. La probabilité de transition $\mathbf{P}_{global} : \mathbf{S}_{global} \times \mathbf{Act}_{\mathfrak{l}} \times \mathbf{S}_{global} \to [0,1]$ est alors définie comme suit.

- Si $\alpha \in Act,\ \langle s,w\rangle \xrightarrow{\alpha} \langle s',w'\rangle,\ |w'| \neq 0$ alors,

$$\mathbf{P}_{global}(\langle s,w\rangle, \alpha, \langle s',w'\rangle) = \frac{1}{\nu(\langle s,w\rangle)} \cdot P_{control}(s,\alpha,s').$$

- Pour la perte d'un message correspondant à une transition $\mathbf{s} \xrightarrow{\mathfrak{l}_{c,i}} \mathbf{t}$ on définit

$$\mathbf{P}_{global}(\mathbf{s}, \mathfrak{l}_{c,i}, \mathbf{t}) = \frac{\tau}{\nu(\mathbf{s})}.$$

- Si $\mathbf{s} = \langle s, \emptyset\rangle$ on pose

$$\mathbf{P}_{global}(\langle s,\emptyset\rangle, \alpha, \langle s',w'\rangle) = \frac{P_{control}(s,\alpha,s')}{\nu(\langle s,\emptyset\rangle)}.$$

- Dans tous les autres cas $\mathbf{P}_{global}(\mathbf{s},\alpha,\mathbf{t}) = 0$.

La chaîne de Markov associée au $PLCS\ \mathcal{PL}$ est $MC(\mathcal{PL}) = (\mathbf{S}_{global}, \mathbf{P}_{global}, L, \mathbf{s}_0)$ où $\mathbf{P}_{global}$ est vue comme une fonction de $\mathbf{S}_{global} \times \mathbf{S}_{global}$ dans $[0,1]$ (on oublie les actions pour ne retenir que les probabilités de transition).

4.2 Premiers résultats

Dans cette section nous allons montrer la décidabilité du model checking des formules de LTL dans le cadre des systèmes à canaux à pertes stochastiques que nous avons introduits précédemment.

Pour cela nous commençons par démontrer des résultats généraux que nous pourrons appliquer à notre cas particulier.

4.2.1 Caractérisation de $\models_{p=1} \Phi$

Notations Soit $\mathcal{A}$ une chaîne de Markov étiquetée d'ensemble d'états dénombrable S. Les états de $\mathcal{A}$ sont étiquetés par $L : S \to AP$.

On suppose en outre l'existence d'un sous-ensemble fini S_0 de S visité infiniment souvent presque sûrement, c'est-à-dire vérifiant : $\mathbb{P}\{\pi | \pi \models \Box\Diamond S_0\} = 1$

Soient $(a_j)_{j\in J}$ et $(b_j)_{j\in J}$ deux familles de propositions atomiques de AP indexées par l'ensemble fini J. On définit alors une formule de LTL $f = \bigvee_{j\in J}(\Diamond\Box a_j \wedge \Box\Diamond b_j)$.

On cherche à caractériser la validité de f avec probabilité 1 dans $\mathcal{A}$.

Définition 4.3 *Soit $G = (S_0, (\rightsquigarrow_j)_{j\in J}, \rightsquigarrow)$ le graphe dont les sommets sont les états de S_0 et où $(\rightsquigarrow_j)_{j\in J}$ et $\rightsquigarrow$ sont différents types d'arêtes définies comme suit.*

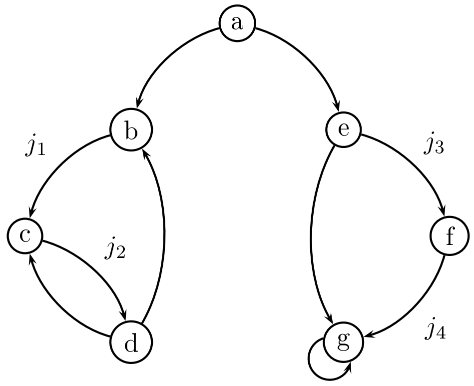


FIG. 4.1 – Les BSCC sur un exemple

Soit $j \in J$. Pour tous sommets s et t de S_0, $s \rightsquigarrow_j t$ si, et seulement si $\exists s_1,\ s_2, ..., s_{n-1} \in S \setminus S_0$ tels que $s_0 = s \to s_1 \to\ ... \to s_{n-1} \to t = s_n$ et $\exists i \in [\![0, n]\!]$ tel que $b_j \in L(s_i)$.

On définit dans un second temps les arêtes $\rightsquigarrow$ par $s \rightsquigarrow t$ si, et seulement si $\nexists j \in J$ tel que $s \rightsquigarrow_j t$ et $\exists s_1,\ ..., s_{n-1}$ tels que $s_0 = s \to s_1 \to\ ... \to s_{n-1} \to t = s_n$.

$s \rightsquigarrow_j t$ signifie donc que t est accessible depuis s dans $\mathcal{A}$ en utilisant des états intermédiaires dans $S \setminus S_0$ et de sorte que b_j est vraie au moins dans un état du parcours. Ainsi, si on suppose que l'état s est visité infiniment souvent avec probabilité 1, b_j sera vrai infiniment souvent également avec probabilité 1.

$s \rightsquigarrow t$ signifie que t est accessible depuis s «directement» (sans états intermédiaires dans S_0) mais tous ces chemins de s à t ne parcourent aucun b_j pour $j \in J$.

Définition 4.4 *On appelle* composante fortement connexe de base *(BSCC) d'un graphe G toute composante fortement connexe de G à partir de laquelle aucune autre composante fortement n'est accessible.*

Les BSCC sont donc les feuilles de l'arbre des composantes fortement connexe d'un graphe G.

On note $\mathcal{C}$ l'ensemble des composantes fortement connexes de base du graphe G toutes arêtes confondues.

Exemple Dans cet exemple, les composantes fortement connexes de base sont les ensembles $\{b, c, d\}$ et $\{g\}$.

Lemme 4.5 *Dans $\mathcal{A}$, $\sum_{C \in \mathcal{C}} \mathbb{P}(\{\pi | \pi \vDash \Diamond C\}) = 1$*

Dans le lemme 4.5, la notation $\Diamond C$ signifie $\Diamond \bigvee_{s \in C} s$.

Démonstration Ce lemme résulte de la définition des composantes fortement connexes de base. Presque tous les chemins finissent par atteindre une composante fortement connexe de base et la projection de ces chemins sur l'ensemble S_0 ne peut alors plus quitter cette composante. $\square$

Avec ces notations et ces hypothèses, nous pouvons énoncer le résultat suivant :

Théorème 4.6 $\mathbb{P}(\{\pi|\pi \models f\}) = 1$ *si, et seulement si* $\forall C \in \mathcal{C},\ \exists j_C \in J$ *tq*
- $\exists(s,t) \in C \times C,\ s \rightsquigarrow_{j_C} t$;
- $\{t \in S | a_{j_C} \notin L(t)\}$ *n'est pas accessible depuis* C.

Démonstration Pour la démonstration nous allons d'abord considérer que la formule f ne contient qu'une seule clause : $f = \Diamond\Box a_j \wedge \Box\Diamond b_j$. Le théorème 4.6 devient alors le suivant.

Lemme 4.7 $\mathbb{P}(\{\pi|\pi \models f\}) = 1$ *si, et seulement si* $\forall C \in \mathcal{C}$,
- $\exists(s,t) \in C \times C,\ s \rightsquigarrow_j t$;
- $\{t \in S | a_j \notin L(t)\}$ *n'est pas accessible depuis* C.

Nous étendrons ensuite le résultat aux disjonctions d'un nombre quelconque de clauses.

$(\Longleftarrow)$

Supposons dans un premier temps que dans toute composante fortement connexe de base C, il existe deux états liés par la relation $\rightsquigarrow_j$ et qu'on ne peut atteindre depuis C que des états vérifiant a_j.

Soit C une composante fortement connexe de base du graphe G. On considère l'ensemble des exécutions dans le système probabiliste $\mathcal{A}$ qui atteignent C. Soit donc $\Pi_C = \{\pi|\pi \models \Diamond C\}$. Une exécution π de Π_C visitera presque sûrement chaque état de C infiniment souvent. Ce dernier point se démontre en plusieurs temps.

Tout d'abord, les définitions des arêtes dans G et des composantes fortement connexes de base permettent d'affirmer qu'une exécution qui atteint $C \in \mathcal{C}$ n'atteindra jamais $C' \in \mathcal{C}$ avec $C' \neq C$.

Si on fixe à présent une composante fortement connexe de base $C \in \mathcal{C}$, presque toute exécution de Π_C – c'est-à-dire qui atteint C – visite infiniment souvent C. En effet, $\mathbb{P}(\{\pi|\pi \models \Box\Diamond C\}) = \mathbb{P}(\{\pi|\pi \models \Box\Diamond S_0\}) \cdot \mathbb{P}(\{\pi|\pi \models \Diamond C\})$, donc $\mathbb{P}(\{\pi|\pi \models \Box\Diamond C\}) = \mathbb{P}(\{\pi|\pi \models \Diamond C\})$.

Ensuite chaque chemin π qui visite C infiniment souvent visite un état $s_\pi \in C$ infiniment souvent car C est fini. La forte connexité de C implique que tous les états de C sont accessibles à partir de s_π. On rappelle que l'accessibilité dans le graphe G implique celle dans $\mathcal{A}$ (cf définition de G, définition 4.3). Alors pour tout état t de C, il existe un chemin γ partant de s_π et gagnant t. La probabilité d'emprunter ce chemin dans $\mathcal{A}$ lorsque l'on se trouve dans s_π est non nulle. Donc l'ensemble des chemins qui visitent une infinité de fois s_π et évitant infiniment souvent γ est de mesure nulle. On en déduit que $\mathbb{P}(\{\pi|\pi \models \Box\Diamond t\}) \geq \mathbb{P}(\{\pi|\pi \models \Box\Diamond s_\pi\}) \cdot \mathbb{P}(\{\pi|\pi\Box\Diamond s_\pi \wedge \models \Box\Diamond\gamma\})$, soit $\mathbb{P}(\{\pi|\pi \models \Box\Diamond t\}) \geq \mathbb{P}(\{\pi|\pi \models \Box\Diamond s_\pi\})$. Ainsi presque toute exécution qui visite C une infinité de fois visite chaque état de C une infinité de fois également : $\mathbb{P}(\{\pi|\pi \models \Box\Diamond C\}) = \mathbb{P}(\{\pi|\pi \models \bigwedge_{t\in C} \Box\Diamond t\})$.

Finalement, $\mathbb{P}(\Pi_C) = \mathbb{P}(\{\pi|\pi \models \bigwedge_{t\in C} \Box\Diamond t\})$. Presque toutes les exécutions de Π_C parcourent infiniment souvent chaque état de C.

En particulier, si s est un état de C origine d'une flèche $\rightsquigarrow_j$ (donné dans le lemme), presque toutes les exécutions de Π_C parcourent infiniment souvent s. Comme précédemment, les exécutions qui visitent une infinité de fois s et qui ne parcourent qu'une nombre fini de fois la flèche $\rightsquigarrow_j$ partant de s forment un ensemble de mesure nulle. Alors $\mathbb{P}(\Pi_C) = \mathbb{P}(\{\pi | \pi \vDash \Box\Diamond \rightsquigarrow_j\})$ ce qui implique : $\mathbb{P}(\Pi_C) = \mathbb{P}(\{\pi | \pi \vDash \Box\Diamond b_j\})$. Presque toutes les exécutions de Π_C vérifient infiniment souvent la proposition b_j.

Enfin, en utilisant le résultat du lemme 4.5, on obtient.

$$\begin{aligned}
\mathbb{P}(\{\pi | \pi \vDash \bigvee_{C \in \mathcal{C}} \Box\Diamond b_j\}) &= \sum_{C \in \mathcal{C}} \mathbb{P}(\{\pi | \pi \vDash \Box\Diamond b_j\}) \\
&= \sum_{C \in \mathcal{C}} \mathbb{P}(\{\pi | \pi \vDash \Diamond C\}) \\
&= 1
\end{aligned} \tag{4.1}$$

D'autre part, depuis C il est impossible d'atteindre un état dont l'étiquette de contient pas a_j. Alors $\Pi_C = \{\pi | \pi \vDash C \wedge \neg\Box\Diamond\neg a_j\} = \{\pi | \pi \vDash C \wedge \Diamond\Box a_j\}$. L'égalité des ensembles impliquant l'égalité des mesures, on a $\mathbb{P}(\Pi_C) = \mathbb{P}(\{\pi | \pi \vDash C \wedge \Diamond\Box a_j\})$.

Le lemme 4.5 nous permet encore de conclure :

$$\begin{aligned}
\mathbb{P}(\{\pi | \pi \vDash \bigvee_{C \in \mathcal{C}} \Diamond\Box a_j\}) &= \sum_{C \in \mathcal{C}} \mathbb{P}(\{\pi | \pi \vDash \Diamond\Box a_j\}) \\
&= \sum_{C \in \mathcal{C}} \mathbb{P}(\Pi_C) \\
&= \sum_{C \in \mathcal{C}} \mathbb{P}(\{\pi | \pi \vDash \Diamond C\}) \\
&= 1
\end{aligned} \tag{4.2}$$

Finalement, $\mathbb{P}(\{\pi | \pi \vDash f\}) = 1$.

Supposons à présent que f est une disjonction de clauses : $f = \bigvee_{j \in J}(\Diamond\Box a_j \wedge \Box\Diamond b_j)$.

D'après ce qui précède, si on fixe $C \in \mathcal{C}$, presque toutes les exécutions de Π_C vérifient infiniment souvent b_{j_C} et toujours a_{j_C} à partir d'un certain moment. A fortiori presque toutes les exécutions de Π_C vérifient la disjonction f. On a donc $\mathbb{P}(\{\pi \in \Pi_C | \pi \Vdash f\}) = \mathbb{P}(\Pi_C)$. Le lemme 4.5 permet encore une fois de conclure :

$$\begin{aligned}
\mathbb{P}(\{\pi | \pi \vDash f\}) &= \mathbb{P}(\{\pi | \pi \vDash f \wedge \bigvee_{C \in \mathcal{C}} \Diamond C\}) \\
&= \mathbb{P}(\bigcup_{C \in \mathcal{C}} \{\pi \in \Pi_C | \vDash f\}) \\
&= \sum_{C \in \mathcal{C}} \mathbb{P}(\{\pi \in \Pi_C | \vDash f\}) \\
&= \sum_{C \in \mathcal{C}} \mathbb{P}(\Pi_C) \\
&= 1
\end{aligned} \tag{4.3}$$

Cette suite d'égalités termine la démonstration de la première implication.
($\Longrightarrow$)

Nous allons montrer à présent montrer la réciproque par la contraposée. Supposons qu'il existe une composante fortement connexe de base $C \in \mathcal{C}$ telle que pour tout $j \in J$ ou bien il n'existe pas de couple $(s,t) \in C \times C$ vérifiant $s \rightsquigarrow_j t$ ou bien il existe $s \in C$ et $t \in S$ tels que $s \rightsquigarrow^*$ et $t \models \neg a_j$.

Dans un premier temps, fixons $j \in J$ et traitons les deux cas qui se présentent.

Premier cas : $\nexists s \rightsquigarrow_j t$ dans C :

Puisque $C \in \mathcal{C}$, la probabilité d'atteindre C depuis l'état initial s_0 est non nulle ; on la note $\mathcal{P}$. On a donc $\mathbb{P}(\Pi_C) = \mathcal{P}$. Presque toutes les exécutions de Π_C visitent une infinité de fois chaque état accessible depuis C et aucun autre. L'hypothèse $\nexists s \rightsquigarrow_j t$ implique donc que $\mathbb{P}(\{\pi \in \Pi_C | \pi \models \Box\Diamond b_j\}) = 0$. Alors $\mathbb{P}(\pi \in \Pi_C | \pi \models \Diamond\Box\neg b_j\}) = 1$. Ceci étant vrai quel que soit $j \in J$ [1], on obtient $\mathbb{P}(\pi \in \Pi_C | \pi \models \bigwedge_{j\in J} \Diamond\Box\neg b_j\}) = 1$. Les formules $\bigwedge_{j\in J} \Diamond\Box\neg b_j$ et $\neg \bigvee_{j\in J} \Box\Diamond b_j$ sont équivalentes donc presque toutes les exécutions de Π_C ne visitent infiniment souvent aucun des b_j. On conclut alors $\mathbb{P}(\{\pi|\pi \not\models \bigvee_{j\in J} \Box\Diamond b_j\}) \geq \mathbb{P}(\Pi_C) \cdot \mathbb{P}(\pi \in \Pi_C | \pi \not\models \bigvee_{j\in J} \Box\Diamond b_j\}) = \mathcal{P} > 0$. Ou encore $\mathbb{P}(\{\pi|\pi \models \bigvee_{j\in J} \Box\Diamond b_j\}) = 1 - \mathcal{P} < 1$.
A fortiori $\mathbb{P}(\{\pi|\pi \models f\}) \leq \mathbb{P}(\{\pi|\pi \models \bigvee_{j\in J} \Box\Diamond b_j\}) < 1$.

Deuxième cas : $\neg a_j$ accessible depuis C :

Si un état t dans lequel $\neg a_j$ est vrai est accessible depuis C, alors comme nous l'avons montré précédemment, t est visité infiniment souvent par presque tous les chemins de Π_C. La mesure de l'ensemble des exécutions qui atteignent C et visite une infinité de fois $t \models \neg a_j$ est donc celle de Π_C c'est-à-dire $\mathcal{P}$: $\mathbb{P}(\{\pi \in \Pi_C | \pi \models \Box\Diamond\neg a_j\}) = \mathbb{P}(\Pi_C) = \mathcal{P}$. De $\mathbb{P}(\{\pi \in \Pi_C | \pi \models \bigwedge_{j\in J} \Box\Diamond\neg a_j\}) \geq \prod_{j\in J} \mathbb{P}(\{\pi \in \Pi_C | \pi \models \Box\Diamond\neg a_j\})$, on déduit $\mathbb{P}(\{\pi \in \Pi_C | \pi \models \bigwedge_{j\in J} \Box\Diamond\neg a_j\}) = 1$. Ce qui permet de conclure $\mathbb{P}(\{ pi|\pi \models \bigwedge_{j\in J} \Box\Diamond\neg a_j\}) > \mathcal{P}$ et donc $\mathbb{P}(\{\pi|\pi \models f\}) \leq 1 - \mathcal{P} < 1$.

Ce qui termine la démonstration. □

4.2.2 Canal vide inévitable ?

Dans [BE99], Baier & Engelen prouvent que dans leur modèle, presque toutes les exécutions visitent infiniment souvent l'ensemble des états globaux pour lesquels le canal est vide. Cependant, il leur faut pour cela utiliser que la probabilité de perte est «suffisamment grande». Dans notre cas, nous allons montrer sans hypothèse supplémentaire que l'ensemble des états où le canal est vide est visité infiniment souvent presque sûrement.

Soit $S_0 = \{\mathbf{s} | |\mathbf{s}| = 0\}$ l'ensemble des états globaux à canal vide. On veut montrer que :

Lemme 4.8 $\mathbb{P}(\{\pi|\pi \models \Box\Diamond S_0\}) = 1$.

Démonstration Lorsque le système se trouve dans un état $\mathbf{s} = \langle s, w\rangle$ la probabilité de perdre un message est $\dfrac{|w| \cdot \tau}{\nu(\mathbf{s})}$, c'est-à-dire $\dfrac{|w| \cdot \tau}{|w| \cdot \tau + \displaystyle\sum_{\alpha \in Act(\langle s,w\rangle)} P_{control}(s, \alpha)}$.

[1] J est fini

On s'aperçoit donc que la probabilité de perte augmente avec la taille du canal et tend vers 1 quand cette dernière tend vers l'infini. Ceci est vrai car les poids attribués aux actions de Act peuvent être choisis dans l'intervalle $[0,1]$ et sont donc bornés.

La probabilité de diminuer la taille du canal est supérieure à celle de perte car la diminution se fait soit par perte soit par lecture de la tête du canal. Alors la probabilité de diminuer la taille du canal (c'est-à-dire de lire ou perdre) tend aussi vers 1 quand la taille du canal tend vers l'infini.

Pour simplifier l'étude de $\mathbf{S}$, on regroupe les états selon la taille de leur canal. On obtient donc des sous-ensembles $S_0,\ S_1,\ \ldots$ de $\mathbf{S}$.

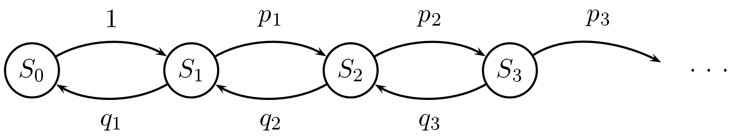
Soit $n \in \mathbb{N} \setminus \{0\}$. Nous allons majorer la somme des poids des actions de Act afin de minorer la probabilité de perte dans un état où le canal est de taille n. On pose $M_n = \max_{|\langle s,w\rangle|=n} \sum_{\alpha \in Act(\langle s,w\rangle)} P_{control}(s,\alpha)$. Pour tout état $\langle s,w\rangle$ de S_n, $\sum_{\alpha \in Act(\langle s,w\rangle)} P_{control}(s,\alpha) \leq M_n$ et donc $\dfrac{|w|\cdot\tau}{|w|\cdot\tau + \sum_{\alpha \in Act(\langle s,w\rangle)} P_{control}(s,\alpha)} \geq \dfrac{|w|\cdot\tau}{|w|\cdot\tau + M_n}$.

Lorsque la taille du canal varie, M_n est toujours fini et on peut par exemple définir les poids de façon à ce que M_n soit borné par 1. Alors, si n tend vers l'infini, la probabilité de perte tend vers 1. Il existe donc $k \in \mathbb{N} \setminus \{0\}$ tel que $\forall n \geq k,\ \mathbb{P}(S_n \to S_{n-1}) > \frac{1}{2}$.

Pour tout entier naturel non nul n, on définit une probabilité q_n de passer de S_n à S_{n-1} ; q_n est en fait le minimum des probabilités de perte ou de lecture dans les états qui ont n messages sur le canal :

$$q_n = \min_{|\langle s,w\rangle|=n} \mathbb{P}(w \to w' \,|\, |w'| = |w| - 1).$$

On définit ensuite $p_n = 1 - q_n$. p_n est un majorant des probabilités d'écriture pour les états au canal de longueur n. On obtient alors le graphe suivant :



Le système ainsi obtenu en minorant les probabilités de retour vers l'origine est tel que si S_0 est visité infiniment souvent avec probabilité 1, il le sera *a fortiori* dans le système de départ.

On peut à présent appliquer le lemme 2.17. Il en résulte que S_0 est visité infiniment souvent presque sûrement. $\square$

4.3 Décidabilité de la vérification

Le théorème 4.6 et le lemme 4.8 permettent de conclure :

Théorème 4.9 *Soit $\mathcal{L}$ un système à canaux à pertes stochastiques et M sa chaîne de Markov associée. Soit Φ une formule de LTL.*

Alors, le problème $M \models_{p=1} \Phi$ est décidable.

Démonstration La démonstration utilise le fait que l'accesibilité est décidable pour les PLCS. On utilise encuite le théorème 4.6 et le lemme 4.8 pour conclure. Par ailleurs, le théorème 4.6 fournit un algorithme de décision. □

Chapitre 5

Systèmes probabilistes et non-déterministes

Nous allons considérer des systèmes à canaux à pertes probabilistes. Les autres actions sont soit probabilistes, soit non-déterministes. Pour cette classe, nous avons étudié les problèmes énoncés dans la troisième partie.

Les processus de décision markoviens tels que nous les avons introduits dans le chapitre 3 font intervenir deux types d'états, les états probabilistes et les états non-déterministes. Pour ce qui est des processus non-déterministes qui communiquent via des canaux qui peuvent perdre de façon probabiliste des messages, ce modèle peut s'adapter en considérant qu'à chaque action des processus (lecture, écriture d'un message ou action interne), une série de pertes de messages peut s'effectuer. On considère que les pertes s'effectuent juste après chaque action des processus, et on ne représentera donc pas les pertes mais uniquement les autres actions.

5.1 Problème d'universalité

Soit $\mathcal{L}$ un PLCS non-déterministe (c'est-à-dire un LCS pour lequel les pertes sont probabilistes et les autres actions non-déterministes). Soit alors $M_{\mathcal{L}} = (X, N, P, P_0)$ son processus de décision markovien associé. Si f est un état particulier de X, nous nous intéressons au problème suivant : :
Pour tout adversaire σ a-t-on $\langle M, \sigma \rangle \models_{p=1} \Box\Diamond f$?

Ce problème est indécidable. Nous le montrons en lui réduisant un problème lui même indécidable, le problème de savoir si le canal d'un système à canal non fiable est borné.

Présentons d'abord le problème que nous allons réduire et qui est indécidable. On note $BLCS$ le problème suivant : «Étant donnés un système à canaux non fiables $\mathcal{L}$ et son état initial $\langle q_0, \epsilon \rangle$, les exécutions de $\mathcal{L}$ à partir de $\langle q_0, \epsilon \rangle$ ont-elles un canal borné ?»

Ce problème a été prouvé indécidable dans [May00].

En fait, Mayr montre l'indécidabilité du problème pour les machines à compteurs non fiables. Ce résultat s'applique aux systèmes à canaux non fiables car un tel système peut simuler le comportement d'une machine à compteurs non fiables.

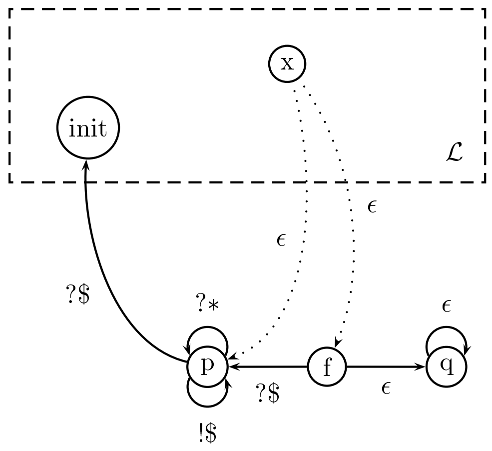


FIG. 5.1 – Construction d'un processus de décision markovien à partir d'un LCS

Nous allons maintenant énoncer le problème auquel $BLCS$ sera réduit. Soit donc P_1 : «Étant donnés un système de décision markovien S et f un état de contrôle de S, est-il vrai que pour tout adversaire σ, $\mathbb{P}(S, \sigma \models \Box\Diamond f) = 1$?»

Voici à présent la réduction de $BLCS$ à P_1. À partir d'un LCS $\mathcal{L}$, on construit un système de décision markovien S et un état particulier f de S de telle sorte que :

$$\exists\sigma,\ \mathcal{P}(S, \sigma \models \Box\Diamond f) > 0 \text{ si, et seulement si } \mathcal{L} \text{ non borné.}$$

De tous les états de $\mathcal{L}$ (y compris $init$) partent deux transitions vers q et f étiquetées par ϵ. On introduit un nouveau symbole \$ qui n'est pas dans l'alphabet de canal de $\mathcal{L}$. $*$ représente n'importe quelle lettre de l 'alphabet du canal de $\mathcal{L}$. Dans l'état q on vide le canal des messages accumulés lors du passage dans $\mathcal{L}$.

Montrons à présent la réduction de $BLCS$ à P_1 :

Théorème 5.1 $\exists\sigma,\ \mathbb{P}(S, \sigma \models \Box\Diamond f) > 0$ *si, et seulement si* $\mathcal{L}$ *non borné.*

Démonstration ($\Longleftarrow$) On suppose dans un premier temps que $\mathcal{L}$ est non borné.

Nous avons tout d'abord besoin d'un lemme pour construire une suite croissante de probabilité différentes de 1 et donc le produit n'est pas nul.

Lemme 5.2 $\exists p_1,\ p_2, \cdots \in \mathbb{R}$ *tels que :*

1. $p_1 < p_2\ ... < p_i <\ ... < 1$
2. $\prod_{i=1}^{\infty} p_i > 0$

Démonstration Définir par exemple $p_i = 1 - \frac{1}{(i+1)^2}$. On a alors $\prod_{i=1}^{\infty} p_i = \frac{\pi^2}{6} - 1$. □

Le lemme suivant nous permet à présent de construire un adversaire assurant presque sûrement le passage en f infiniment souvent.

Lemme 5.3 *$\forall n \in \mathbb{N}$, $\exists s_n$ état de $\mathcal{L}$, $\exists w_n$ mot sur l'alphabet de $\mathcal{L}$ et $\exists \pi_n$: $\langle init, \epsilon\rangle \to \langle s_n, w_n\rangle$ tels que la probabilité de passer de $\langle s_n, w_n\rangle$ à $\langle s_n, \epsilon\rangle$ en perdant tout le contenu du canal est inférieure à $1 - p_n$: $\mathbb{P}(\langle f, w_n\rangle \to \langle f, \epsilon\rangle) < 1 - p_n$.*

Ce lemme découle du fait que $\mathcal{L}$ est non borné et utilise que la probabilité de perte augmente avec le nombre de messages dans le canal.

Remarque 5.4 *Dans π_n, les états parcourus mais aussi les actions effectuées et les pertes subies sont importantes.*

L'action de l'adversaire se décompose en phases indexées par les entiers. Nous allons décrire la n-ème phase.

L´état initial est l'état initial de $\mathcal{L}$, à savoir $init$. À partir de $init$, l'adversaire σ tente de former π_n. Si les pertes s'accordent avec celles espérées, σ continue de suivre π_n. Si à un instant, on s'écarte du chemin π_n, σ sort de $\mathcal{L}$ pour atteindre l'état q. Si au contraire, σ parvient à atteindre $\langle s_n, w_n\rangle$ en suivant π_n, il quitte s_n pour f.

Dans l'état q, σ vide le canal par $?*$ en écrivant \$ pour marquer la fin. Lorsque le canal ne contient plus de lettres de $\mathcal{L}$, c'est-à-dire lorsque \$ est en tête de canal (si le canal est vide, σ réécrit \$ jusqu'à ce qu'il puisse le lire), σ exécute la transition de q à $init$ en lisant \$ sur le canal.

Dans l'état f, si le canal n'est pas vide σ réalise la transition de f vers q. Sinon, σ oriente l'exécution vers l'état puits p.

Ayant décrit σ, on peut maintenant montrer qu'un ensemble non négligeable des exécutions de S cohérentes avec σ visite infiniment souvent l'état de contrôle f.

Depuis l'état initial $init$, la probabilité est non nulle que les pertes coïncident avec celles le long de π_n et donc, la probabilité est non nulle pour σ de former correctement π_n et d'atteindre $\langle s_n, w_n\rangle$. Puisque la phase n est répétée tant que π_n n'est pas réussi, presque toutes les exécutions en phase n atteindrons $\langle s_n, w_n\rangle$.

Ensuite, la probabilité de tout perdre lorsqu'on se trouve en $\langle f, w_n\rangle$ est strictement inférieure à $1 - p_n$. Et donc l'ensemble des exécutions qui visitent f lors de la n-ème phase est de mesure strictement supérieure à p_n. Alors, l'ensemble des chemins qui visitent infiniment souvent f est de mesure supérieure au produit des p_n pour $n \in \mathbb{N}$.

Finalement, $\mathbb{P}(\pi | \pi \vDash \Box\Diamond f) \geq \prod_{i=1}^{\infty} p_i > 0$.

($\Longrightarrow$) Nous montrons cette implication par la contraposée. Supposons donc que lors des exécutions dans $\mathcal{L}$, le canal est borné.

Soit σ un adversaire quelconque. On considère l'ensemble des exécutions cohérentes avec σ qui visitent infiniment souvent l'état f. Si π visite une infinité

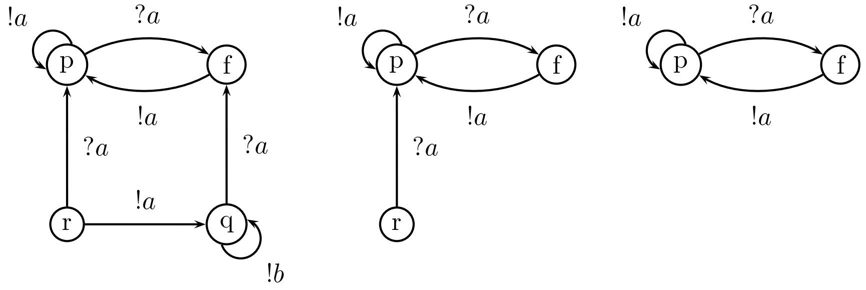


Fig. 5.2 – Élagage sur un exemple de PDM

de fois f alors puisque $\mathcal{L}$ est borné, π visite également presque sûrement un état global $\langle f, w\rangle$ infiniment souvent. $\mathbb{P}(\{\pi,\ \exists w,\ \pi \vDash \Box\Diamond\langle f, w\rangle | \pi \vDash \Box\Diamond f\}) = \mathbb{P}(\{\pi \vDash \Box\Diamond f\})$.

Depuis $\langle f, w\rangle$, la probabilité est non nulle de perdre tous les messages du canal et donc d'arriver dans $\langle f, \epsilon\rangle$. Ainsi, là encore presque sûrement, π perdra tous les messages du canal à partir de $\langle f, w\rangle$.$\mathbb{P}(\{\pi \vDash \Diamond\langle f, \epsilon\rangle | \pi \vDash \Box\Diamond\langle f, w\rangle\}) = \mathbb{P}(\{\pi,\ \exists w,\ \pi \vDash \Box\Diamond\langle f, w\rangle\})$.

Dans ce cas, la seule transition possible est $\langle f, \epsilon\rangle \to \langle p, \epsilon\rangle$. Finalement π se termine dans p et ne peut visiter infiniment souvent f.

D'où l'égalité : $\mathbb{P}(\{\pi \vDash \Diamond\langle p, \epsilon\rangle | \pi \vDash \Box\Diamond f\}) = \mathbb{P}(\{\pi \vDash \Box\Diamond f\})$. Cette dernière égalité est possible uniquement si $\mathbb{P}(\{\pi \vDash \Box\Diamond f\}) = 0$. On a donc $\forall\sigma,\ \mathbb{P}(S, \sigma \vDash \Box\Diamond f) = 0$. Ceci termine la démonstration. $\Box$

5.2 Problème d'existence d'un adversaire satisfaisant

Soit $\mathcal{L}$ un système non-déterministe à canaux à pertes stochastiques. Soit $M_{\mathcal{L}} = (X, N, P, P_0)$ le processus de décision markovien associé. Si f est un état particulier de X, nous nous intéressons au problème suivant : :
Existe-t-il un adversaire σ tel que $\langle M_{\mathcal{L}}, \sigma\rangle \vDash_{p=1} \Box\Diamond f$?

Nous montrons que ce problème est décidable dans le cadre des systèmes à canaux à pertes probabilistes et donnons une méthode de construction d'un tel adversaire, quand il existe.

Nous ne considérerons que des systèmes où seules les pertes sont probabilistes. Les autres actions (action interne, lecture ou écriture sur le canal) sont non-déterministes.

Soit donc M un processus de décision markovien d'état initial x_0 et f un état de contrôle de ce processus. Puisqu'à chaque instant il est possible (la probabilité est non nulle) de perdre tous les messages du canal, il faut envisager cette possibilité et exiger que depuis tous les états de contrôle, on peut atteindre l'état f même en partant avec un canal vide. S'il existe dans X des états à partir desquels quand le canal est vide, f n'est plus atteignable, on enlève ces états ainsi que toutes les transitions qui en partent ou qui y arrivent. On répète cette étape plusieurs fois jusqu'à ce que l'ensemble X se stabilise.

La figure 5.2 illustre cette manipulation « d'élagage ».

Dans l'exemple ci-dessus, à la première étape, l'état q est retiré. En effet, partant de $\langle q, \emptyset \rangle$, il est impossible d'atteindre f. Par contre pour l'état p par exemple, le déroulement suivant est possible s'il n'y a pas de perte : $\langle p, \emptyset \rangle \to^{!a} \langle p, a \rangle \to^{?a} \langle f, \emptyset \rangle$. D'autres chemins sont possibles, en écrivant plusieurs a sur le canal si les pertes épargnent au moins un message.

Une fois l'état q enlevé avec toutes les transitions le concernant, l'état r ne permet plus d'atteindre f si on part avec un canal vide. Alors cet état est mis de côté à son tour. Les états p et f eux peuvent toujours à partir d'un canal vide atteindre f (en au moins un coup pour f).

Pour cet exemple, à la fin du troisième passage, le système s'est stabilisé. Il est représenté à droite sur la figure ci-dessus.

Une fois cette opération terminée, on obtient un nouveau LCS $\mathcal{L}$ et son système de décision markovien associé $M_{\mathcal{L}'}$ qui est une restriction de M.

Théorème 5.5 *Il existe un adversaire σ tel que $\langle M', \sigma \rangle \models_{p=1} \Box\Diamond f$ si, et seulement si x_0 est un état de M'.*

Démonstration $(\Leftarrow)$

Cette implication est simple et nous la montrons par la contraposée. Supposons que x_0 ne soit pas un état de M'. Alors $\langle x_0, \epsilon \rangle$ ne permet pas d'atteindre l'état f et donc $\langle M', \sigma \rangle \models_{p=1} \neg\Diamond f$. Même en supposant que le canal n'est pas vide au départ, la probabilité étant non nulle de perdre tout le contenu du canal, on aurait $\mathbb{P}(\{\pi | \pi \models \Diamond f\}) < 1$ et a fortiori $\mathbb{P}(\{\pi | \pi \models \Box\Diamond f\}) < 1$.

$(\Rightarrow)$

Pour montrer cette implication, nous allons construire un adversaire et montrer qu'il est satisfaisant.

On construit un arbre orienté T de racine $\langle f, \epsilon \rangle$. Les sommets de T sont des couples $\langle q, w \rangle$ où q est un état de X et w représente le contenu du canal. T se construit de proches en proches. Lorsqu'on considère le sommet $\langle q, w \rangle$, si p est un prédécesseur de q dans M', $p \to^{alpha} q$ on ajoute le sommet $\langle p, w' \rangle$ et l'arête $\langle p, w' \rangle \to^{alpha} \langle q, w \rangle$ dans T où :

- si $\alpha = ?a$, $w' = a \cdot w$,
- si $\alpha = !a$ et $w = v \cdot a$, $w' = v$,
- si $\alpha = !a$ et $w \neq v \cdot a$, $w' = w$, et
- si $\alpha = \tau$, $w' = w$.

On arrête un branche lorsqu'on construit un sommet $\langle q, \epsilon \rangle$ (en faisant une exception pour la racine, bien entendu) ou un sommet $\langle q, w \rangle$ et qu'un de ses ancêtres est $\langle q, w' \rangle$ avec w' sous-mot de w.

Pour l'exemple ci-dessus, l'arbre T est celui représenté fugure 5.3.

Une fois l'arbre T construit, on peut définir l'adversaire simplement. Chaque arête de l'arbre est une règle d'évolution. On les liste de la racine de l'arbre aux feuilles. On parcourt ensuite cette liste pour trouver la première règle qui convient et l'appliquer : si on se trouve dans l'état $\langle q, w \rangle$, on peut appliquer les règles pour lesquelles le premier terme est de la forme $\langle q, v$ où w est un sur-mot de v et $w_1 = v_1$ (où w_1 est la première lettre du mot w). Si aucun sommet autre que la racine n'est étiqueté par $\langle f, w \rangle$, l'adversaire peut choisir n'importe quelle transition possible depuis f. En appliquant cette méthode, l'adversaire essaie toujours de remonter vers la racine de l'arbre, à savoir $\langle f, \epsilon \rangle$.

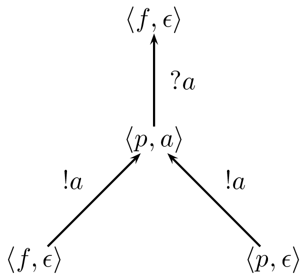


FIG. 5.3 – Arbre T pour l'exemple de la figure 5.2

Toujours pour notre exemple, la liste de règles est la suivante :

$$\langle p, a \rangle \rightarrow^{?a} \langle f, \epsilon \rangle, \ \langle f, \epsilon \rangle \rightarrow^{!a} \langle p, a \rangle, \ \langle p, \epsilon \rangle \rightarrow^{!a} \langle p, a \rangle$$

Il est important d'emprunter la première règle de la liste qui convient car on augmente alors les chances d'atteindre f rapidement. Cependant, il serait possible d'utiliser n'importe quelle règle qui convient.

On dit qu'une transition $\langle q, w \rangle \rightarrow^{\alpha} \langle p, v \rangle$ est *parfaite* si l'adversaire exécute la transition $\langle q, w \rangle \rightarrow^{\alpha} \langle p, v \rangle$ correspondant à une arête de l'arbre et qu'après les pertes, on se trouve encore dans l'état $\langle p, v \rangle$ (c'est-à-dire que l'état de contrôle est p et le contenu du canal est un mot v' sur-mot de v tel que ${v'}_1 = v_1$).

À chaque étape, la probabilité est non nulle que la transition soit parfaite, et même la probabilité est non nulle qu'il y ait n transitions parfaites successives, si n est la hauteur de l'arbre. Puisque T est fini, au moins un de ses sommets est visité infiniment souvent. Alors si on applique le lemme 2.16 il vient que f sera visité infiniment souvent avec probabilité 1.

L'adversaire que nous avons décrit est donc satisfaisant : $\langle M', \sigma \rangle \models_{p=1} \Box\Diamond f$.
$\Box$

Théorème 5.6 *Le problème P_2 est décidable.*

5.3 Adversaire à mémoire finie

Le problème précédent restreint aux adversaires à mémoire finie devient décidable. On le prouve en utilisant la décidabilité de P_2. Définissons tout d'abord P_3 :

P_3 : «Étant donné un système de décision markovien S et un état f de S, a-t-on $\forall\sigma$ à mémoire finie $\mathbb{P}(S, \sigma \models \Box\Diamond f) = 1$?»

Il est clair que P_3 est une restriction de P_2. Le rapport avec P_1 n'est pas immédiat. Il apparaît en fait que pour ce qui est des adversaires à mémoire finie, l'existence d'un adversaire satisfaisant est équivalente à l'existence d'un adversaire pour lequel l'ensemble des exécutions visitant infiniment souvent f est de mesure non nulle. Plus précisément, on a le lemme suivant :

$$\sigma \xrightarrow{u_0} \overset{p_0}{\text{———}} \sigma \xrightarrow{u_1} \overset{p_1}{\text{———}} \cdots \cdots \xrightarrow{u_n} \overset{p_n}{\text{———}} \langle f, w\rangle$$

FIG. 5.4 – Exemple de chemin de σ à f

Lemme 5.7 *Soit x_0 l'état initial de S.*

Alors, les deux assertions suivantes sont équivalentes.

1. *$\exists u$ adversaire à mémoire finie tel que $\mathbb{P}(\langle x_0, \epsilon\rangle, u \vDash \Box\Diamond f) > 0$.*
2. *f est atteignable depuis x_0 et $\exists u$ tel que $\mathbb{P}(\langle f, \epsilon\rangle, u \vDash \Box\Diamond f) = 1$.*

Démonstration Nous allons prouver ce lemme dans le cas des adversaires sans mémoire. La preuve pour le cas des adversaires à mémoire finie faisant intervenir des notations plus lourdes mais suivant néanmoins le même schéma.

($\Longleftarrow$) On suppose dans un premier temps que depuis $\langle x_0, \epsilon\rangle$ on peut atteindre $\langle f, \epsilon\rangle$ et qu'il existe un adversaire u tel que l'ensemble des exécutions commençant en $\langle f, \epsilon\rangle$ et visitant infiniment souvent f est de mesure 1. Puisque f est atteignable depuis l'état initial, la probabilité est non nulle d'atteindre $\langle f, \epsilon\rangle$: $\mathbb{P}(\{\pi \vDash \Diamond\langle f, \epsilon\rangle) = p > 0$. On utilise ensuite l'adversaire donné en hypothèse pour visiter f infiniment souvent.

($\Longrightarrow$) Supposons à présent l'existence d'un adversaire sans mémoire u tel que $\mathbb{P}(\langle x_0, \epsilon\rangle, u \vDash \Box\Diamond f) > 0$. On a alors besoin du sous-lemme suivant :

Sous-lemme 5.8 *Soit u un adversaire à mémoire finie. Si $\mathbb{P}(\langle x_0, \epsilon\rangle, u \vDash \Box\Diamond f) > 0$ alors $\mathbb{P}(\langle x_0, \epsilon\rangle, u \vDash \Box\Diamond\langle f, \epsilon\rangle) > 0$.*

Preuve Ici encore on suppose que l'adversaire est sans mémoire, le résultat restant vrai pour les adversaires à mémoire finie.

Si S_0 est l'ensemble des configurations à canal vide, on a déjà montré que presque sûrement S_0 est visité infiniment souvent : $\mathbb{P}(\langle x_0, \epsilon\rangle, u \vDash \Box\Diamond S_0) = 1$. On sait d'autre part par hypothèse que l'ensemble des exécutions qui visitent f infiniment souvent n'est pas négligeable. On en déduit donc $\mathbb{P}(\langle x_0, \epsilon\rangle, u \vDash \Box\Diamond S_0 \wedge \Box\Diamond f) > 0$. Supposons que toute configuration σ de S_0 vérifie $\mathbb{P}(\langle x_0, \epsilon\rangle, u \vDash \Box\Diamond\sigma \wedge \Box\Diamond f) = 0$. Puisque S_0 est fini, on aurait alors $\mathbb{P}(\langle x_0, \epsilon\rangle, u \vDash \Box\Diamond S_0 \wedge \Box\Diamond f) = 0$ ce qui est absurde donc il existe une configuration σ de S_0 telle que $\mathbb{P}(\langle x_0, \epsilon\rangle, u \vDash \Box\Diamond\sigma \wedge \Box\Diamond f) > 0$.

À la figure 5.3 on considère une partie d'une exécution qui visite infiniment souvent à la fois f et σ. Les flèches étiquettées par u représentent l'action réalisée par l'adversaire. Les arêtes étiquetées par p représentent les pertes « subies » à la fin de ces actions. Après avoir réalisé u_n, si les pertes sont totales, on obtient l'état $\langle f, \epsilon\rangle$. Sur ce chemin particulier de σ à f, les probabilités $p_0, \cdots p_n$ sont non nulles. D'autre part l'adversaire σ est sans mémoire (il fait donc le choix de la transition à exécuter en ne connaissant que l'état courant). Alors, si σ est visité infnimment souvent, les pertes seront infiniment souvent $p_0, \cdots p_n$ et u exécutera les actions $u_0, \cdots u_n$. Ainsi, sous l'hypothèse de passer infiniment souvent par la configuration σ, $\langle f, \epsilon\rangle$ sera visité infiniment souvent. On a donc l'inégalité $\mathbb{P}(\langle x_0, \epsilon\rangle, u \vDash \Box\Diamond\langle f, \epsilon\rangle) \geq \mathbb{P}(\langle x_0, \epsilon\rangle, u \vDash \Box\Diamond\sigma \wedge \Box\Diamond f) > 0$ D'où le résultat suivant :

$$\mathbb{P}(\langle x_0, \epsilon\rangle, u \vDash \Box\Diamond\langle f, \epsilon\rangle) > 0.$$

Ceci termine la démontration du sous-lemme 5.8, dans le cas où u est un adversaire sans mémoire. □

On peut à présent reprendre la démonstration du lemme 5.7.

On définit une notation $\Diamond_k$ telle que $\Diamond_k\Phi$ est vrai si, et seulement si Φ est vraie k fois lors de l'exécution. On peut exprimer $\Diamond_k$ à l'aide de $\Diamond_{k-1}$ (et donc de $\Diamond$ par récurrence) : $\forall\Phi,\ \Diamond_k\Phi \equiv \Diamond(\Phi \wedge \bigcirc\Diamond_{k-1}\Phi)$. On pose ensuite $L_k = \{\pi \vDash \Diamond_k f\}$ comme l'ensemble des exécutions qui visitent au moins k fois l'état f. Soit p_k la mesure de l'ensemble L_k : $p_k = \mathbb{P}(L_k)$. Pour passer $k+1$ fois dans l'état f, il faut y passer k fois et à partir de là y repasser encore une fois. Ces deux évènements sont indépendants. Alors, la mesure de $L_{k=1}$ est le produit de la mesure de L_k par celle de L_1, c'est-à-dire $p_{k+1} = p_k \cdot p_1$. On obtient donc que pour tout $k \in \mathbb{N},\ p_k = (p_1)^k$. Il est d'autre part vrai que la probabilité de passer au moins k fois par l'état f est inférieur à celle d'y passer au moins $k-1$ fois. Ainsi la suite $(p_i)_{i\geq 1}$ est décroissante : $p_1 \geq p_2 \geq \cdots \geq p_{k-1} \geq p_k \cdots$.

On définit à présent p_∞ la mesure de l'ensemble des chemins qui visitent infiniment souvent f. Alors p_∞ est la borne inférieure des p_k : $p_\infty = \liminf\limits_{k\to\infty} p_k$. Supposons que $p_\infty < 1$. Alors il existe $k \geq 1$ tel que $p_k < 1$ (sinon, $\forall k \geq 1,\ p_k = 1$ et alors $p_\infty = 1$). Puisque $p_k = (p_1)^k$, il vient alors $p_1 < 1$. Enfin pour tout $k \geq 1$, $p_\infty \leq p_k = (p_1)^k$. De $p_1 < 1$, on déduit donc $p_\infty = 0$. On a donc prouvé que si $\Box\Diamond f$ n'est pas vraie avec probabilité 1, alors $\Box\Diamond f$ est presque sûrement faux : $p_\infty < 1 \Rightarrow p_\infty = 0$.

On sait par hypothèse que sous l'adversaire u, la probabilité de visiter infiniment souvent f est non nulle. D'après ce qui précède on peut alors conclure que $p_\infty = 1$. Presque toutes les exécutions cohérentes avec u visitent infiniment souvent f. □

Le lemme 5.7 nous permet donc de nous ramener au problème d'existence d'un adversaire satisfaisant résolu dans la partie 5.2. On peut donc énoncer le théorème :

Théorème 5.9 *Soit P_3 le problème : « Étant donnés un processus de décision markovien S et une formule de LTL Φ, existe-t-il un adversaire à mémoire finie u tel que $\mathbb{P}(S, u \vDash \Phi) > 0$? ». Alors, P_3 est décidable.*

Démonstration La démonstration découle du théorème 1 et du lemme 5.7. □

Conclusion

L'objet de ce travail était d'étudier les systèmes stochastiques et en particulier les systèmes à canaux à pertes stochastiques, en y alliant parfois du non-déterminisme. Notre étude s'appuyait au départ sur les travaux de Baier et Engelen dans [BE99] pour les PLCS et de Coucourbetis et Yannakakis [CY90] pour les systèmes probabilistes concurrents, c'est-à-dire modélisé par des PDM. Il semblait intéressant de considérer les systèmes stochastiques vue l'importance et la diversité de leurs applications pour modéliser des systèmes informatiques comme nous l'avons vu dans l'introduction.

Nous avons commencé par introduire les définitions de chaînes de Markov et processus de décision markoviens qui modélisent respectivement les systèmes à canaux à pertes stochastiques et les systèmes non déterministes à canaux à pertes stochastiques.

À partir de ces notions, nous avons discuté de la définition des pertes stochastiques dans les quelques articles sur les PLCS [BE99] [ABPJ00] [PN97]. Cette définition n'était pas satisfaisante pour deux raisons essentiellement. Premièrement, contrairement à ce qui se passe en pratique, la probabilité de perte ne dépendait pas du contenu du canal. Deuxièmement, les résultats de décidabilité obtenus dans [BE99] n'était valables que pour des probabilités de perte élevées (de l'ordre de $\frac{1}{2}$). Nous avons donc défini une nouvelle probabilité de perte, augmentant lorsque le contenu du canal augmente et laissant espérer des résultats de décidabilité pour un taux de perte quelconque, voire même inconnu.

En suivant la démarche de Baier et Engelen, nous avons alors montré la décidabilité de la vérification avec probabilité 1 de formules de la logique du temps linéaire LTL pour les PLCS, et ce quel que soit le taux de perte non nul. Contrairement aux articles existant à notre connaissance, nous avons également considéré dans ce résultat le cas des processus à ensemble d'état infini dénombrable.

Pour ce qui est des LCS à pertes stochastiques, toutes les autres actions étant déterministes, nous avons rappelé la notion d'adversaire décrivant l'action de l'extérieur du système [Var85] [CY90]. Puis toujours en considérant des processus de décision markoviens dénombrables (et plus uniquement finis), nous avons examiné trois problèmes. Tout d'abord la vérification avec probabilité 1 de formules de LTL quel que soit l'adversaire, c'est-à-dire même face à un environnement le plus adverse. Ce problème a été prouvé indécidable par une réduction du problème du canal borné pour un LCS, lui même indécidable [May00]. Cette indécidabilité est à mettre en regard du résultat de décidabilité obtenu pour les systèmes uniquement probabilistes. Nous avons ensuite donné un algorithme permettant de décider de l'existence d'un adversaire satisfaisant (sous lequel une formule de LTL est vérifiée avec probabilité 1) et de le construire le cas échéant.

Enfin, nous avons montré que lorsqu'on se restreint aux adversaires à mémoire finie, le problème d'universalité des adversaires satisfaisant devient décidable.

Ce travail de DEA nous a permis de « côtoyer » à la fois les systèmes stochastiques et surtout les systèmes infinis par le biais de certains systèmes stochastiques infinis. Un prolongement de ce travail serait donc de se pencher à présent sur des systèmes infinis plus généraux, d'abord probabilistes puis quelconques.

Bibliographie

[ABPJ00] P. A. Abdulla, C. Baier, S. Purushothaman Iyer, and B. Jonsson. Reasoning about probabilistic lossy channel systems. In *Proc. 11th Int. Conf. Concurrency Theory (CONCUR'2000), University Park, PA, USA, Aug. 2000*, volume 1877 of *Lecture Notes in Computer Science*, pages 320–333. Springer, 2000.

[AJ96a] P. A. Abdulla and B. Jonsson. Undecidable verification problems for programs with unreliable channels. *Information and Computation*, 130(1) :71–90, 1996.

[AJ96b] P. A. Abdulla and B. Jonsson. Verifying programs with unreliable channels. *Information and Computation*, 127(2) :91–101, 1996.

[Alf97] L. de Alfaro. Temporal logics for the specification of performance and reliability. In *Proc. 14th Ann. Symp. Theoretical Aspects of Computer Science (STACS'97), Lübeck, Germany, Feb.-Mar. 1997*, volume 1200 of *Lecture Notes in Computer Science*, pages 165–176. Springer, 1997.

[BA95] A. Bianco and L. de Alfaro. Model checking of probabilistic and nondeterministic systems. In *Proc. 15th Conf. Found. of Software Technology and Theor. Comp. Sci. (FST&TCS'95), Bangalore, India, Dec. 1995*, volume 1026 of *Lecture Notes in Computer Science*, pages 499–513. Springer, 1995.

[BE99] C. Baier and B. Engelen. Establishing qualitative properties for probabilistic lossy channel systems : An algorithmic approach. In *Proc. 5th Int. AMAST Workshop Formal Methods for Real-Time and Probabilistic Systems (ARTS'99), Bamberg, Germany, May 1999*, volume 1601 of *Lecture Notes in Computer Science*, pages 34–52. Springer, 1999.

[BK98] C. Baier and M. Kwiatkowska. Model checking for a probabilistic branching time logic with fairness. *Distributed Computing*, 11(3) :125–155, 1998.

[Bré99] P. Brémaud. *Markov Chains, Gibbs fields, Monte Carlo simulations and Queues*. Springer, 1999.

[BZ83] D. Brand and P. Zafiropulo. On communicating finite-state machines. *Journal of the ACM*, 30(2) :323–342, 1983.

[CFI96] G. Cécé, A. Finkel, and S. Purushothaman Iyer. Unreliable channels are easier to verify than perfect channels. *Information and Computation*, 124(1) :20–31, 1996.

[CY90] C. Courcoubetis and M. Yannakakis. Markov decision processes and regular events (extended abstract). In *Proc. 17th Int. Coll. Automata, Languages, and Programming (ICALP'90), Warwick University, England, July 1990*, volume 443 of *Lecture Notes in Computer Science*, pages 336–349. Springer, 1990.

[CY95] C. Courcoubetis and M. Yannakakis. The complexity of probabilistic verification. *Journal of the ACM*, 42(4) :857–907, 1995.

[Der70] C. Derman. *Finite State Markovian Decision Processes.* Academic Press, New York, 1970.

[Fin94] A. Finkel. Decidability of the termination problem for completely specified protocols. *Distributed Computing*, 7(3) :129–135, 1994.

[LS82] D. Lehmann and S. Shelah. Reasoning with time and chance. *Information and Control*, 53 :165–198, 1982.

[May00] R. Mayr. Undecidable problems in unreliable computations. In *Proc. 4th Latin American Symposium on Theoretical Informatics (LATIN'2000), Punta del Este, Uruguay, Apr. 2000*, volume 1776 of *Lecture Notes in Computer Science*, pages 377–386. Springer, 2000.

[MS02] B. Masson and Ph. Schnoebelen. On verifying fair lossy channel systems. In *Proc. 27th Int. Symp. Math. Found. Comp. Sci. (MFCS'2002), Warsaw, Poland, Aug. 2002*, volume 2420 of *Lecture Notes in Computer Science*, pages 543–555. Springer, 2002.

[Nor98] J. Norris. *Markov Chains.* Cambridge University Press, 1998.

[Pan01] P. Panangaden. Measure and probability for concurrency theorists. *Theoretical Computer Science*, 253(2) :287–309, 2001.

[PN97] S. Purushothaman Iyer and M. Narasimha. Probabilistic lossy channel systems. In *Proc. 7th Int. Joint Conf. Theory and Practice of Software Development (TAPSOFT'97), Lille, France, Apr. 1997*, volume 1214 of *Lecture Notes in Computer Science*, pages 667–681. Springer, 1997.

[Sch02] Ph. Schnoebelen. Verifying lossy channel systems has nonprimitive recursive complexity. *Information Processing Letters*, 83(5) :251–261, 2002.

[Var85] M. Y. Vardi. Automatic verification of probabilistic concurrent finite-state programs. In *Proc. 26th IEEE Symp. Foundations of Computer Science (FOCS'85), Portland, OR, USA, Oct. 1985*, pages 327–338, 1985.

[Var99] M. Y. Vardi. Probabilistic linear-time model checking : An overview of the automata-theoretic approach. In *Proc. 5th Int. AMAST Workshop Formal Methods for Real-Time and Probabilistic Systems (ARTS'99), Bamberg, Germany, May 1999*, volume 1601 of *Lecture Notes in Computer Science*, pages 265–276. Springer, 1999.