Systèmes temporisés probabilistes
2009 - 2010

S. Haddad [1]

13 octobre 2010

1. Professeur de l'ENS Cachan, haddad@lsv.ens-cachan.fr, http://www.lsv.ens-cachan.fr/~haddad/

Table des matières

Chapitre 1

Chaînes de Markov : rappels

1.1 Un modèle stochastique de systèmes à événements discrets

Nous supposons connues du lecteur les bases de la théorie des probabilités. Pour plus de détails, on pourra se reporter aux ouvrages suivants : [FOA 98, FOA 02] en français ou [FEL 68, FEL 71] en anglais.

Notations

- $\Pr(E)$ désigne la probabilité d'un événement E et $\Pr(A \mid B)$ la probabilité de A sachant B.
- L'adverbe *presque*, dans des expressions telles que *presque partout* ou *presque sûrement*, signifie pour un ensemble de probabilité 1.
- $\mathbb{R}$ (resp. $\mathbb{R}^+, \mathbb{R}^{+*}$) désigne les réels (resp. les réels non négatifs, strictement positifs). Si x est un réel alors $\lfloor x \rfloor$ désigne sa partie entière.
- Si $E \subseteq \mathbb{R}$ alors $inf(E)$ (resp. $sup(E)$) désigne la borne inférieure (resp. supérieure) de E.

Une exécution d'un système à événements discrets (« Discrete Event System » DES) se caractérise par une suite (*a priori* infinie) d'événements $\{e_1, e_2, \ldots\}$ séparés par des intervalles de temps. Seuls les événements peuvent changer l'état du système.

Formellement, le comportement stochastique d'un DES est déterminé par deux familles de variables aléatoires :

- $S_0, \ldots, S_n, \ldots$ à valeurs dans l'espace (discret) des états du système, noté S. Dans la suite sauf mention explicite, nous supposerons que cet espace est fini. S_0 représente l'état initial du système et S_n $(n > 0)$ l'état courant après le $n^{ième}$ événement. L'occurrence d'un événement ne modifie pas nécessairement l'état du système, par conséquent S_{n+1} peut être égal à S_n.
- $T_0, ..., T_n, ...$ à valeurs dans $\mathbb{R}^+$ où T_0 représente l'intervalle de temps avant le premier événement et T_n $(n > 0)$ représente l'intervalle de temps entre le $n^{ième}$ et le $(n+1)^{ième}$ événement. Notons que cet intervalle peut être nul (*e.g.* une suite d'instructions considérées comme instantanées au regard de transactions de base de données avec des entrées/sorties).

Lorsque la distribution initiale S_0 est concentrée en un état s, on dira que le processus démarre en s (*i.e.* $\Pr(S_0 = s) = 1$).

A priori, aucune restriction n'est imposée sur ces familles de variables aléatoires. Cependant, pour les catégories de processus que nous étudierons, un DES ne peut exécuter une infinité d'actions en un temps fini (ce qu'on appelle aussi une exécution non Zénon). Autrement dit :

$$\sum_{n=0}^{\infty} T_n = \infty \; presque\ sûrement \tag{1.1}$$

Cette propriété nous autorise à définir l'état du système à tout instant. Soit $N(\tau)$, la variable

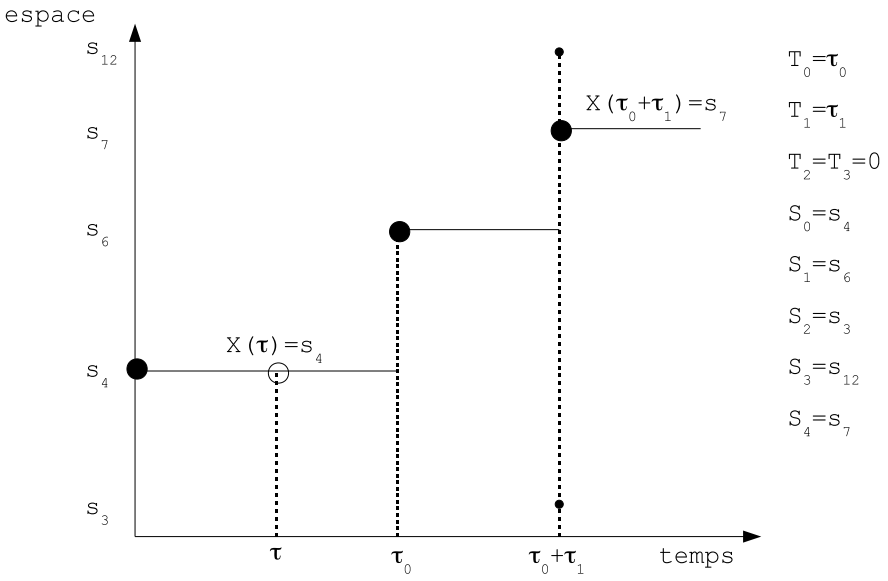

FIGURE 1.1 – Une réalisation du processus stochastique

aléatoire définie par :

$$N(\tau) =_{def} inf(\{n \mid \sum_{k=0}^{n} T_k > \tau\})$$

D'après l'équation (1.1), $N(\tau)$ est définie *presque partout*. Comme on peut le voir sur la figure 1.1, $N(\tau)$ présente des sauts d'amplitude supérieure à 1. L'état $X(\tau)$ du système à l'instant τ, est alors simplement $S_{N(\tau)}$. Il est important de noter que $X(\tau)$ n'est pas équivalent au processus stochastique, mais qu'il permet, dans la plupart des cas, de procéder aux analyses standard. Le schéma de la figure 1.1 présente une *réalisation* possible du processus et illustre l'interprétation de chacune des variables aléatoires introduites plus haut. Dans cet exemple, le processus est initialement dans l'état s_4 et y reste jusqu'à l'instant τ_0 où il passe dans l'état s_6. À l'instant $\tau_0 + \tau_1$, le système visite successivement en un temps nul, les états s_3 et s_{12} avant d'atteindre l'état s_7 où il séjourne un certain temps. L'observation $X(\tau)$ en temps continu occulte les états évanescents s_3 et s_{12} du processus.

L'évaluation de performance d'un DES conduit à deux types d'analyse :

- L'étude du comportement transitoire, c'est à dire l'obtention de mesures en fonction du temps écoulé depuis l'état initial. Cette étude vise les phases d'initialisation des systèmes et les systèmes à états terminaux. Parmi les domaines d'application, on peut citer l'analyse de fiabilité et de sûreté de fonctionnement.
- L'étude du comportement stationnaire du système. Pour de nombreuses applications, ce qui intéresse le modélisateur est le comportement du système une fois la phase initiale passée, lorsqu'il se stabilise.

Ceci suppose bien entendu qu'un tel comportement stationnaire existe. Ce qui se résume, en notant $\boldsymbol{\pi}(\tau)$ la distribution de $X(\tau)$, par :

$$\lim_{\tau \to \infty} \boldsymbol{\pi}(\tau) = \boldsymbol{\pi} \tag{1.2}$$

où $\boldsymbol{\pi}$ est aussi une distribution, appelée *distribution stationnaire*.

Les distributions transitoires ou stationnaires ne sont qu'un moyen de calculer des *indices de performance*. Par exemple, la probabilité stationnaire qu'un serveur soit opérationnel, la probabilité

qu'à l'instant τ, une connexion soit établie ou le nombre moyen de clients d'un service sont de tels indices.

Afin de raisonner de manière générique sur les DES, on supposera donné dans la suite un ensemble de fonctions définies sur l'ensemble des états et à valeurs dans $\mathbb{R}$. Ainsi une fonction f peut être vue comme un indice de performance et étant donnée une distribution $\boldsymbol{\pi}$, la quantité $\sum_{s \in S} \boldsymbol{\pi}(s) \cdot f(s)$ représente la mesure de cet indice.

Lorsque l'indice est une fonction à valeurs dans $\{0, 1\}$, on peut l'assimiler à une *proposition atomique* satisfaite en un état si la fonction vaut 1. Dans la suite on notera $\mathcal{P}$, l'ensemble des propositions atomiques et $s \vDash \phi$, avec s un état et ϕ une proposition atomique, le fait que s vérifie (ou satisfait) ϕ. Dans ce cas, étant donnée une distribution $\boldsymbol{\pi}$, la quantité $\sum_{s \vDash \phi} \boldsymbol{\pi}(s)$ représente la mesure de cet indice.

1.2 Chaînes de Markov à temps discret

Présentation

Une chaîne de Markov à temps discret (en anglais Discrete Time Markov Chain ou DTMC) possède les caractéristiques suivantes :

- L'intervalle de temps entre les instants T_n est une constante de valeur 1
- L'état suivant un état atteint ne dépend que de cet état et les probabilités de transition restent constantes [1] au cours du temps :

$$\Pr(S_{n+1} = s_j \mid S_0 = s_{i_0}, ..., S_n = s_i) =$$

$$\Pr(S_{n+1} = s_j \mid S_n = s_i) = p_{ij} =_{def} \mathbf{P}[i, j]$$

Nous utiliserons indifféremment les deux notations pour les transitions d'état.

Comportement transitoire et stationnaire d'une DTMC

Dans ce paragraphe nous rappelons des résultats classiques en fournissant des justifications intuitives qui ne sauraient constituer des preuves mathématiques. La plupart de celles-ci se trouvent dans les compléments théoriques.

L'analyse du comportement transitoire ne présente pas de difficulté. Les changements d'état se font aux instants $\{1, 2, \ldots\}$. Etant données une distribution initiale $\boldsymbol{\pi}_0$ et la matrice de transition $\mathbf{P}$, alors $\boldsymbol{\pi}_n$ la distribution de S_n (*i.e.* l'état de la chaîne à l'instant n) est donnée par la formule $\boldsymbol{\pi}_n = \boldsymbol{\pi}_0 \cdot \mathbf{P}^n$ qui s'obtient à l'aide d'une récurrence élémentaire.

L'analyse du comportement asympotique des DTMC (pour un ensemble d'états quelconque) conduit à la classification suivante des états :

- Un état s est *transitoire* si la probabilité d'y revenir est inférieure à 1. Par conséquent, sa probabilité d'occurrence $\Pr(S_n = s)$ tend vers 0 lorsque n tend vers l'infini. Un état est appelé *récurrent* s'il n'est pas transitoire.
- Un état est *récurrent nul* si la durée moyenne du retour à cet état est infinie. Intuitivement, une fois atteint, cet état apparaîtra à des intervalles dont la durée moyenne tendra vers l'infini et par conséquent sa probabilité d'occurrence tendra aussi vers 0. Ce raisonnement intuitif est mathématiquement justifié.
- Un état est *récurrent non nul* si la durée moyenne du retour à cet état est finie. Si une distribution stationnaire existe alors elle est concentrée sur les états récurrents non nuls.

Nous allons détailler cette analyse dans le cas d'un espace d'états fini. Considérons le graphe $G(\mathbf{P})$ construit de la manière suivante (voir la figure 1.2) :

- l'ensemble des sommets est l'ensemble des états de la chaîne ;
- il y a un arc de s_i à s_j si $p_{ij} > 0$.

Etudions les composantes fortement connexes (c.f.c.) de ce graphe (voir la figure 1.3). Si une c.f.c. a un arc sortant, alors nécessairement, les états de cette c.f.c. sont transitoires. A l'inverse, tous les états d'une c.f.c. puits (*i.e.* sans arc sortant) sont récurrents non nuls. Dans le cas extrême où une c.f.c. puits est réduite à un état s (*i.e.* $\mathbf{P}[s, s] = 1$), on dit que s est un état *absorbant*.

1. d'où le terme de chaîne *homogène* utilisé dans les études sur les chaînes de Markov en toute généralité

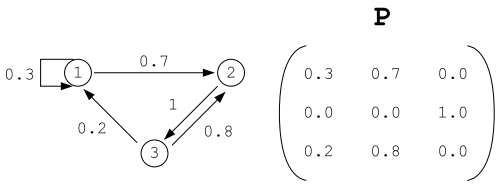

FIGURE 1.2 – Un exemple de DTMC

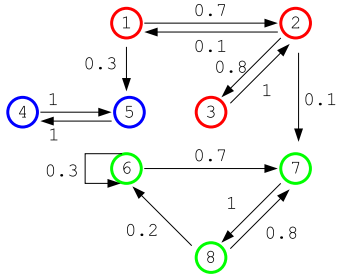

FIGURE 1.3 – Composantes fortement connexes d'une DTMC

Lorsque le graphe $G(P)$ est fortement connexe, la chaîne est dite *irréductible*. Dans le cas général, chaque c.f.c. puits constitue une sous-chaîne irréductible.

Etudions l'existence d'une distribution stationnaire dans le cas d'une chaîne irréductible. Remarquons d'abord qu'elle n'est pas toujours garantie. Ainsi, une chaîne constituée de deux états s_0 et s_1, de distribution initiale concentrée en un état et où $p_{0,1} = p_{1,0} = 1$, alterne entre les deux états et ne converge donc pas vers une distribution stationnaire. En généralisant, une chaîne irréductible est dite *périodique* de période $k > 1$ si on peut partitionner les états en sous-ensembles $S_0, S_1, \ldots, S_{k-1}$ tels que des états de S_i on accède, en un pas, exclusivement aux états de $S_{(i+1) \mod k}$. La périodicité est alors le plus grand k qui permet d'obtenir cette partition. La périodicité d'une chaîne se détermine par un algorithme en temps linéaire (par rapport à la taille du graphe) dont nous décrivons les principes et que nous illustrons sur la figure 1.4. On construit un arbre orienté couvrant les sommets par un parcours en largeur. Il n'est pas nécessaire de faire un parcours en largeur mais celui-ci est le plus efficace car il minimise la hauteur de l'arbre. Ce parcours en largeur détermine une hauteur des sommets noté h. On affecte un poids aux arcs du graphe : le poids $w(u, v)$ d'un arc (u, v) est défini par $h(u) - h(v) + 1$ ainsi les arcs de l'arbre ont un poids nul. La périodicité du graphe est alors le pgcd des poids non nuls des arcs.

Prouvons cette affirmation. Appelons d la périodicité du graphe et notons $S_0, \ldots, S_{d-1}$ la partition des états avec $r \in S_0$ où r est la racine de l'arbre. Appelons d' le pgcd des poids des arcs.

Soient deux chemins ayant même origine et même extrémité, la différence de longueurs entre ces chemins doit être un multiple de d par définition de la périodicité.

- Soit un arc (u, v) de poids non nul. Appelons σ_u, le chemin de r à u le long de l'arbre et σ_v le chemin de r à v le long de l'arbre. La longueur de σ_u est $h(u)$, celle de σ_v est $h(v)$. A l'aide de l'arc (u, v), on obtient un nouveau chemin $\sigma_u v$ de r à v. La différence de longueur entre les deux chemins est égale à $h(u) - h(v) + 1 = w(u, v)$. Par conséquent $d | w(u, v)$. Ceci étant vrai pour tout arc (u, v), on en déduit que $d | d'$.
- Partitionnons maintenant les états en $S'_0, \ldots, S'_{d'-1}$ avec $s \in S'_i$ ssi $h(s) \mod d' = i$. Par construction, un arc de l'arbre joint un sommet de S'_i à un sommet de $S'_{i+1 \mod d'}$. Un arc (u, v) hors de l'arbre joint $u \in S'_{h(u) \mod d'}$ à $v \in S'_{h(v) \mod d'}$ mais $h(u) - h(v) + 1$

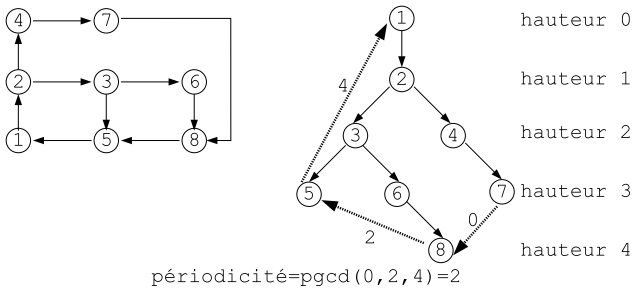

FIGURE 1.4 – Un calcul de périodicité

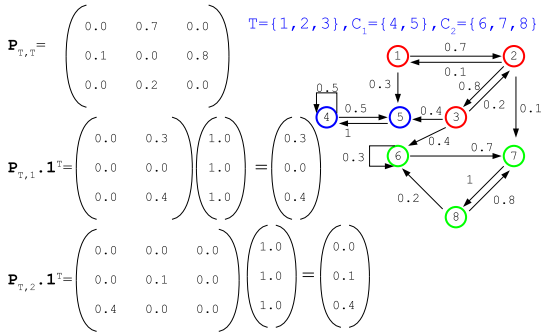

FIGURE 1.5 – Une DTMC non irréductible et des sous-matrices

mod $d' = 0$. Par conséquent, $S'_{h(v) \mod d'} = S'_{h(u)+1 \mod d'}$. Par définition, de la périodicité $d' \leq d$. Puisque $d|d'$, on obtient $d = d'$.

Il s'avère qu'une chaîne irréductible et apériodique (dite alors *ergodique*) admet une distribution stationnaire et que celle-ci est *indépendante de la distribution initiale*. Le calcul de cette distribution est relativement facile. En effet, on a $\boldsymbol{\pi}_{n+1} = \boldsymbol{\pi}_n \cdot \mathbf{P}$. En passant à la limite (justifiée), on obtient $\boldsymbol{\pi} = \boldsymbol{\pi} \cdot \mathbf{P}$. De plus, $\boldsymbol{\pi}$ est la seule distribution solution de :

$$\mathbf{X} = \mathbf{X} \cdot \mathbf{P} \tag{1.3}$$

Remarquons qu'une distribution initiale, solution de cette équation, est *invariante* : quelque soit l'instant d'observation la distribution courante est identique à la distribution initiale. Afin de résoudre l'équation (1.3), on peut procéder à un calcul direct en complétant par l'équation de normalisation $\mathbf{X} \cdot \mathbf{1}^T = 1$ où $\mathbf{1}^T$ désigne le vecteur colonne composé de 1. Mais les calculs itératifs sont plus intéressants si l'espace d'états est de taille importante. Le plus simple consiste à itérer $\mathbf{X} \leftarrow \mathbf{X} \cdot \mathbf{P}$ [STE 94].

Intéressons-nous maintenant au cas (presque) général en supposant uniquement que les c.f.c. puits appelées aussi c.f.c. terminales (notées $\{\mathcal{C}_1, \ldots, \mathcal{C}_k\}$) sont apériodiques de distributions stationnaires $\{\boldsymbol{\pi}_1, \ldots, \boldsymbol{\pi}_k\}$ (voir la figure 1.5). Dans ce cas, la chaîne admet aussi une distribution stationnaire (qui cette fois-ci dépend de la distribution initiale). Cette distribution est donnée par la formule $\boldsymbol{\pi} = \sum_{i=1}^{k} \Pr(\text{d'atteindre } \mathcal{C}_i) \cdot \boldsymbol{\pi}_i$. Il reste donc à calculer la probabilité d'atteindre une c.f.c. puits. On évalue cette quantité en partant d'un état fixé puis on la conditionne suivant la distribution initiale : $\Pr(\text{d'atteindre } \mathcal{C}_i) = \sum_{s \in S} \boldsymbol{\pi}_0(s) \cdot \boldsymbol{\pi}'_{\mathcal{C}_i}(s)$ où $\boldsymbol{\pi}'_{\mathcal{C}_i}(s) = \Pr(\text{d'atteindre } \mathcal{C}_i \mid S_0 = s)$. Soit $\mathbf{P}_{T,T}$ la sous-matrice de transition de la chaîne restreinte aux états transitoires et soit $\mathbf{P}_{T,i}$ la sous-matrice de transition de la chaîne des états transitoires vers les états de $\mathcal{C}_i$, alors $\boldsymbol{\pi}'_{\mathcal{C}_i} = (\sum_{n \geq 0} (\mathbf{P}_{T,T})^n) \cdot \mathbf{P}_{T,i} \cdot \mathbf{1}^T = (\mathbf{I} - \mathbf{P}_{T,T})^{-1} \cdot \mathbf{P}_{T,i} \cdot \mathbf{1}^T$. La première égalité s'obtient en

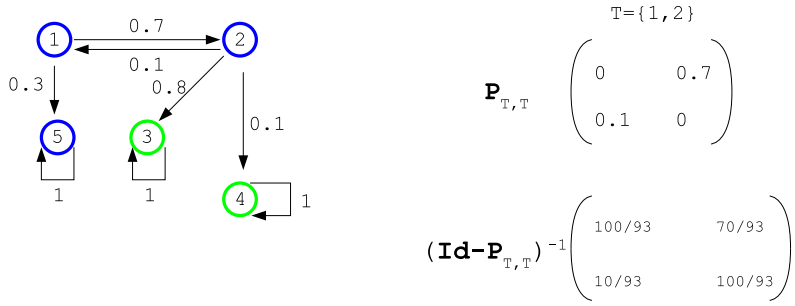

FIGURE 1.6 – Comportement transitoire d'une DTMC non irréductible

conditionnant l'accessibilité de $\mathcal{C}_i$ par la longueur possible du chemin qui y conduit tandis que la seconde se vérifie immédiatement.

Notons une dernière propriété des chemins dans une DTMC (propriété que nous utiliserons à plusieurs reprises) :

Presque sûrement un chemin aléatoire infini se termine dans un c.f.c. puits et visite infiniment souvent tous ses états.

1.3 Chaînes de Markov à temps continu

Présentation

Une chaîne de Markov à temps continu (en anglais Continuous Time Markov Chain ou CTMC) a les caractéristiques suivantes :

- L'intervalle de temps entre les instants T_n est une variable aléatoire exponentielle négative dont le taux ne dépend que de l'état S_n. Autrement dit

$$\Pr(T_n \leq \tau \,|\, S_0 = s_{i_0}, ..., S_n = s_i, T_0 \leq \tau_0, ..., T_{n-1} \leq \tau_{n-1}) =$$

$$\Pr(T_n \leq \tau \,|\, S_n = s_i) = 1 - e^{-\lambda_i \cdot \tau}$$

- L'état suivant un état courant ne dépend que de cet état et les probabilités de transition restent constantes [2] au cours du temps :

$$\Pr(S_{n+1} = s_j \,|\, S_0 = s_{i_0}, ..., S_n = s_i, T_0 \leq \tau_0, ..., T_n \leq \tau_n) =$$

$$\Pr(S_{n+1} = s_j \,|\, S_n = s_i) = p_{ij} =_{def} \mathbf{P}[i,j]$$

La chaîne discrète définie par la matrice $\mathbf{P}$ est appelée *chaîne incluse*. Elle observe les changements d'état de la CTMC sans tenir compte du temps écoulé. Un état de la CTMC est absorbant s'il est absorbant pour la DTMC incluse.

La chaîne est dite *irréductible* si la chaîne incluse est irréductible.

Comportement transitoire et stationnaire d'une CTMC

Dans les chaînes de Markov à temps continu, en raison de l'absence de mémoire de la loi exponentielle, l'évolution du DES à tout instant est uniquement conditionnée par son état courant.

Plus précisément, le processus se caractérise par sa distribution initiale $\boldsymbol{\pi}(0)$, la matrice $\mathbf{P}$ et les λ_i. Appelons $\boldsymbol{\pi}(\tau)$ la distribution de $X(\tau)$ et $\pi_k(\tau) = \boldsymbol{\pi}(t)(s_k)$. Si δ est petit, entre τ et $\tau + \delta$ la probabilité de l'occurrence de plus d'un événement est négligeable et la probabilité d'occurrence

2. ici aussi, on parle de chaîne *homogène*

d'un changement d'état de k à k' est approximativement égale à $\lambda_k \cdot \delta \cdot p_{kk'}$ (par définition de la loi exponentielle).

$$\pi_k(\tau + \delta) \approx \pi_k(\tau) \cdot (1 - (1 - p_{kk})\lambda_k \cdot \delta) + \sum_{k'} \pi_{k'}(\tau) \cdot \lambda_{k'} \cdot \delta \cdot p_{k'k}$$

D'où

$$\frac{\pi_k(\tau + \delta) - \pi_k(\tau)}{\delta} \approx \pi_k(\tau) \cdot (p_{kk} - 1)\lambda_k + \sum_{k'} \pi_{k'}(\tau) \cdot \lambda_{k'} \cdot p_{k'k}$$

Et finalement :

$$\frac{d\pi_k}{d\tau} = \pi_k(\tau) \cdot (p_{kk} - 1)\lambda_k + \sum_{k'} \pi_{k'}(\tau) \cdot \lambda_{k'} \cdot p_{k'k}$$

Définissons la matrice $\mathbf{Q}$ par : $q_{kk'} = \lambda_k \cdot p_{kk'}$ pour $k \neq k'$ et $q_{kk} = (p_{kk} - 1)\lambda_k (= -\sum_{k' \neq k} q_{kk'})$. Alors l'équation précédente se réécrit :

$$\frac{d\boldsymbol{\pi}}{d\tau} = \boldsymbol{\pi} \cdot \mathbf{Q} \tag{1.4}$$

La matrice $\mathbf{Q}$ est appelée le *générateur infinitésimal* de la CTMC. D'après l'équation (1.4), celui-ci spécifie complètement l'évolution de celle-ci.

Cas des chaînes finies. Si cette équation établit le caractère sans mémoire d'une CTMC, elle ne fournit pas un moyen pratique de calculer le comportement transitoire de la chaîne. Afin d'y parvenir, nous décrivons une deuxième CTMC équivalente à la première du point de vue probabiliste (une technique introduite dans [JEN 53] et connue sous le nom d'*uniformisation* voir la figure 1.7). Choisissons une valeur $\mu \geq sup(\{\lambda_i\})$. Quelque soit un état atteint, la durée qui précède le prochain changement d'état suit une loi exponentielle de paramètre (uniforme) μ. Le changement d'état est quant à lui conduit par la matrice de transition $\mathbf{P}^\mu$ définie par $\forall i \neq j, \mathbf{P}^\mu[s_i, s_j] = (\mu)^{-1} \cdot \lambda_i \cdot \mathbf{P}[s_i, s_j]$. Le calcul (immédiat) du générateur infinitésimal de cette deuxième chaine montre qu'il est égal à celui de la première chaîne. On a donc affaire au même processus stochastique *si on ne tient pas compte des transitions*. La distribution transitoire $\boldsymbol{\pi}(\tau)$ s'obtient de la façon suivante. On calcule la probabilité d'être en s à l'instant τ sachant qu'il y a eu n changements d'états dans l'intervalle $[0, \tau]$. Cette probabilité est donnée par la chaîne incluse et plus précisément par $\boldsymbol{\pi}(0) \cdot (\mathbf{P}^\mu)^n$. Puis on «déconditionne» en calculant la probabilité de n changements sachant que l'intervalle entre deux changements suit la loi exponentielle. Cette probabilité est donnée par $e^{-\mu \cdot \tau} \cdot (\mu \cdot \tau)^n / n!$. On obtient donc :

$$\boldsymbol{\pi}(\tau) = \boldsymbol{\pi}(0) \cdot \left(e^{-\mu \cdot \tau} \sum_{n \geq 0} \frac{(\mu \cdot \tau)^n (\mathbf{P}^\mu)^n}{n!} \right)$$

Dans la pratique, la somme infinie ne pose pas de problème car cette somme converge très rapidement et la sommation peut être stoppée dès que la précision requise est supérieure à $e^{-\mu \cdot \tau} \cdot (\mu \cdot \tau)^n / n!$.

Examinons maintenant le comportement asympotique d'une CTMC. La manière la plus simple d'analyser ce comportement consiste à étudier la chaîne incluse. Comme nous l'avons observé lors de l'approche par uniformisation, celle-ci n'est pas unique. Intéressons-nous à une DTMC obtenue avec un choix de $\mu > sup(\{\lambda_i\})$. Dans ce cas, tout état s vérifie $\mathbf{P}^\mu[s, s] > 0$ et par conséquent chaque c.f.c. puits de cette chaîne est ergodique. Ceci implique qu'elle admet une distribution stationnaire. Cette distribution mesure la probabilité stationnaire d'occurrence d'un état. Mais puisque la description (uniforme) de la chaîne implique un temps de séjour moyen identique dans chacun des états $(1/\mu)$, elle nous fournit aussi la distribution stationnaire de la CTMC.

Dans le cas particulier (mais fréquent) où la chaine incluse est ergodique, cette distribution est obtenue par résolution de l'équation $\mathbf{X} = \mathbf{X} \cdot \mathbf{P}^\mu$. Nous remarquons que $\mathbf{P}^\mu = \mathbf{I} + (1/\mu)\mathbf{Q}$. Donc la distribution est aussi l'unique solution de l'équation :

$$\mathbf{X} \cdot \mathbf{Q} = 0 \quad \text{et} \quad \mathbf{X} \cdot \mathbf{1}^T = 1 \tag{1.5}$$

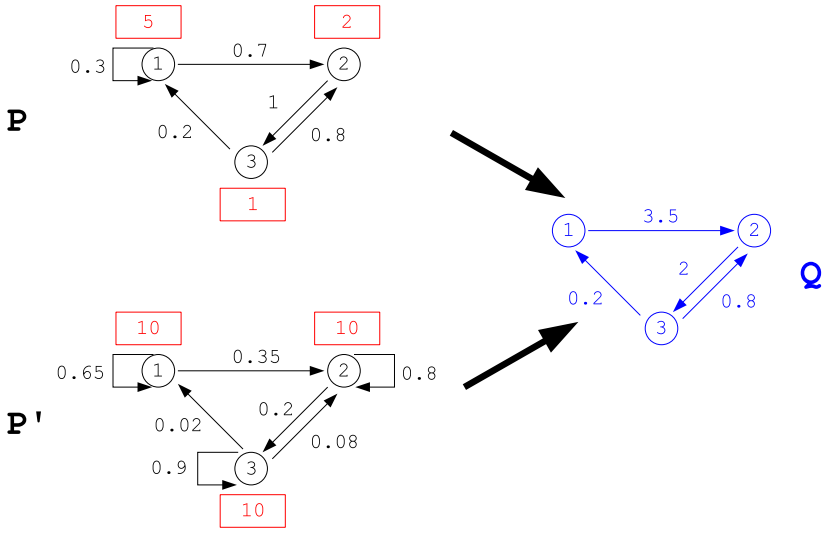

FIGURE 1.7 – Illustration de la technique d'uniformisation

Par analogie, on dit alors que la CTMC est ergodique. On trouvera dans les compléments théoriques le traitement des chaînes infinies irréductibles.

1.4 Compléments théoriques

Nous incluons ici les démonstrations mathématiques des affirmations que nous avons faites précédemment. Elles ne servent qu'au lecteur curieux d'en savoir un peu plus sur la nature des preuves.

1.4.1 Processus de renouvellement à temps discret

Soit une variable aléatoire Z de distribution f à valeurs dans $\mathbb{N}^*$. On note f_i la probabilité que $Z = i$. On construit un processus stochastique à temps discret $(T_n = 1)$ à valeurs dans $\{0, 1\}$ de la façon suivante. On pose $X_0 = 1$. On fait un tirage aléatoire de Z. Supposons que le résultat du tirage soit $Z = i$. Alors $X_i = 1$ et $\forall 0 < j < i$ $X_j = 0$. Puis on itère le processus : on fait un nouveau tirage aléatoire de Z. Supposons que le résultat du tirage soit $Z = i'$. Alors $X_{i+i'} = 1$ et $\forall 0 < j < i'$ $X_{i+j} = 0$ etc. En notant Z_k, la variable aléatoire associée au $k$ième tirage de Z, on a $\forall k \in \mathbb{N}^*$ $X_{\sum_{k'<k} Z'_k} = 1$ et $X_i = 0$ pour $i \notin \{\sum_{k'<k} Z'_k\}_{k\in\mathbb{N}^*}$. Les tirages de Z sont indépendants. On dira que les $\sum_{k'<k} Z'_k$ sont les *instants de renouvellement*.

On peut généraliser la notion de processus de renouvellement de deux façons différentes. Tout d'abord Z peut être à valeurs dans $\mathbb{N}^* \cup \{\infty\}$. Dans le cas où un tirage renvoie ∞, on fixe toutes les valeurs non encore déterminées de X_i à 0.

La deuxième généralisation consiste à retarder le processus stochastique par une variable aléatoire B de distribution b à valeurs dans $\mathbb{N}$. On note b_i la probabilité que $B = i$. On procède alors comme suit. On fait un tirage aléatoire de B. Supposons que le résultat du tirage soit $B = i$. Alors $X_i = 1$ et $\forall 0 \leq j < i$ $X_j = 0$. Puis on procède comme précédemment aux tirages successifs de la variable Z.

L'objet de notre étude est le comportement asymptotique de $u_n = \Pr(X_n = 1)$. On note

d'abord l'équation de renouvellement de base :

$$u_n = u_0 f_n + \ldots + u_{n-1} f_1 \tag{1.6}$$

Cette équation repose sur une décomposition en cas selon la valeur du premier tirage de f sachant que les tirages sont indépendants.

On peut écrire cette équation de manière plus synthétique en introduisant les séries entières ($s \leq 1$) $U(s) = \sum_{n\in\mathbb{N}} u_n s^n$ et $F(s) = \sum_{n\in\mathbb{N}} f_n s^n$. Pour $s < 1$, l'équation (1.6) se réécrit $U(s) - 1 = U(s)F(s)$ ou encore $U(s) = \frac{1}{1-F(s)}$.

Ceci nous permet d'obtenir notre premier résultat dont l'interprétation est claire.

Proposition 1 *Le nombre moyen d'instants de renouvellement* $\sum_{n\in\mathbb{N}} u_n$ *est fini ssi* $\sum_{n\in\mathbb{N}} f_n < 1$. *Dans ce cas,* $\sum_{n\in\mathbb{N}} u_n = \frac{1}{1-\sum_{n\in\mathbb{N}} f_n}$.

Preuve
Puisque les u_n et les f_n sont positifs $lim_{s\to 1^-} U(s) = U(1)$ (avec $U(1)$ fini ou infini) et $lim_{s\to 1^-} F(s) = F(1)$.

Supposons que $F(1)$ soit inférieur à 1, en passant à la limite l'égalité $U(s) = \frac{1}{1-F(s)}$ devient $U(1) = \frac{1}{1-F(1)}$ ce qui est le résultat annoncé.

Supposons maintenant que $U(1)$ soit fini, en passant à la limite l'égalité $U(s) - 1 = U(s)F(s)$, on obtient $U(1) - 1 = U(1)F(1)$. D'où $F(1) = \frac{U(1)-1}{U(1)} < 1$.

c.q.f.d. ◊◊◊

Par conséquent si $F(1) < 1$, $lim_{n\to\infty} u_n = 0$. Lorsque $F(1) < 1$, on dit que le processus est *transitoire* sinon il est dit *récurrent*. Dans la suite nous supposons que $F(1) = 1$. Une distribution f est dite apériodique si le pgcd des $\{n \mid f_n > 0\}$ est égal à 1. Nous discuterons des problèmes liés à la périodicité de f.

Soit $\mu = \sum_{i\in\mathbb{N}^+} i f_i$ la moyenne de f, les instants de renouvellement sont espacés en moyenne de μ. Lorsque μ est infini, on dit que le processus est *récurrent nul* sinon il est dit *récurrent non nul*. Intuitivement, on conjecture alors que $\lim_{n\to\infty} u_n = \mu^{-1}$. Cette conjecture est vraie mais techniquement difficile à prouver. C'est l'objet des prochains développements. Afin d'alléger les notations, nous définissons $\eta = \mu^{-1}$.

Le lemme suivant est une première indication de la véracité de la conjecture. Nous introduisons les quantités intermédiaires $\rho_k = \sum_{i>k} f_i$. Par un réordonnancement élémentaire des sommes, on obtient $\mu = \sum_{k\in\mathbb{N}} \rho_k$. D'autre part en sommant l'équation (1.6) pour n variant de 1 à N, on obtient l'équation :

$$\rho_0 u_N + \rho_1 u_{N-1} + \ldots + \rho_N u_0 = 1 \tag{1.7}$$

Cette formule s'obtient aussi directement par une décomposition selon le dernier instant de renouvellement dans l'intervalle $[0, N]$.

Lemme 2 *Supposons que* $\limsup_{n\to\infty} u_n = \eta$. *Alors* $\lim_{n\to\infty} u_n = \eta$.

Preuve
Si $\mu = \infty$ et donc $\eta = 0$, il n'y a rien à prouver.

Intéressons-nous au cas μ fini. Soit une sous-suite extraite $u_{n_1}, u_{n_2}, \ldots$, qui converge vers η' ($\leq \eta$ par hypothèse). Fixons $r \in \mathbb{N}^+$ et $\varepsilon > 0$.

Les hypothèses garantissent l'existence d'un m tel que $\forall n_i \geq m \ |u_{n_i} - \eta'| \leq \varepsilon \wedge \forall 1 \leq r' \leq r \ u_{n_i - r'} - \eta \leq \varepsilon$. D'après l'équation (1.7)

$$\rho_0 u_{n_i} + \rho_1 u_{n_i-1} + \ldots + \rho_{n_i} u_0 = 1$$

D'où

$$\rho_0(\eta' + \varepsilon) + (\eta + \varepsilon) \sum_{r'=1}^{r} \rho_{r'} + \sum_{r'>r} \rho_{r'} \geq 1$$

En faisant tendre ε vers 0 :

$$\rho_0\eta' + \eta\sum_{r'=1}^{r}\rho_{r'} + \sum_{r'>r}\rho_{r'} \geq 1$$

Puis r vers ∞ ($\rho_0 = 1$) :

$$\eta' + \eta(\mu - 1) \geq 1$$

C'est à dire :

$$\eta' - \eta \geq 0$$

Puisque $\eta' \leq \eta$, on en déduit que $\eta' = \eta$. Puisque la sous-suite extraite convergente était quelconque, $\lim_{n\to\infty} u_n = \eta$.

c.q.f.d. ◊◊◊

Nous rappelons maintenant un lemme d'arithmétique élémentaire.

Lemme 3 *Soient $a_1, \ldots, a_k$ des nombres dont le pgcd est 1. Alors il existe n_0 tel que $\forall n \geq n_0$ $\exists u_1, \ldots, u_k \in \mathbb{N}$ $n = a_1u_1 + \ldots a_ku_k$.*

Preuve
A l'aide de l'algorithme d'Euclide, on obtient des nombres $y_1, \ldots, y_k \in \mathbb{Z}$ tels que :

$$1 = a_1y_1 + \ldots + a_ky_k$$

Posons $s = a_1 + \ldots + a_k$ et $x = \sup_i |y_i|(s-1)$.
Soit $n \geq xs$. Effectuons la division euclidienne de n par s : $n = qs + r = \sum_{i=1}^{k}(q + ry_i)a_i$ et $q + ry_i$ est positif d'après nos hypothèses.

c.q.f.d. ◊◊◊

Le lemme suivant utilise l'apériodicité de f.

Lemme 4 *Soit f une distribution apériodique et $(w_n)_{n\in\mathbb{N}}$ telle que pour tout n, $0 \leq w_n \leq \nu$ et :*

$$w_n = \sum_{k=1}^{\infty} f_k w_{n+k} \tag{1.8}$$

Si $w_0 = \nu$ alors pour tout n, $w_n = \nu$.

Preuve
Notons $A = \{k \mid f_k > 0\}$.
$\nu = w_0 = \sum_{k=1}^{\infty} f_k w_k \leq \nu \sum_{k=1}^{\infty} f_k = \nu$
Pour qu'il y ait égalité il faut que $w_k = \nu$ pour tout $k \in A$. Soit $k \in A$,
$\nu = w_k = \sum_{k'=1}^{\infty} f_k w_{k+k'} \leq \nu \sum_{k=1}^{\infty} f_k = \nu$
Par conséquent, il faut que $w_{k+k'} = \nu$ pour tout $k, k' \in A$. En itérant, on a $w_k = \nu$ pour tout k, combinaison linéaire d'éléments de A.

f est apériodique. Donc d'après le lemme 3, il existe n_0 tel que pour tout $n \geq n_0$, $w_{n_0} = \nu$. Par conséquent :
$w_{n_0-1} = \sum_{k=1}^{\infty} f_k w_{n_0-1+k} = \nu \sum_{k=1}^{\infty} f_k = \nu$
En itérant le procédé, on conclut.

c.q.f.d. ◊◊◊

Le lemme suivant est une des nombreuses variations sur le thème de la méthode diagonale.

Lemme 5 *On associe à tout $n \in \mathbb{N}$, une suite $(x_{n,m})_{m\in\mathbb{N}}$ avec $0 \leq x_{n,m} \leq \nu$. Alors il existe une suite infinie $m_1 < m_2 < \ldots$ telle que pour tout $n \in \mathbb{N}$ la suite extraite $(x_{n,m_k})_{k\in\mathbb{N}}$ converge.*

Preuve
Puisque les $x_{n,m}$ sont bornés, on peut extraire une suite d'indices $(m_k^0)_{k\in\mathbb{N}}$ telle que $(x_{0,m_k^0})_{k\in\mathbb{N}}$ soit convergente.

Supposons que nous ayons une suite extraite d'indices $(m_k^n)_{k\in\mathbb{N}}$ après n étapes, alors on extrait de cette suite une nouvelle suite $(m_k^{n+1})_{k\in\mathbb{N}}$ telle que $(x_{n+1,m_k^{n+1}})_{k\in\mathbb{N}}$ soit convergente.

Considérons maintenant la suite d'indices $m_k = m_k^k$. Soit $n \in \mathbb{N}$ quelconque, à partir du $n$ième terme la suite $(x_{n,m_k})_{k\in\mathbb{N}}$ est une suite extraite de la suite $(x_{n,m_k^n})_{k\in\mathbb{N}}$ et donc elle converge.

c.q.f.d. ◊◊◊

Nous sommes maintenant en mesure d'établir notre conjecture

Théorème 6 *Soit f une distribution apériodique de moyenne (non nécessairement finie) μ. Alors* $\lim_{n\to\infty} u_n = \mu^{-1}$

Preuve
Posons $\nu = \limsup_{n\to\infty} u_n$ (compris entre 0 et 1).
Soit $(r_m)_{m\in\mathbb{N}}$, une suite extraite d'indices correspondant à cette limite. A chaque entier n, on associe la suite $(u_{n,m})_{m\in\mathbb{N}}$ définie par $u_{n,m} = u_{r_m-n}$ si $n \le r_m$ et $u_{n,m} = 0$ sinon.

D'après le lemme 5, il existe une suite $m_1, m_2, \ldots$ tel que pour tout n, $(u_{n,m_k})_{k\in\mathbb{N}}$ tend vers une limite que nous notons w_n (pour retrouver les notations du lemme 4). D'après la définition de ν, on a $0 \le w_n \le \nu$ et $w_0 = \nu$. L'équation (1.6) se lit :

$$u_{n,m_k} = \sum_{i=1}^{\infty} f_i u_{n+i,m_k}$$

On peut passer cette égalité à la limite car les u_n sont bornés et $\sum_{i=1}^{\infty} f_i = 1$ donc est fini. On obtient alors les hypothèses du lemme 4. Par conséquent, pour tout n, $w_n = \nu$.

D'après l'équation (1.7),

$$\rho_0 u_{m_k} + \rho_1 u_{m_k-1} + \ldots + \rho_{m_k} u_0 = 1$$

Examinons cette égalité lorsque m_k tend vers l'infini. Pour tout r fixé, $\rho_0 u_{m_k} + \rho_1 u_{m_k-1} + \ldots + \rho_r u_{m_k-r}$ tend vers $\nu \sum_{r'=0}^{r} \rho_{r'}$. Par conséquent si $\mu = \infty$ alors $\nu = 0$ et le résultat est établi.
Dans le cas contraire la limite du terme gauche est supérieure ou égale $\nu \sum_{r'=0}^{r} \rho_{r'}$ pour tout r' donc supérieure ou égale à $\nu\mu$. De même $\rho_0 u_{m_k} + \rho_1 u_{m_k-1} + \ldots + \rho_{m_k} u_0 \le \rho_0 u_{m_k} + \rho_1 u_{m_k-1} + \ldots + \rho_r u_{m_k-r} + \sum_{r'=r+1}^{\infty} \rho_{r'}$ Par conséquent la limite du terme gauche est inférieure ou égale à $\nu \sum_{r'=0}^{r} \rho_{r'} + \sum_{r'=r+1}^{\infty} \rho_{r'}$. Ceci étant vrai pour tout r, on conclut que la limite du terme gauche est égale à $\nu\mu$. Par conséquent $\nu = \mu^{-1}$ et le lemme 2 permet de conclure.

c.q.f.d. ◊◊◊

Lorsque la distribution est périodique de période p, en examinant les instants np, on réduit le cas périodique au cas apériodique.

Théorème 7 *Soit f une distribution périodique de période p et de moyenne (non nécessairement finie) μ. Alors* $\lim_{n\to\infty} u_{np} = p\mu^{-1}$ *et* $\forall n \ n \mod p \neq 0 \Rightarrow u_n = 0$.

Examinons le processus retardé dont la distribution du retard est b avec b_i la probabilité d'un retard de durée i. Nous notons v_i la probabilité que i soit un instant de renouvellement du processus retardé. u_i et f_i ont la même signification que précédemment. On obtient immédiatement :

$$v_n = b_n + b_{n-1}u_1 + \ldots + b_0 u_n$$

En introduisant les séries génératrices $B(s) = \sum_{i\in\mathbb{N}} b_i s^i$ et $V(s) = \sum_{i\in\mathbb{N}} v_i s^i$ ceci se traduit par :

$$V(s) = B(s)U(s) = \frac{B(s)}{1 - F(s)}$$

On peut aussi généraliser le retard en supposant qu'il est possible qu'il n'y ait pas de premier instant de renouvellement (i.e. $B(1) < 1$). Le théorème suivant caractérise le comportement asymptotique de v_n.

Théorème 8
- *Si* $\lim_{n\to\infty} u_n = \omega$ *alors* $\lim_{n\to\infty} v_n = B(1)\omega$
- *Si* $\sum_{n\to\infty} u_n = U(1)$ *est fini alors* $\sum_{n\to\infty} v_n = B(1)U(1)$

Preuve
Notons $r_k = \sum_{k'>k} b_{k'}$. D'après la définition de v_n pour $n > k$ on a :

$$\sum_{k'=0}^{k} b_{k'} u_{n-k'} \leq v_n \leq \sum_{k'=0}^{k} b_{k'} u_{n-k'} + r_k$$

Soit $\varepsilon > 0$. Alors il existe k tel qu'on ait $r_k \leq \varepsilon$ et il existe n_0 tel que pour $n \geq n_0$ on ait $|\omega - u_n| \leq \varepsilon$. Par conséquent pour tout $n > n_0 + k$

$$\omega B(1)+2\varepsilon \leq (\omega-\varepsilon)(B(1)-\varepsilon) \leq \sum_{k'=0}^{k} b_{k'} u_{n-k'} \leq v_n \leq \sum_{k'=0}^{k} b_{k'} u_{n-k'}+r_k \leq (\omega+\varepsilon)B(1)+\varepsilon \leq \omega B(1)+2\varepsilon$$

ce qui démontre la première affirmation.
La deuxième affirmation est triviale puisque $V(s) = B(s)U(s)$.

c.q.f.d. ◊◊◊

Ce théorème s'applique immédiatement dans le cas d'un processus de renouvellement apériodique. Nous laissons le soin au lecteur d'énoncer et de prouver un théorème analogue pour un processus de renouvellement retardé périodique.

1.4.2 DTMC

Nous rappelons quelques notations et nous en introduisons de nouvelles.
- $p_{i,j}$ désigne la probabilité d'atteindre en un pas l'état j depuis l'état i.
- Pour $n \in \mathbb{N}$, $p^n_{i,j}$ désigne la probabilité d'atteindre en n pas l'état j depuis l'état i. Ces quantités sont les coefficients de la matrice $\mathbf{P}^n$ qui est aussi une matrice stochastique.
- Pour $n \in \mathbb{N}$, $f^n_{i,j}$ désigne la probabilité d'atteindre en n pas l'état j depuis l'état i *pour la première fois*. On note $f_{i,j} = \sum_{n\in\mathbb{N}} f^n_{i,j}$ la probabilité d'atteindre j depuis i. On note $\mu_i = \sum_{n\in\mathbb{N}} n f^n_{i,i}$ le temps moyen d'un retour en i (significatif seulement si $f_{i,i} = 1$).

Une première équation lie ces différentes quantités :

$$p^n_{i,j} = \sum_{m=0}^{n} f^m_{i,j} p^{n-m}_{j,j}$$

Cette équation est obtenue par décomposition en cas selon le temps de première atteinte de i depuis j.

A chaque état i, on peut associer un processus de renouvellement où les instants de renouvellement correspondent à l'atteinte de i. On remarque alors que $\{f^n_{i,i}\}_{n\in\mathbb{N}}$ est la distribution du temps de renouvellement et que $\{p^n_{i,i}\}_{n\in\mathbb{N}}$ est la distribution du processus de renouvellement.

A chaque paire d'états (i, j), on peut associer un processus de renouvellement retardé où les instants de renouvellement correspondent à l'atteinte de i et la distribution du retard est donnée par $\{f^n_{j,i}\}_{n\in\mathbb{N}}$. $\{p^n_{i,i}\}_{n\in\mathbb{N}}$ est alors la distribution du processus de renouvellement retardé.

En accord avec le début du chapitre un état est *transitoire, récurrent nul, récurrent non nul, périodique* si le processus de renouvellement associé a ces caractéristiques. On dit aussi qu'un état est *ergodique* s'il est récurrent non nul et apériodique.

Par application immédiate des résultats sur les processus de renouvellement, on a :

– Un état i est transitoire ssi $\sum_{n\in\mathbb{N}} p^n_{i,i} < \infty$.
– Un état i est récurrent nul ssi $\sum_{n\in\mathbb{N}} p^n_{i,i} = \infty$ et $\lim_{n\to\infty} p^n_{i,i} = 0$. Dans ce cas pour tout j, on a $\lim_{n\to\infty} p^n_{j,i} = 0$.
– Un état apériodique i est récurrent non nul ssi $\sum_{n\in\mathbb{N}} p^n_{i,i} = \infty$ et $\mu_i < \infty$. Dans ce cas pour tout j, on a $\lim_{n\to\infty} p^n_{j,i} = f_{j,i}\mu_i^{-1}$.

Un sous-ensemble d'états S' est *clos* si pour tout $i \in S'$, on a $\sum_{j\in S'} p_{i,j} = 1$. A tout état i, on peut associer sa cloture $Cl(i) = \{j \mid f_{i,j} > 0\}$. Un sous-ensemble clos peut être étudié en isolation car il constitue une DTMC. Une chaîne est *irréductible* si pour tout paire d'états i, j on a $f_{i,j} > 0$ (ou de manière équivalente $\sum_{n\in\mathbb{N}} p^n_{i,j} > 0$). L'importance de l'irréductibilité est démontrée par le théorème suivant.

Théorème 9 *Tous les états d'un chaîne irréductible sont du même type.*

Preuve
Soient i, j deux états de la chaîne, il existe r et s tels que $p^r_{i,j} > 0$ et $p^s_{j,i} > 0$. D'autre part,

$$p^{n+r+s}_{i,i} \geq p^r_{i,j} p^n_{j,j} p^s_{j,i} \tag{1.9}$$

Par conséquent si $\sum_{n\in\mathbb{N}} p^n_{i,i}$ est fini alors $\sum_{n\in\mathbb{N}} p^n_{j,j}$ est fini. Si $\lim_{n\to\infty} p^n_{i,i} = 0$ alors $\lim_{n\to\infty} p^n_{j,j} = 0$. Les rôles de i et j étant interchangeables, on en déduit que i est transitoire (resp. récurrent nul, récurrent non nul) ssi j est transitoire (resp. récurrent nul, récurrent non nul).

Intéressons-nous maintenant à la périodicité. Supposons i périodique de période t. D'après l'équation (1.9), en posant n=0, on déduit que $r + s$ est un multiple de t. Par conséquent, si n n'est pas un multiple de t, alors $p^n_{j,j} = 0$ ce qui signifie que la période de j est supérieure ou égale à celle de i. Les rôles de i et j étant interchangeables, on en déduit qu'ils ont même période.

c.q.f.d. ◊◊◊

Théorème 10 *Soit i un état récurrent alors $Cl(i)$ est irréductible et pour toute paire d'états $(j, k) \in Cl(i)$, on a $f_{j,k} = 1$.*

Preuve
Soit $j \in Cl(i)$. Par définition, $f_{i,j} > 0$. D'autre part $1 - f_{i,i} \geq f_{i,j}(1 - f_{j,i})$. Puisque i est récurrent on a $f_{i,i} = 1$ ce qui implique $f_{j,i} = 1$.

Soit maintenant $k \in Cl(i)$, $f_{j,k} \geq f_{j,i} f_{i,k} > 0$. Par conséquent la chaîne est irréductible. Puisque cette chaîne est irréductible, tous les états sont récurrents et on peut reprendre le début de la preuve avec k. Ce qui démontre $f_{j,k} = 1$.

c.q.f.d. ◊◊◊

En résumant, une chaîne peut être partitionnée entre les états transitoires disons T et les chaînes irréductibles $C_1, C_2, \ldots$. Remarquons qu'une chaîne infinie peut être composée uniquement d'états transitoires comme dans la chaîne où les états sont les entiers et $p_{i,i+1} = 1$. Dans les chaînes finies, il en va autrement.

Théorème 11 *Dans une chaîne finie, les états transitoires correspondent aux c.f.c. non terminales et les chaînes irréductibles aux c.f.c. terminales. De plus les états des c.f.c. terminales sont récurrents non nuls.*

Preuve
Soit i appartenant à un c.f.c. non terminale alors $Cl(i)$ contient au moins une c.f.c. terminale. Par conséquent, $Cl(i)$ n'est pas irréductible et i est transitoire.

Soit maintenant la chaîne correspondant à une c.f.c. terminale (un ensemble clos). Soit $\mathbf{P}$ sa matrice de transition. Fixons un état i et remarquons que $\sum_j p^n_{i,j} = 1$. Par conséquent, il existe au moins un j tel que $p^n_{i,j}$ ne tende pas vers 0 quand n tend vers l'infini. Ceci signifie que j est récurrent non nul et puisque tous les états d'une chaîne irréductible sont du même type, tous les états de la c.f.c. sont récurrent non nuls.

c.q.f.d. $\Diamond\Diamond\Diamond$

Nous établissons maintenant le théorème fondamental des chaînes de Markov énoncé dans la première partie du chapitre. Un état est dit *ergodique* ssi il est récurrent non nul et apériodique.

Théorème 12 *Dans une chaîne irréductible où les états sont ergodiques :*
Les limites $u_i = \lim_{n\to\infty} p^n_{j,i}$ *existent et sont indépendantes de* j.
De plus elles vérifient $u_i > 0$, $\sum_{i\in S} u_i = 1$ *et* $\forall i\ u_i = \sum_{j\in S} u_j p_{j,i}$.
Réciproquement, soit une chaîne irréductible et apériodique.
Supposons donnés des u_i *tels que* $u_i \geq 0$, $\sum_{i\in S} u_i = 1$ *et* $\forall i\ u_i = \sum_{j\in S} u_j p_{j,i}$.
Alors $u_i = \mu_i^{-1}$.

Preuve
D'après la théorie du renouvellement sur les processus retardés $\lim_{n\to\infty} p^n_{j,i} = f_{j,i}\mu_i^{-1} = \mu_i^{-1}$ puisque la chaîne est iréductible.
Notons $S = \{i_0, i_1, \ldots\}$ (le cas S fini se traite de manière similaire mais plus simplement). On

$$p^{n+1}_{k,i} = \sum_{j\in S} p^n_{k,j} p_{j,i} \geq \sum_{m\leq M} p^n_{k,i_m} p_{i_m,i}$$

Par conséquent, en passant à la limite :

$$u_i \geq \sum_{m\leq M} u_{i_m} p_{i_m,i}$$

et en faisant tendre M vers l'infini :

$$u_i \geq \sum_{j\in S} u_j p_{j,i}$$

D'autre part,

$$1 = \sum_{i\in S} p^{n+1}_{k,i} = \sum_{i\in S}\sum_{j\in S} p^n_{k,j} p_{j,i} = \sum_{j\in S} p^n_{k,j} \sum_{i\in S} p_{j,i} = \sum_{j\in S} p^n_{k,j}$$

Avec le même raisonnement que précédemment en passant à la limite on obtient :

$$1 \geq \sum_{j\in S} u_j$$

Par conséquent en sommant $u_i \geq \sum_{j\in S} u_j p_{j,i}$ sur i, on obtient :

$$\sum_{i\in S} u_i \geq \sum_{i\in S}\sum_{j\in S} u_j p_{j,i} = \sum_{j\in S} u_j \sum_{i\in S} p_{j,i} = \sum_{j\in S} u_j$$

On a donc l'égalité des sommes, donc aussi l'égalité des termes, i.e. :

$$u_i = \sum_{j\in S} u_j p_{j,i}$$

En itérant :

$$u_i = \sum_{j\in S} u_j p^n_{j,i}$$

et par passage à la limite justifié en notant que $\sum_{j\in S} u_j$ est fini et que les $p^n_{j,i}$ sont bornés par 1 :

$$u_i = \sum_{j\in S} u_j u_i$$

Puisque u_i est strictement positif, on conclut que :

$$\sum_{i \in S} u_i = 1$$

Réciproquement, supposons donnés des u_i tels que $u_i \geq 0$, $\sum_{i \in S} u_i = 1$ et $\forall i \ u_i = \sum_{j \in S} u_j p_{j,i}$. Choisissons $u_i > 0$, on itère la dernière équation ce qui nous donne :

$$u_i = \sum_{j \in S} u_j p^n_{j,i}$$

Si tous les $p^n_{j,i}$ tendent vers 0 alors (puisque $\sum_{i \in S} u_i = 1$ et les $p^n_{j,i}$ sont bornés) on peut passer à la limite l'égalité et on obtient $u_i = 0$ ce qui est contradictoire.

Donc i est récurrent non nul (et ergodique d'après les hypothèses). Par conséquent tous les états sont ergodiques et les $p^n_{j,i}$ tendent vers μ_i^{-1}. L'équation limite s'écrit donc :

$$u_i = \sum_{j \in S} u_j \mu_i^{-1} = \mu_i^{-1}$$

c.q.f.d. ◊◊◊

Nous voudrions aussi obtenir une caractérisation (plus ou moins effective) de récurrence pour un état. Nous énonçons cette caractérisation après un bref développement. Soit S' un sous-ensemble d'états, $\mathbf{P}$ réduit aux états de S', notée $\mathbf{P}'$, représente le comportement de la chaîne tant qu'elle reste dans les états de S'. Ainsi $\mathbf{P}'^n[i,j]$ est la probabilité qu'à l'instant n, la chaîne soit dans l'état j sans jamais quitter S', sachant qu'elle a démarré dans l'état i. On observe que $\sum_{j \in S'} \mathbf{P}'^n[i,j]$ est la probabilité qu'à l'instant n, la chaîne soit n'ait pas quitté S', sachant qu'elle a démarré dans l'état i. On note cette quantité $pin^n_{S'}[i]$.

Proposition 13 *Pour tout i, $\lim_{n \to \infty} pin^n_{S'}[i]$ existe. Si on note $pin_{S'}[i]$ cette limite, alors $pin_{S'}$ est la solution maximale de l'équation :*

$$\forall i \ x[i] = \sum_{j \in S'} \mathbf{P}[i,j] x[j] \wedge 0 \leq x[i] \leq 1 \tag{1.10}$$

Preuve
Par définition la suite $pin^n_{S'}[i]$ est décroissante et elle est minorée par 0 donc elle est convergente.
$\sum_{j \in S'} \mathbf{P}'^{n+1}[i,j] = \sum_{j,j' \in S'} \mathbf{P}[i,j'] \mathbf{P}'^n[j',j]$
D'où :
$pin^{n+1}_{S'}[i] = \sum_{j' \in S'} \mathbf{P}[i,j'] pin^{n+1}_{S'}[j']$
Cette égalité passe à la limite car $\sum_{j' \in S'} \mathbf{P}[i,j'] \leq 1$ et les $pin^n_{S'}[i]$ sont compris entre 0 et 1.
D'où en remplaçant j' par j :
$pin_{S'}[i] = \sum_{j \in S'} \mathbf{P}[i,j] pin_{S'}[j]$
Autrement dit les $pin_{S'}[i]$ forment une solution de l'équation (1.10).

Soit maintenant x une solution de cette équation. On a $\forall i \ x[i] \leq pin^0_{S'}[i] = 1$. Puis en supposant cette inéquation valide pour n.
$x[i] = \sum_{j \in S'} \mathbf{P}[i,j] x[j] \leq \sum_{j \in S'} \mathbf{P}[i,j] pin^n_{S'}[i] = pin^{n+1}_{S'}[i]$
Par passage à la limite, la maximalité est obtenue.

c.q.f.d. ◊◊◊

Nous avons donc une caractérisation de la récurrence dans le cas infini (le cas fini est traité par le théorème 11).

Théorème 14 *Soit une chaîne de Markov irréductible dont l'espace d'états est* $\mathbb{N}$. *Alors* 0 *est récurrent ssi la solution maximale de l'équation :*

$$\forall i > 0 \; x[i] = \sum_{j>0} \mathbf{P}[i,j]x[j] \wedge 0 \leq x[i] \leq 1$$

est le vecteur nul. Autrement dit, le vecteur nul en est l'unique solution.

Preuve
Si x désigne la solution maximale alors $x[i]$ représente la probabilité de ne pas revenir en 0 en démarrant en i.

Si l'état 0 est persistent la probabilité de retour est 1. Or pour tout état i, il existe une probabilité non nulle d'atteindre depuis 0 l'état i, donc $x[i]$ doit être nulle.

Si la solution maximale est nulle alors la probabilité de rester dans les états $\mathbb{N}^*$ est nulle quelque soit l'état de départ. Par conséquent la probabilité de retourner en 0 est égale à 1.

c.q.f.d. ◊◊◊

Enfin nous généralisons le résultat du théorème 12 aux chaînes irréductibles dont les états sont récurrents. Pour cela nous introduisons la probabilité suivante : ${}_rp_{ij}^{(n)}$ représente la probabilité que partant de i on atteigne j après n transitions sans jamais rencontrer r. Nous autorisons i à être égal à r et pour le cas $n = 0$, nous posons ${}_rp_{ij}^{(0)} \equiv 1_{i=j}$.

On observe que ${}_r\pi_{ij} \equiv \sum_{n\in\mathbb{N}} {}_rp_{ij}^{(n)}$ représente le nombre moyen de visites en j sans rencontrer r. Puisque les états sont récurrents, la probabilité de rencontrer r est égale à 1. Soit maintenant la chaîne obtenue en rendant r absorbant ($p_{rr} = 1$), tous les états différents de r sont transitoires et d'après les critères énoncés au début du paragraphe le nombre moyen de visites à ces états est fini, i.e. ${}_r\pi_{ij} < \infty$.

Théorème 15 *Soit une chaîne irréductible dont les états sont récurrents et* r *un état quelconque. Alors le vecteur* $\mathbf{u}$ *défini par* $\mathbf{u}_i \equiv {}_r\pi_{ri}$ *vérifie :*

$$\mathbf{u} = \mathbf{u} \cdot \mathbf{P} \quad et \quad \forall i \; \mathbf{u}_i > 0 \quad et \quad \mathbf{u}_r = 1$$

Inversement, soit $\mathbf{u}$ *tel que* $\mathbf{u} = \mathbf{u} \cdot \mathbf{P}$ *et* $\forall i \; \mathbf{u}_i \geq 0$, *alors il existe* λ *tel que* $\mathbf{u}_i = \lambda \cdot {}_r\pi_{ri}$

Preuve
Soit $\mathbf{u}$ défini par $\mathbf{u}_i \equiv {}_r\pi_{ri}$. On a ${}_rp_{rr}^{(0)} = 1$ et ${}_rp_{rr}^{(n)} = 0$ pour $n > 0$, d'où $\mathbf{u}_r = 1$. Puisque la chaîne est irréductible, il existe une probabilité non nulle d'atteindre un état i quelconque depuis r, d'où $\mathbf{u}_i > 0$.
A partir de la définition de ${}_rp_{ij}^{(n)}$, on obtient pour $i \neq r$, ${}_rp_{ri}^{(n+1)} = \sum_{j\in\mathbb{N}} {}_rp_{rj}^{(n)} p_{ji}$.
En sommant sur n, on obtient :
$\sum_{n\geq 1} {}_rp_{ri}^{(n)} = \sum_{n\geq 0} \sum_{j\in\mathbb{N}} {}_rp_{rj}^{(n)} p_{ji}$
Puisque ${}_rp_{ri}^{(0)} = 0$, on en déduit $\pi_{ri} = \sum_{j\in\mathbb{N}} \pi_{rj} p_{ji}$.

Dans le cas $i = r$, on observe que $\sum_{j\in\mathbb{N}} {}_rp_{rj}^{(n)} p_{jr}$ est la probabilité d'un premier retour en r à la $n+1$ème transition. En sommant, on en déduit que $\sum_{j\in\mathbb{N}} \pi_{rj} p_{jr}$ est la probabilité d'un retour en r. Puisque r est récurrent cette quantité est égale à 1.

Supposons maintenant qu'il existe $\mathbf{u}$ tel que $\mathbf{u} = \mathbf{u} \cdot \mathbf{P}$ et $\forall i \; \mathbf{u}_i \geq 0$. D'après la première équation si $\mathbf{u}_i = 0$ pour i arbitraire alors $\mathbf{u}_j = 0$ pour tout j tel que $p_{ji} > 0$. Par induction, on déduit que $\mathbf{u}_j = 0$ pour tout j qui permet d'atteindre k. Or la chaîne est irréductible. Donc un tel vecteur $\mathbf{u}$ est soit nul, soit strictement positif sur toutes ses composantes.

Dans le cas où $\mathbf{u}$ est strictement positif, on peut supposer (en appliquant un facteur multiplicatif) que $\mathbf{u}_r = 1$. Par conséquent pour $i \neq r$,
$\mathbf{u}_i = p_{ri} + \sum_{j\neq r} \mathbf{u}_j p_{ji} = p_{ri} + \sum_{j\neq r} \left(p_{rj} + \sum_{k\neq r} \mathbf{u}_k p_{kj} \right) p_{ji} = p_{ri} + {}_rp_{ri}^{(2)} + \sum_{k\neq r} \mathbf{u}_k \cdot {}_rp_{ki}^{(2)}$

En procédant par induction on obtient :
$\mathbf{u}_i = p_{ri} + {}_rp_{ri}^{(2)} + \ldots + {}_rp_{ri}^{(n)} + \sum_{j \neq r} \mathbf{u}_j \cdot {}_rp_{ji}^{(n)}$
Par passage à la limite, on en déduit que $u_i \geq {}_r\pi_{ri}$. D'où $\mathbf{u}_i - {}_r\pi_{ri}$ est aussi une solution positive du système d'équations. Comme elle est nulle sur la composante r, elle est nulle sur toutes les composantes.

c.q.f.d. ◊◊◊

1.4.3 Processus de renouvellement à temps continu

On rappelle que le support d'une fonction est l'ensemble des points où elle est non nulle.

Limites de fonctions et de mesures

Dans ce paragraphe, on énonce quelques résultats (pour la plupart élémentaires) sur les limites de fonctions et de mesures qui serviront lors de l'étude du comportement asymptotique du processus de renouvellement.

Lemme 16 *Soient $(x_n)_{n\in\mathbb{N}}$ une suite de réels bornée tel qu'il existe l, limite de toute suite extraite convergente. Alors la suite $(x_n)_{n\in\mathbb{N}}$ converge vers l.*

Preuve
Supposons qu'il existe $\varepsilon > 0$ tel que $\forall n\ \exists n' > n\ |x_{n'} - l| \geq \varepsilon$. En itérant sur cette propriété on extrait une suite $(x_{n_r})_{r\in\mathbb{N}}$ éloignée d'au moins ε de l. Puisque la suite initiale est bornée on extrait de la suite $(x_{n_r})_{r\in\mathbb{N}}$ une suite convergente qui converge donc vers l, ce qui est contradictoire.

c.q.f.d. ◊◊◊

Lemme 17 *Soient $(x_n)_{n\in\mathbb{N}}$ une suite de points réels et f_m une suite de fonctions de $\mathbb{R}$ dans $\mathbb{R}$. Alors il existe une suite extraite de $m_1 < m_2 < \ldots$ telle que pour tout $n \in \mathbb{N}$ la suite extraite $\{f_{m_k}(x_n)\}_{k\in\mathbb{N}}$ converge dans $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$ (dans $\mathbb{R}$ si pour tout x_n, $\sup_m |f_m(x_n)| < \infty$).*

Preuve
Il s'agit simplement d'une réécriture du lemme 5.

c.q.f.d. ◊◊◊

La notion d'équicontinuité est analogue à celle de continuité uniforme mais elle s'applique à une famille de fonctions.

Définition 18 *Soit $\{f_n\}_{n\in\mathbb{N}}$ une suite de fonctions réelles, on dit que cette suite est* équicontinue *si :*

$$\forall \varepsilon > 0\ \exists \delta > 0\ \forall n\ \forall x, x'\ |x - x'| \leq \delta \Rightarrow |f(x) - f(x')| \leq \varepsilon$$

Proposition 19 *Soit $\{f_n\}_{n\in\mathbb{N}}$ une suite de fonctions équicontinue telle qu'il existe B avec pour tout x et tout n, $|f_n(x)| \leq B$. Alors il existe une sous-suite extraite qui converge, uniformément sur tout intervalle fini, vers une fonction uniformément continue f.*

Preuve
On choisit un ensemble dénombrable dense de points $\{a_i\}_{i\in\mathbb{N}}$. D'après le lemme 17, il existe une sous-suite extraite $\{f_{n_r}\}_{r\in\mathbb{N}}$ qui converge sur tous les points a_i.

Choisissons un intervalle fini I. Soit maintenant $\varepsilon > 0$ et δ correspondant à la définition de l'équicontinuité. D'après l'hypothèse de densité, il existe un sous-ensemble fini d'indices S tels que pour tout $x \in I$, il existe a_i avec $i \in S$ et $|x - a_i| \leq \delta$. D'autre part, il existe r_0 tel que pour tout $r, r' \geq r_0$ et tout $i \in S$, on ait $|f_{n_r}(a_i) - f_{n_{r'}}(a_i)| \leq \varepsilon$, par conséquent pour tout $x \in I$, $|f_{n_r}(x) - f_{n_{r'}}(x)| \leq 3\varepsilon$. Ceci démontre que $f_{n_r}(x)$ est une suite de Cauchy et donc admet une limite $f(x)$; la démonstration précédente assure aussi que la convergence est uniforme sur l'intervalle I.

La continuité uniforme s'obtient en passant à la limite l'implication
$|x - x'| \leq \delta \Rightarrow |f_{n_r}(x) - f_{n_r}(x')| \leq \varepsilon$.

c.q.f.d. $\Diamond\Diamond\Diamond$

On rappelle qu'une mesure (réelle) μ associe à chaque ensemble mesurable E de $\mathbb{R}$ (et en particulier à chaque intervalle) une valeur positive finie ou infinie $\mu\{E\}$ telle que (1) $\mu\{\emptyset\} = 0$ et (2) pour toute famille dénombrable d'ensembles disjoints E_i, on ait $\mu\{\biguplus_{i\in\mathbb{N}} E_i\} = \sum_{i\in\mathbb{N}} \mu\{E_i\}$. On s'intéresse uniquement aux mesures localement finies, i.e. telles que pour tout I, intervalle fini, on ait $\mu\{I\} < \infty$.

Un *point de continuité* a de μ vérifie $\lim_{a'\to a\ a'<a} \mu\{[b, a']\} = \mu\{[b, a]\}$ avec $b < a$ (cette définition est indépendante de b). L'ensemble des points de discontinuité, appelés aussi *atomes* est dénombrable et a, point de discontinuité, vérifie $\mu\{a\} > 0$. Un *intervalle de continuité* est un intervalle dont les bornes sont des points de continuité (par convention $-\infty, +\infty$ sont considérés commes des points de continuité).

Définition 20 *Une suite de mesures* $\{\mu_n\}_{n\in\mathbb{N}}$ converge *vers une mesure* μ *ssi pour tout* I*, intervalle fini de continuité de* μ*, on a :*

$$lim_{n\to\infty}\mu_n(I) = \mu(I)$$

Proposition 21 *Soit une suite de mesures* $\{\mu_n\}_{n\in\mathbb{N}}$ *vérifiant* $\sup_n(\mu_n\{I\}) < \infty$ *pour tout intervalle fini* I*. Alors :*

- $\{\mu_n\}_{n\in\mathbb{N}}$ *possède une sous-suite extraite qui converge vers une mesure.*
- *Soit* μ *une mesure. Si toute suite extraite convergente de* $\{\mu_n\}_{n\in\mathbb{N}}$ *converge vers* μ *alors* $\{\mu_n\}_{n\in\mathbb{N}}$ *converge vers* μ*.*

Preuve
On choisit un point r qui n'est un atome d'aucune mesure μ_n et un sous-ensemble dénombrable $\{a_i\}_{i\in n}$ dense de $\mathbb{R}\backslash\{r\}$ et on considère les fonctions $f_n(x) = \mu_n([r, x])$ si $x > r$ et $f_n(x) = \mu_n([x, r])$ si $x < r$. On applique le lemme 17 à cette suite de fonctions et de points. Soit f_{n_s} la suite extraite, on définit $g(a_i) \equiv \lim_{s\to\infty} f_{n_s}(a_i)$ puis $g(x)$ par :

$$g(x) \equiv \inf(g(a_i) \mid a_i \geq x) \text{ pour } x > r \text{ et } g(x) \equiv \inf(g(a_i) \mid a_i \leq x) \text{ pour } x < r$$

La fonction g est définie sur $\mathbb{R} \setminus \{r\}$, décroissante sur $]-\infty, r[$ et croissante sur $]r, -\infty[$. Elle a donc des limites à droite $g(x^-)$ et à gauche $g(x^+)$ en tout x. On introduit alors la fonction h qui coïncide avec g sur ses points de continuité et telle que pour tout point de discontinuité $x < r$, $h(x) \equiv g(x^-)$ et tout point de discontinuité $x > r$, $h(x) \equiv g(x^+)$. Il est maintenant possible de définir une mesure μ par $\mu\{[a, r[\} \equiv h(a) - g(r^-)$, $\mu\{]r, b]\} \equiv h(b) - g(r^+)$ et $\mu\{r\} = g(r^+) + g(r^-)$ (preuve laissée au lecteur).

Démontrons que μ_{n_s} tend μ. Nous le faisons dans le cas d'un intervalle de continuité $[a, b]$ avec $-\infty < a < r < b < \infty$ et laissons les autres cas au lecteur. Soit $\varepsilon > 0$, il existe :
$a_{i_1} \leq a \leq a_{i_2} < r < a_{i_3} \leq b \leq a_{i_4}$ tel que
$g(a_{i_1}) \geq h(a) \geq g(a_{i_2}) \geq g(a_{i_1}) - \varepsilon$ et $g(a_{i_3}) \leq h(b) \leq g(a_{i_4}) \leq g(a_{i_3}) + \varepsilon$.
D'autre part il existe s_0 tel que pour tout $s \geq s_0$, et tout $1 \leq j \leq 4$ on ait $|g(a_{i_j}) - f_{n_s}(a_{i_j})| \leq \varepsilon$. Par conséquent, $\mu\{[a, b]\} \leq \mu\{[a_{i_2}, a_{i_3}]\} + 2\varepsilon \leq \mu_{n_s}\{[a_{i_2}, a_{i_3}]\} + 4\varepsilon \leq \mu_{n_s}\{[a, b]\} + 4\varepsilon$. On démontre de manière similaire que $\mu\{[a, b]\} \geq \mu_{n_s}\{[a, b]\} - 4\varepsilon$.

Supposons maintenant que toute suite extraite convergente de $\{\mu_n\}_{n\in\mathbb{N}}$ converge vers μ mais que $\{\mu_n\}_{n\in\mathbb{N}}$ ne converge pas vers μ. Il existe $\varepsilon > 0$ et I un intervalle de continuité de μ tel que $\forall n\ \exists n' > n\ |\mu_{n'}\{I\} - \{I\}| \geq \varepsilon$. En itérant sur cette propriété on extrait une suite $(\mu_{n_s})_{s\in\mathbb{N}}$ éloignée d'au moins ε de $\mu\{I\}$. Puisque la suite extraite vérifie les hypothèses de la proposition, on extrait de la suite $(\mu_{n_s})_{s\in\mathbb{N}}$ une suite convergente qui converge donc vers μ, ce qui est contradictoire.

c.q.f.d. $\Diamond\Diamond\Diamond$

On peut s'interroger sur cette notation de convergence « faible ». Comme le démontre la proposition 23, elle est adéquate pour établir des limites d'intégrale.

Notations. $\mathcal{C}_f$ désigne l'ensemble des fonctions continues u dont le support (i.e. $u^{-1}(\mathbb{R}^*)$) est borné.

Lemme 22 *Soit μ et μ' deux mesures vérifiant $\int u(x)\mu\{dx\} = \int u(x)\mu'\{dx\}$ pour tout $u \in \mathcal{C}_f$ alors $\mu = \mu'$.*

Preuve
Soit I un intervalle fini, sa fonction indicatrice peut être obtenue comme limite croissante de fonctions de $\mathcal{C}_f$. Le théorème de convergence monotone permet de conclure.

c.q.f.d. ◊◊◊

Proposition 23 *Soit une suite de mesures $\{\mu_n\}_{n\in\mathbb{N}}$ vérifiant $\sup(\mu_n\{I\}) < \infty$ pour tout intervalle fini I. Supposons que cette suite converge vers une mesure μ.*
Alors pour tout $u \in \mathcal{C}_f$, $lim_{n\to\infty} \int u(x)\mu_n\{dx\} = \int u(x)\mu\{dx\}$.

Preuve
Soit $u \in \mathcal{C}_f$ avec $M = \sup(|u(x)|)$. Choisissons $\varepsilon > 0$ arbitraire. Soit I un intervalle de continuité fini contenant le support de u. Notons $B \equiv \sup(\mu_n\{I\})$. Puisque u est uniformément continue, on peut partitionner I en intervalles de continuité $I_1, \ldots, I_k$ tel que pour tout $x \in I_j$ $|u(x) - u_j| \leq \varepsilon$ pour un $u_j \in u(I_j)$. Définissons v par $v(x) = u_j$ pour $x \in I_j$ et $v(x) = 0$ pour $x \in I^c$. Par hypothèse, il existe un n_0 tel que pour $n \geq n_0$ et tout j , on a $|\mu_n\{I_j\} - \mu\{I_j\}| \leq \varepsilon/k$. On a :
$\left|\int u(x)\mu\{dx\} - \int u(x)\mu_n\{dx\}\right| = \left|\sum_{j=1}^k \int_{I_j} u(x)\mu\{dx\} - \int_{I_j} u(x)\mu_n\{dx\}\right|$
$= \left|\sum_{j=1}^k \int_{I_j} u(x) - v(x)\mu\{dx\} + \int_{I_j} v(x)\mu\{dx\} - \int_{I_j} v(x)\mu_n\{dx\} + \int_{I_j} v(x) - u(x)\mu_n\{dx\}\right|$
$\leq \sum_{j=1}^k \int_{I_j} |u(x) - v(x)|\,\mu\{dx\} + M\varepsilon + \sum_{j=1}^k \int_{I_j} |v(x) - u(x)|\mu_n\{dx\}$
$\leq (\mu\{I\} + M + B)\varepsilon$

c.q.f.d. ◊◊◊

Le théorème de renouvellement

On confondra dans la suite, fonction de distribution et mesure de probabilité sur $\mathbb{R}$. Pour une mesure μ concentrée sur $\mathbb{R}^+$, on définit $\mu(x)$ par $\mu(x) \equiv \mu\{[0, x]\}$.

La convolution de deux distributions F, G notée $F \star G$ est la distribution d'une somme de deux variables indépendantes de distribution F et G. Elle est définie par :

$$F \star G(x) = \int_{-\infty}^{\infty} F(x - y)G\{dy\}$$

Dans le cas de variables positives elle s'écrit aussi :

$$F \star G(x) = \int_0^{\infty} F(x - y)G\{dy\} = \int_0^{x} F(x - y)G\{dy\}$$

On notera $F^{k\star}$, F convolée $k - 1$ fois avec elle-même. $F^{0\star}$ consiste en la distribution de Dirac concentrée en 0 i.e. $F^{0\star}(0) = 1$.

On introduit maintenant l'équation de renouvellement dont l'étude conduira aux résultats recherchés. Soit z une fonction nulle sur $\mathbb{R}^{-*}$. On s'intéresse aux solutions Z de l'équation :

$$Z(x) = z(x) + \int_0^{x} Z(x - y)F\{dy\} \tag{1.11}$$

On introduit à cet effet la mesure $U \equiv \sum_{n=0}^{\infty} F^{n\star}$.

Lemme 24 *Soit une distribution F de support $]0,\infty[$ et soit z une fonction bornée sur les intervalles finis. Alors :*

- *Pour tout x, $U(x)$ est fini. Plus précisément pour tout $h \geq 0$, il existe C_h tel que $U\{I\} \leq C_h$ pour tout intervalle I de longueur h.*
- *La fonction Z définie par $Z(x) \equiv \int_0^x z(x-y)U\{dy\}$ est l'unique solution de l'équation 1.11 bornée sur les intervalles finis.*

Preuve
Posons $U_n \equiv \sum_{k=0}^{n} F^{k\star}$. On remarque que :

$$\int_0^x (1 - F(x-y))\, U_n\{dy\} = 1 - F^{(n+1)\star}(x) \leq 1$$

Choisissons deux nombres strictement positifs τ et η tels que $1 - F(\tau) \geq \eta$. Par conséquent, $\eta(U_n(x) - U_n(x-\tau)) = \eta \int_{x-\tau}^{x} U_n\{dy\} \leq \int_{x-\tau}^{x} (1 - F(x-y))\, U_n\{dy\} \leq 1$. Par passage à la limite, on conclut que $U\{I\}$ est bornée par η^{-1} sur tout intervalle I de longueur τ, que $U\{I\}$ est bornée par $C_h \equiv \eta^{-1}(1 + \lfloor \frac{h}{\tau} \rfloor)$ sur tout intervalle I de longueur h et par suite que $U(x) \leq C_x$ est fini.

Par construction, $U_n(x)$ tend vers $U(x)$. Posons $Z_n = U_n \star z$, $Z_n(x)$ tend vers $Z(x)$ uniformément sur tout intervalle fini : $|Z(x) - Z_n(x)| \leq \sup_{y \leq x}(|z(y)|)(U(x) - U_n(x)))$. On remarque que $Z_{n+1} = z + F \star Z_n$. Puisque la convergence des Z_n est uniforme sur tout intervalle fini, on en déduit que $F \star Z_n$ tend vers $F \star Z$. D'où $Z = z + F \star Z$.

Notons V la différence de deux solutions bornées sur tout intervalle fini de l'équation 1.11. V satisfait $V = F \star V$. D'où par induction $V = F^{k\star} \star V$. $F^{k\star}$ tend vers 0 (U est fini) et V est borné. Par passage à la limite $V = 0$.

c.q.f.d. ◊◊◊

Afin d'établir le théorème de renouvellement, nous avons besoin d'une notion de fonction intégrable un peu plus forte que la notion usuelle.

Définition 25 *Une fonction z de $\mathbb{R}^+$ dans $\mathbb{R}^+$ est* directement Riemann intégrable *si en notant $m_{kh} = \inf(z(x) \mid kh \leq x < (k+1)h)$ et $M_{kh} = \sup(z(x) \mid kh \leq x < (k+1)h)$, on a :*

$$\lim_{h \to 0} h \sum_{k \in \mathbb{N}} m_{kh} = \lim_{h \to 0} h \sum_{k \in \mathbb{N}} M_{kh}$$

Nous utiliserons essentiellement cette notion dans le cas particulier suivant.

Proposition 26 *Une fonction décroissante et intégrable au sens de Lebesgue est directement Riemann intégrable.*

Preuve
Une fonction z est intégrable au sens de Lebesgue si :
$\sup\left(\sum_{i \in \mathbb{N}} \inf\left(z(x) \mid x \in E_i\right) \cdot m(E_i) \mid \{E_i\}_{i \in \mathbb{N}} \text{ partition mesurable dénombrable de } \mathbb{R}^+\right) < \infty$
avec m la mesure de Lebesgue sur la droite réelle.
Par conséquent, $\lim_{h \to 0} h \sum_{k \in \mathbb{N}} m_{kh}$ est finie et puisque $h \sum_{k \in \mathbb{N}} M_{kh} \leq hM_{0h} + h \sum_{k \in \mathbb{N}} m_{kh}$ en raison de la décroissance de z on conclut que les deux limites convergent.

c.q.f.d. ◊◊◊

La proposition suivante établit une corrélation entre le comportement asympotique de la mesure U et celui d'une solution Z de l'équation de renouvellement.

Proposition 27 *Soit F une distribution sur $\mathbb{R}^{+*}$ et U la mesure définie par $U \equiv \sum_{k \in \mathbb{N}} F^{k\star}$. Supposons qu'il existe η un réel positif et une suite d'instants t_n tel que :*

$$\lim_{t_n \to \infty} U(t_n) - U(t_n - h) = h\eta \text{ pour tout } \ h > 0$$

Alors pour toute fonction z directement Riemann intégrable, la solution correspondante Z de l'équation de renouvellement vérifie :

$$\lim_{n\to\infty} Z(t_n) = \eta \int_0^\infty z(x)dx \tag{1.12}$$

Preuve
Soit z_{kh}, la fonction indicatrice de l'intervalle $[kh, kh+h[$ et Z_{kh} la solution correspondante de l'équation de renouvellement. z étant fixé, m_{kh} et M_{kh} sont définis comme précédemment.

$Z_{kh}(x) \leq C_h$ pour tout k et tout x. Par conséquent, les sommes infinies de fonctions $Z_h^m \equiv \sum_k m_{kh} Z_{kh}$ et $Z_h^M \equiv \sum_k M_{kh} Z_{kh}$ sont finies et encadrent Z.
Pour tout ε, il existe k_0 tel qu'on ait $\sum_{k\geq k_0} M_{kh} \leq \varepsilon$. Choisissons n_0 tel que pour tout $n \geq n_0$, $|U(t_n) - U(t_n - h) - h\eta| \leq \varepsilon/k_0$, alors :
$|\sum_k M_{kh} Z_{kh}(t_n) - \sum_k h\eta M_{kh}| \leq$
$|\sum_{k<k_0} M_{kh} Z_{kh}(t_n) - \sum_{k<k_0} h\eta M_{kh}| + |\sum_{k\geq k_0} M_{kh} Z_{kh}(t_n)| + |h\eta \sum_{k\geq k_0} M_{kh}|$
$\leq (1 + C_h + h\eta)\varepsilon$
On en conclut que $\lim_{n\to\infty} Z_h^M(t_n) = \eta \sum_k h M_{kh}$.
Par un même raisonnement $\lim_{n\to\infty} Z_h^m(t_n) = \eta \sum_k h m_{kh}$.
Par conséquent, toute limite l d'une suite extraite convergente de $Z(t_n)$ vérifie :

$$\eta \sum_k h m_{kh} \leq l \leq \eta \sum_k h M_{kh}$$

En faisant tendre h vers 0, on obtient $l = \eta \int_0^\infty z(x)dx$. Puisque les $Z(t_n)$ sont bornés, on conclut que $\lim_{n\to\infty} Z(t_n)$ existe (lemme 16) et est égale à $\eta \int_0^\infty z(x)dx$.

c.q.f.d. ◊◊◊

Un *point d'accroissement* d'une mesure μ est un réel x tel que pour tout I intervalle ouvert contenant x, $\mu(I) > 0$. Une mesure est *arithmétique* s'il existe un réel $\lambda > 0$ tel que la mesure soit concentrée sur les atomes $k\lambda$ pour $k \in \mathbb{Z}$. Le plus grand λ vérifiant cette propriété est appelé la *période* de la mesure. La théorie du renouvellement a été étudiée dans le cas d'une distribution arithmétique au paragraphe 1.4.1. Nous nous intéressons ici au cas non arithmétique. Le lemme suivant établit une propriété essentielle des distributions non arithmétiques.

Lemme 28 *Soit une distribution non arithmétique F de support $]0, \infty[$ (i.e. $F(0) = 0$) et soit Σ, l'ensemble des points d'accroissement des distributions $F, F^{2\star}, F^{3\star}, \ldots$ (inclus dans ceux de $U = \sum_{i\in\mathbb{N}} F^{i\star}$). Alors Σ est* asymptotiquement dense *dans $\mathbb{R}^+$:*

$$\forall \varepsilon > 0 \ \exists x_\varepsilon \ \forall x \geq x_\varepsilon \ \Sigma \cap [x, x+\varepsilon] \neq \emptyset$$

Preuve
On observe d'abord que si a et b appartiennent à Σ alors $a + b \in \Sigma$ (preuve laissée au lecteur).

Supposons que $\delta \equiv \inf(b-a \mid a < b \in \Sigma) > 0$. Choisissons un couple $a, b \in \Sigma$ tel que $h \equiv b - a < 2\delta$. Soit $n \in \mathbb{N}$ tel que $nb \geq (n+1)a$, alors $\Sigma \cap [na, (n+1)a] = \{na + kh \mid na \leq na + kh \leq (n+1)a\}$. Puisque $(n+1)a \in \Sigma$, on en déduit que a et b sont des multiples de h. Soit c un autre point d'accroissement et soit n choisi maintenant tel $nh \geq c$. Alors $na \leq na + c \leq nb$, Par conséquent, c est aussi un multiple de h.

Nous avons donc établi que pour tout ε, il existe $a < b$ deux points de Σ avec $b - a < \varepsilon$. Comme vu précédemment, pour n_0 assez grand, $\bigcup_{n\geq n_0} [na, nb] = [n_0 a, \infty[$. Ce qui établit la propriété recherchée.

c.q.f.d. ◊◊◊

Lemme 29 *Soit F une distribution non arithmétique de support $]0,\infty[$ et soit g une fonction bornée et uniformément continue vérifiant pour tout x $g(x) \leq g(0)$. Si :*

$$g(x) = \int_0^\infty g(x-y)F\{dy\}$$

Alors pour tout x, on a $g(x) = g(0)$.

Preuve
Par induction, on déduit que $g(x) = \int_0^\infty g(x-y)F^{k\star}\{dy\}$. Par conséquent l'égalité n'est possible que si $g(-y) = g(0)$ pour tout $y \in \Sigma$ défini comme au lemme précedent. Puisque Σ est asympotiquement dense et que g est uniformément continue on déduit que $\lim_{y\to\infty} g(-y) = g(0)$.
Il existe $\delta > 0$ tel que $F(\delta) < 1$. Par conséquent, pour tout k et tout n :

$$F^{n\star}(k\delta) < \binom{n}{n-k}(1-F(\delta))^{n-k}$$

D'où pour tout k, $\lim_{n\to\infty} F^{n\star}(k\delta) = 0$.
Soient x et $\varepsilon > 0$ arbitraires, il existe y_0 tel que $\forall y \geq y_0$ $g(x-y) \geq g(0) - \varepsilon$. Soit maintenant n tel que $F^{n\star}(y_0) \leq \varepsilon$. D'où : $g(x) = \int_0^\infty g(x-y)F^{n\star}\{dy\} \geq \int_{y_0}^\infty g(x-y)F^{n\star}\{dy\} \geq (g(0)-\varepsilon)(1-\varepsilon)$.
En passant à la limite $g(x) \geq g(0)$. Puisque $g(x) \leq g(0)$, on en déduit que $g(x) = g(0)$.

c.q.f.d. $\Diamond\Diamond\Diamond$

Lemme 30 *Soit z une fonction continue dont le support est inclus dans $[0,h]$. Soit Z la solution correspondante de l'équation de renouvellement. Alors Z est uniformément continue et pour tout $a \geq 0$ on a :*

$$\lim_{x\to\infty} Z(x+a) - Z(x) = 0$$

Preuve
Dans un premier temps, supposons que z admet une dérivée continue. Considérons l'intervalle $[0,M]$ avec $M \geq x+\delta$. Pour tout y, on a $\delta^{-1}(z(x-y)-z(x+\delta-y)) = z'(x+\delta_x-y)$ avec $0 < \delta_x < \delta$. z' est uniformément continue dans $[0,M]$, soit $\varepsilon > 0$ il existe $\delta > 0$ tel que $|z'(u) - z'(v)| \leq \varepsilon$ si $|u-v| \leq \delta$.
Par conséquent :
$|\int_0^\infty \delta^{-1}(z(x-y) - z(x+\delta-y))U\{dy\} - \int_0^\infty \delta^{-1}(z'(x-y))U\{dy\}|$
$= |\int_0^M z'(x-y+\delta_x) - z'(x-y)U\{dy\}| \leq U(M)\varepsilon$.
Donc $Z(x)$ est dérivable de dérivée $\int_0^\infty z'(x-y)U\{dy\}$ et vérifie l'équation de renouvellement correspondant à z'.

Soit une fonction v continue de support $[0,h]$ et V la solution correspondante de l'équation de renouvellement. Le support de la fonction $v(x+\delta)-v(x)$ est contenue dans un intervalle de longueur $h+2\delta$ et par conséquent : $|V(x+\delta) - V(x)| \leq C_{h+2\delta} \sup|v(x+\delta) - v(x)|$. Ce qui démontre que puisque v est uniformément continue V est aussi uniformément continue. On applique ce raisonnement à z' ce qui établit que Z' est uniformément continue. D'autre part, Z' est bornée par $\sup(|z'|)C_h$.

Par conséquent, $\eta \equiv \limsup_{x\to\infty} Z'(x)$ est finie. Choisissons une séquence t_n telle que $Z'(t_n)$ tende vers η. La famille de fonctions $\zeta_n(x) \equiv Z'(t_n+x)$ est équicontinue. D'après la proposition 19, on peut en extraire une sous-suite $Z'(t_{n_r}+x)$ qui converge, uniformément sur tout intervalle fini, vers une limite ζ uniformément continue (et bornée).

Puisque ζ_n vérifie l'équation :

$$\zeta_n(x) = z'(t_n+x) + \int_0^\infty \zeta_n(x-y)F\{dy\}$$

On passe à la limite (justifiée pour l'intégrale par le théorème de convergence dominée) ce qui donne :

$$\zeta(x) = \int_0^\infty \zeta(x-y)F\{dy\}$$

ζ vérifie les hypothèses du lemme 29 (car $\zeta(0) = \eta$).

Par conséquent pour tout x, $Z'(t_{n_r} + x) \to \eta$ uniformément sur tout intervalle fini. Soit a quelconque, puisque $Z(t_{n_r} + a) - Z(t_{n_r}) = Z'(t_{n_r} + x)a$ pour un $x \in [0, a]$, on déduit que $\lim_{r\to\infty} Z(t_{n_r} + a) - Z(t_{n_r}) = a\eta$. Or Z est borné, donc $\eta = 0$. Le même raisonnement conduit à : $\liminf_{x\to\infty} Z'(x)$=0. D'où $\lim_{x\to\infty} Z'(x)$ existe et est égale à 0.

Par le théorème des accroissements finis, le résultat est établi pour une fonction z continument dérivable. Mais toute fonction continue à support dans $[0, h]$ peut être approchée à ε près par une fonction z_1, continument dérivable à support dans $[0, h]$. Soit Z_1 la solution correspondante de l'équation de renouvellement. Puisque $|z(x) - z_1(x)| \leq \varepsilon$, on a $|Z(x) - Z_1(x)| \leq C_h\varepsilon$. Soit a quelconque, pour x assez grand, $|Z_1(x + a) - Z_1(x)| \leq \varepsilon$. D'où $|Z(x + a) - Z(x)| \leq (2C_h + 1)\varepsilon$, ce qui achève la démonstration.

c.q.f.d. ◊◊◊

Théorème 31 *Soit F une distribution sur $\mathbb{R}^{+*}$ non arithmétique d'espérance (finie ou infinie) μ et U la mesure définie par $U \equiv \sum_{k\in\mathbb{N}} F^{k\star}$. Alors :*

$$\lim_{t\to\infty} U(t) - U(t + h) = \frac{h}{\mu} \text{ pour tout } \ h > 0$$

Preuve

Soit M une mesure quelconque, notons par M_t la mesure définie par $M_t\{I\} \equiv M\{I + t\}$ où I est un intervalle et $I + t$ est la translation par t de l'intervalle I. Soit I un intervalle fini quelconque, nous savons que $\sup_{t\in\mathbb{R}} U_t\{I\}$ est fini. En appliquant la proposition 21, on déduit qu'il existe une séquence $t_k \to \infty$ tel que $U_{t_k}\{I\}$ tende vers une mesure V.

Soit z une fonction continue dont le support est contenu dans $[0, a]$ et Z la solution correspondante de l'équation de renouvellement. Soit $x \geq 0$ un réel quelconque, on applique la proposition 23 :

$$\lim_{k\to\infty} Z(t_k+x+a) = \lim_{k\to\infty} \int_{t_k+x}^{t_k+x+a} z(t_k+x-y)U\{dy\} = \lim_{k\to\infty} \int_0^a z(a-y)U_{t_k+x}\{dy\} = \int_0^a z(a-y)V_x\{dy\}$$

Puisque $\lim_{k\to\infty} Z(t_k+x+a) = \lim_{k\to\infty} Z(t_k+a)$ (lemme 30), on en déduit que V et V_x coïncident sur les fonctions continues à support fini. D'après le lemme 22, $V = V_x$. La mesure V est donc invariante par translation. Nous laissons le soin au lecteur de démontrer que $V\{I\}$ est proportionnel à la longueur de I pour I un intervalle fini. Soit γ le facteur de proportionnalité, on déduit que : $\lim_{k\to\infty} U(t_k + h) - U(t_k) = h\gamma$ (tout intervalle est un intervalle de continuité de V).

En appliquant la proposition 27, on déduit que pour toute fonction z directement Rieman intégrable et Z la solution correspondante de l'équation de renouvellement, on a :

$$\lim_{k\to\infty} Z(t_k) = \gamma \int_0^\infty z(y)dy$$

Or la fonction $z = 1 - F$ est décroissante et Z la solution correspondante de l'équation de renouvellement est la constante 1 (preuve laissée au lecteur). De plus $\int_0^\infty z(y)dy$ est égale à μ. Si $\mu < \infty$ alors z est directement intégrable et par conséquent $\mu\gamma = 1$. Si $\mu = \infty$, on tronque z on conclut que $\gamma \int_0^a z(y)dy \leq 1$ pour tout a ce qui entraîne $\gamma = 0$.

Par conséquent γ est indépendant de la suite extraite et par application de la proposition 21, le résultat est établi.

c.q.f.d. ◊◊◊

Théorème 32 *Soit z une fonction directement intégrable, soit F une distribution sur $\mathbb{R}^{+*}$ non arithmétique d'espérance (finie ou infinie) μ soit Z la solution correspondante de l'équation de renouvellement. Alors :*

$$\lim_{x\to\infty} Z(x) = \mu^{-1} \int_0^\infty z(y)dy$$

Preuve
Il suffit de recopier la preuve de la proposition 27 en remplaçant t_n par x.

c.q.f.d. ◊◊◊

On généralise de manière triviale les résultats précédents au cas où F possède un atome en 0, i.e. $0 < p \equiv F(0) < 1$. En effet, on se ramène au cas précédent en considérant que les instants de renouvellement sont produits de la manière suivante :

- On choisit un nombre de répétitions d'occurrences de renouvellement au même instant avec une loi de Bernouilli de paramètre p.
- On choisit le prochain instant de renouvellement suivant la distribution G définie par $G(0) \equiv 0$ et $G(x) = (1-p)^{-1}F(x)$ pour $x > 0$.

Notons $U = \sum_{i\in\mathbb{N}} F^{i\star}$ et $V = \sum_{i\in\mathbb{N}} G^{i\star}$. D'après l'interprétation qui vient d'être développée, on a $U = (1-p)^{-1}V$. Par conséquent, les résultats sont identiques (preuve laissée au lecteur).

On généralise ensuite les résultats au cas d'un processus de renouvellement retardé, à savoir que le premier instant de renouvellement ne situe plus à l'instant 0 mais est fourni par une distribution G. Après cet instant, le processus se comporte comme un processus de renouvellement standard. En adoptant les mêmes notations $V(t)$, le nombre d'instants de renouvellement jusqu'à t, vérifie : $V = G \star U$. Par conséquent pour $h > 0$, on a :

$$V(t+h) - V(t) = \int_0^{t+h} U(t+h-y) - U(t-y)G\{dy\}$$

Soit t_0 tel que $1 - G(t_0) \leq \varepsilon$ et soit t_1 tel que pour tout $t \geq t_1$, on ait $|U(t+h) - U(t) - h/\mu| \leq \varepsilon$. Alors pour tout $t \geq t_0 + t_1$, on a :
$|V(t+h) - V(t) - h/\mu|$
$\leq \int_0^{t_0} |U(t+h-y) - U(t-y) - h\mu|G\{dy\} + \int_{t_0}^{t+h} |U(t+h-y) - U(t-y)|G\{dy\} + h/\mu \int_{t_0}^{\infty} G\{dy\}$
$\leq (1 + C_h + h/\mu)\varepsilon$

On peut effectuer un même raisonnement pour les solutions « retardées » de l'équation de renouvellement à condition qu'elles soient *bornées* ce qui conduit au théorème suivant qui inclut les généralisations précédentes.

Théorème 33 *Soit G une distribution quelconque sur $\mathbb{R}^+$, soit F une distribution sur $\mathbb{R}^+$ non arithmétique d'espérance (finie ou infinie) μ et U la mesure définie par $U \equiv \sum_{k\in\mathbb{N}} F^{k\star}$ et $V \equiv G \star U$. Alors :*

$$\lim_{t\to\infty} V(t) - V(t+h) = \frac{h}{\mu} \text{ pour tout } h > 0$$

De plus, soit z une fonction directement intégrable et soit Z la solution correspondante de l'équation de renouvellement. Si Z est bornée alors :

$$\lim_{x\to\infty} (G \star Z)(x) = \mu^{-1} \int_0^{\infty} z(y)dy$$

Ici $G \star Z$ est définie de manière analogue par $(G \star Z)(x) \equiv \int_0^x Z(x-y)G\{dy\}$.

1.4.4 CTMC

On rappelle qu'une CTMC est indifféremment spécifiée par son générateur infinitésimal $\mathbf{Q}$ ou sa matrice de transition $\mathbf{P}$ et son vecteur des taux de sortie λ. On rappelle aussi qu'on dit qu'une chaîne est dite irréductible si la chaîne incluse l'est aussi. La classification des états (transitoire, récurrent nul ou non nul) est identique à celle du cas discret. Nous laissons au lecteur le soin de démontrer que dans une CTMC irréductible tous les états ont le même statut (en s'aidant de la preuve pour le cas discret). On remarque aussi que le caractère récurrent dépend uniquement de $\mathbf{P}$ (mais pas le fait que les états soient récurrents nuls ou non nuls). Par conséquent, les états sont récurrents dans la CTMC ssi ils sont récurrents dans la DTMC incluse.

Nous fournissons d'abord un théorème analogue au théorème 15 dans le cas discret.

Théorème 34 *Soit une* CTMC *irréductible dont les états sont récurrents. Soit* $\mathbf{v}$ *un vecteur strictement positif solution de* $\mathbf{v} = \mathbf{v} \cdot \mathbf{P}$ *(unique à un facteur multiplicatif près). Alors le vecteur* $\mathbf{u}$ *défini par* $\mathbf{u}_i \equiv \frac{\mathbf{v}_i}{\lambda_i}$ *vérifie :*

$$\mathbf{u} \cdot \mathbf{Q} = 0$$

Inversement, soit $\mathbf{u}'$ *tel que* $\mathbf{u}' \cdot \mathbf{Q} = 0$ *et* $\forall i\ \mathbf{u}'_i \geq 0$*, alors il existe* λ *tel que* $\mathbf{u}'_i = \lambda \cdot \frac{\mathbf{v}_i}{\lambda_i}$

Preuve
L'existence du vecteur $\mathbf{v}$ strictement positif et unique à un facteur multiplicatif près est assurée par le théorème 15.
On a : $\forall i\ (p_{ii} - 1)\mathbf{v}_i + \sum_{j \neq i} p_{ji}\mathbf{v}_j = 0$
Soit : $\forall i\ (p_{ii} - 1)\lambda_i\mathbf{u}_i + \sum_{j \neq i} \lambda_j p_{ji}\mathbf{u}_j = 0$
Ce qui donne le résultat voulu : $\forall i\ q_{ii}\mathbf{u}_i + \sum_{j \neq i} q_{ji}\mathbf{u}_j = 0$

On observe que la transformation des équations peut se faire dans l'autre sens, ce qui achève la preuve.

c.q.f.d. ◊◊◊

Théorème 35 *Soit une* CTMC *irréductible dont les états sont récurrents. Si les états sont récurrents nuls alors la distribution transitoire tend vers 0 à l'infini sinon elle tend vers une distribution stationnaire* $\mathbf{u}$ *qui est l'unique solution de* $\mathbf{u} \cdot \mathbf{Q} = 0 \wedge \mathbf{u} \cdot \mathbf{1} = 1$.

De plus, soit $\mathbf{v}$ *un vecteur strictement positif solution de* $\mathbf{v} = \mathbf{v} \cdot \mathbf{P}$ *(unique à un facteur multiplicatif près). Alors les états sont récurrents non nuls ssi* $s \equiv \sum_{i \in \mathbb{N}} \frac{\mathbf{v}_i}{\lambda_i}$ *est fini.*

Preuve
Choisissons un état de la chaîne r. Puisque les états sont récurrents, la distribution F du temps de retour en r est bien définie et elle a une espérance (éventuellement infinie) que nous notons T_r. Notons $z_i(\tau)$ la probabilité d'être en i à l'instant τ sachant qu'initialement on est en r et qu'on n'a pas rencontré à nouveau r. Notons $Z_i(\tau)$ la probabilité d'être en i à l'instant τ sachant qu'initialement on est en i. On a : $Z_i(\tau) = z_i(\tau) + \int_0^\tau Z(\tau - y)F\{dy\}$.

Notons maintenant G la distribution (qui dépend de la distribution initiale de la chaîne) du temps d'atteinte de r et $Y_i(\tau)$ la probabilité d'être en i à l'instant τ après une visite en r. $Y_i = G \star Z_i$. En appliquant le théorème sur les processus de renouvellement retardés, on obtient $\lim_{\tau \to \infty} Y_i(\tau) = \frac{1}{T_r} \int_0^\infty z_i(\tau)d\tau$. Sachant que le probabilité de rencontrer r est 1, cette limite est aussi la limite de la probabilité d'être en i à l'instant τ. Il y a donc une limite de la distribution transitoire indépendante de la distribution initiale.

On remarque que $\sum_i \int_0^\infty z_i(\tau)d\tau = \int_0^\infty \sum_i z_i(\tau)d\tau$ (convergence monotone vers la somme infinie). Or $\sum_i z_i(\tau)$ représente la probabilité de ne pas avoir rencontré à nouveau r à l'instant t. Par conséquent, $\sum_i \int_0^\infty z_i(\tau)d\tau = T_r$.

Si $T_r = \infty$, cas des états récurrents nuls, alors la limite de la distribution transitoire est nulle sinon cette limite est bien une distribution $\mathbf{u}$ comme annoncé dans le théorème.

L'intégrale $\int_0^\infty z_i(\tau)d\tau$ compte le temps de séjour moyen en i avant de rencontrer à nouveau r. Elle peut se calculer en multipliant le nombre moyen de visites en i (avant de rencontrer à nouveau r) ${}_r\pi_{ri}$ par la durée moyenne d'un séjour en i, $\frac{1}{\lambda_i}$, soit : $\frac{{}_r\pi_{ri}}{\lambda_i}$. En appliquant les théorèmes 34 et 15, on conclut que $\mathbf{u}$ est l'unique solution de $\mathbf{u} \cdot \mathbf{Q} = 0 \wedge \mathbf{u} \cdot \mathbf{1} = 1$.

Puisque T_r est fini ssi $\sum_i \frac{{}_r\pi_{ri}}{\lambda_i}$ est fini la dernière assertion du théorème s'en suit.

c.q.f.d. ◊◊◊

Le lecteur attentif aura noté que ce théorème reste valable pour les processus semi-markoviens en adoptant comme convention que $\frac{1}{\lambda_i}$ est la durée moyenne de séjour dans l'état i et à condition qu'au moins une distribution de temps de séjour ne soit pas arithmétique.

Remarquons enfin que dès que les états d'une CTMC ne sont plus récurrents, la propriété exprimée par l'équation 1.1 n'est plus garantie. Par exemple, soit une chaîne infinie telle que les

seules transitions soient : $i \xrightarrow{2^i} i+1$. Alors le temps moyen d'une exécution est égale à 2, ce qui implique que presque sûrement les exécutions se déroulent en temps fini !

Chapitre 2

Model checking de DTMC finies

2.1 Logiques temporelles pour les DTMC

Nous introduisons ici une version « probabiliste » de la logique CTL* [EME 86] que nous désignerons sous le nom de PCTL*. La syntaxe de cette logique est définie inductivement à l'aide de formules d'état et de chemin.

Définition 36 *Soit $\mathcal{P}$, un ensemble de propositions atomiques.*
Une formule d'état de PCTL (relative à $\mathcal{P}$) est définie inductivement par :*
- *E_1 : Si $\phi \in \mathcal{P}$ alors ϕ est une formule d'état de PCTL* ;*
- *E_2 : Si ϕ et ψ sont des formules d'état de PCTL* alors $\neg\phi$ et $\phi \wedge \psi$ sont des formules de PCTL* ;*
- *E_3 : Si φ est une formule de chemin de PCTL*, $a \in [0,1]$ est un rationnel, $\bowtie \in \{=, \neq, <, \leq, >, \geq\}$ alors $P_{\bowtie a}\varphi$ est une formule d'état de PCTL*.*

Une formule de chemin de PCTL (relative à $\mathcal{P}$) est définie inductivement par :*
- *C_1 : Une formule d'état de PCTL* est une formule de chemin ;*
- *C_2 : Si φ et θ sont des formules de chemin de PCTL* alors $\neg\varphi$ et $\varphi \wedge \theta$ sont des formules de chemin de PCTL* ;*
- *C_3 : Si φ et θ sont des formules de chemin de PCTL* alors $\mathcal{X}\varphi$ et $\varphi\mathcal{U}\theta$ sont des formules de chemin de PCTL*.*

Comme dans le cas des systèmes de transitions non probabilisés, deux fragments de cette logique sont particulièrement intéressants. Le premier fragment noté PCTL par analogie avec CTL est constitué des règles de formation E_1, E_2, E_3, C'_3 où C'_3 s'énonce « Si ϕ et ψ sont des formules d'état de PCTL alors $\mathcal{X}\phi$ et $\phi\mathcal{U}\psi$ sont des formules de chemin de PCTL ». Le deuxième fragment noté PLTL par analogie avec LTL est constitué des règles de formation E_1, E_3, C'_1, C_2, C_3 où C'_1 s'énonce « Si $\varphi \in \mathcal{P}$ alors φ est une formule de chemin de PLTL ».

Nous expliquons dans les prochaines sections comment évaluer une formule de PCTL, de PLTL et de PCTL*.

La sémantique des formules est donnée ci-dessous. On considère $\mathcal{M}$ une chaîne de Markov dont les états sont étiquetés par un sous-ensemble de propositions atomiques. Cette étiquette correspond à la valuation $\nu : S \mapsto 2^{\mathcal{P}}$ On note s un état de la chaîne et $\sigma = s_0, s_1, \ldots$ un chemin infini dans le graphe associé à la chaîne de Markov. Le suffixe $s_i, s_{i+1}, \ldots$ est noté σ_i. On note aussi $\mathcal{M}, s \models \phi$ la satisfaction de la formule d'état ϕ par l'état s et $\sigma \models \varphi$ la satisfaction de la formule de chemin φ par le chemin σ.

Définition 37 *Soit $\mathcal{M}$ une chaîne de Markov, s un état de la chaîne et σ un chemin de la chaîne. La satisfaction d'une formule d'état ϕ par s est définie inductivement par :*
- *Si $\phi \in \mathcal{P}$ alors $\mathcal{M}, s \models \phi$ ssi ϕ étiquette s ;*
- *Si $\phi \equiv \neg\psi$ alors $\mathcal{M}, s \models \phi$ ssi $\mathcal{M}, s \not\models \psi$;*

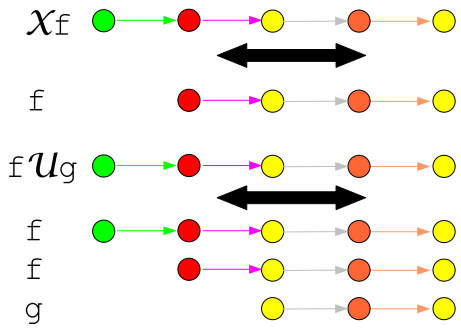

FIGURE 2.1 – Interprétation des opérateurs temporels $\mathcal{X}$ et $\mathcal{U}$

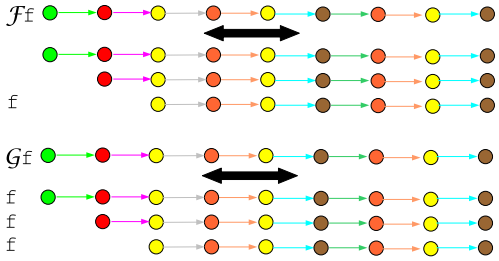

FIGURE 2.2 – Interprétation des opérateurs temporels $\mathcal{F}$ et $\mathcal{G}$

– $\phi \equiv \psi_1 \wedge \psi_2$ *alors* $\mathcal{M}, s \models \phi$ *ssi* $\mathcal{M}, s \models \psi_1$ *et* $\mathcal{M}, s \models \psi_2$;
– *Si* $\phi \equiv P_{\bowtie a}\varphi$ *alors* $\mathcal{M}, s \models \phi$ *ssi* $\Pr(\{\sigma \models \varphi\} \mid s_0 = s) \bowtie a$.

La satisfaction d'une formule de chemin φ *par* σ *est définie inductivement par :*

– *Si* φ *est une formule d'état alors* $\sigma \models \varphi$ *ssi* $\mathcal{M}, s_0 \models \varphi$;
– *Si* $\varphi \equiv \neg\theta$ *alors* $\sigma \models \varphi$ *ssi* $\sigma \not\models \theta$;
– *Si* $\varphi \equiv \theta_1 \wedge \theta_2$ *alors* $\sigma \models \varphi$ *ssi* $\sigma \models \theta_1$ *et* $\sigma \models \theta_2$;
– *Si* $\varphi \equiv \mathcal{X}\theta$ *alors* $\sigma \models \varphi$ *ssi* $\sigma_1 \models \theta$;
– *Si* $\varphi \equiv \theta_1 \mathcal{U} \theta_2$ *alors* $\sigma \models \varphi$ *ssi* $\exists i\ \sigma_i \models \theta_2$ *et* $\forall j < i\ \sigma_j \models \theta_1$.

Nous illustrons à la figure 2.1 l'interprétation des opérateurs temporels.

Cette sémantique suppose implicitement que l'ensemble des chemins qui vérifient une formule est mesurable. Cette supposition est justifiée et se démontre à l'aide de résultats élementaires de la théorie de la mesure mais qui dépassent le cadre de ce document (voir par exemple [VAR 85]). Aussi nous ne reviendrons plus sur ce point.

Des abréviations de formules sont fréquemment utilisées. Ainsi $\mathcal{F}\varphi \equiv \mathbf{tt}\ \mathcal{U}\varphi$ désigne le fait que φ sera nécessairement vraie sur un suffixe et $\mathcal{G}\varphi \equiv \neg\mathcal{F}\neg\varphi$ désigne le fait que φ sera vraie sur tous les suffixes. Nous illustrons à la figure 2.2 l'interprétation de ces opérateurs temporels.

2.2 Vérification de PCTL

Etant données une DTMC et une formule ϕ de PCTL, l'algorithme de vérification procède par évaluation successive des sous-formules de ϕ en « remontant » l'arbre syntaxique de la formule ϕ des feuilles à la racine et en étiquetant chaque état avec les sous-formules qu'il vérifie. Ainsi

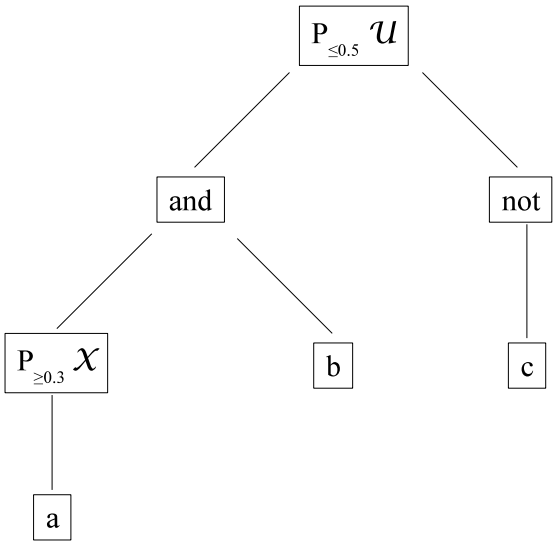

FIGURE 2.3 – Arbre syntaxique de $P_{\leq 0.5}((P_{\geq 0.3}\mathcal{X}a) \wedge b)\mathcal{U}(\neg c)$

chaque étape de l'algorithme évalue une formule en interprétant les opérandes de l'opérateur le plus externe comme des propositions atomiques. Ainsi sur l'exemple de la figure 2.3, on évaluera d'abord $(P_{\geq 0.3}\mathcal{X}a)$ qu'on remplacera par une proposition atomique disons a' puis $a' \wedge b$ qu'on remplacera par une formule atomique disons b', puis $\neg c$ qu'on remplacera par une formule atomique disons c' et enfin on évaluera $P_{\leq 0.5}b'\mathcal{U}c'$.

D'après les règles de construction, les formules à considérer sont les suivantes : $\neg\psi, \psi \wedge \chi, P_{\bowtie a}\mathcal{X}\psi, P_{\bowtie a}\psi\mathcal{U}\chi$ où ψ et χ sont des (formules transformées en) propositions atomiques. Nous indiquons ci-dessous comment l'algorithme procède en justifiant la correction de l'algorithme.

$\boxed{\phi = \neg\psi}$ L'algorithme étiquette avec ϕ chaque état non étiqueté avec ψ.

$\boxed{\phi = \psi \wedge \chi}$ L'algorithme étiquette avec ϕ chaque état étiqueté avec ψ et χ.

$\boxed{\phi = P_{\bowtie a}\mathcal{X}\psi}$ L'algorithme calcule la probabilité, disons p_s, d'atteindre en un pas un état étiqueté par ψ. Autrement dit, $p_s \equiv \sum_{s' \models \psi} \mathbf{P}[s, s']$ avec $\mathbf{P}$ la matrice de transition de la chaîne. s est alors étiqueté par ϕ ssi $p_s \bowtie a$.

$\boxed{\phi = P_{\bowtie a}\psi\mathcal{U}\chi}$ L'algorithme calcule la probabilité d'atteindre un état étiqueté par χ en passant uniquement par des états étiquetés par ψ. Notons p_s cette probabilité. Si $s \models \chi$ alors $p_s = 1$; si $s \not\models \chi$ et $s \not\models \psi$ alors $p_s = 0$. Afin de calculer p_s dans les autres cas, l'algorithme transforme la chaîne de Markov en rendant absorbant les états décrits précédemment, puis il calcule la probabilité dans cette chaîne d'atteindre les états qui satisfont χ devenus des composantes fortement connexes puits. Le calcul de cette probabilité a été décrit dans la section 1.2 et il est illustré par la figure 2.4. s est alors étiqueté par ϕ ssi $p_s \bowtie a$.

La figure 2.5 illustre le cas d'une c.f.c. terminale (les états 3 et 4) de la chaîne initiale qui vérifie $\neg\chi \wedge \psi$. Cette c.f.c. conduit à une probabilité nulle.

Le fragment qualitatif de PCTL

Intéressons-nous maintenant au fragment qualitatif de PCTL. Celui-ci est défini par restriction des opérateurs à $P_{\bowtie 1}\varphi$ et $P_{\bowtie 0}\varphi$.

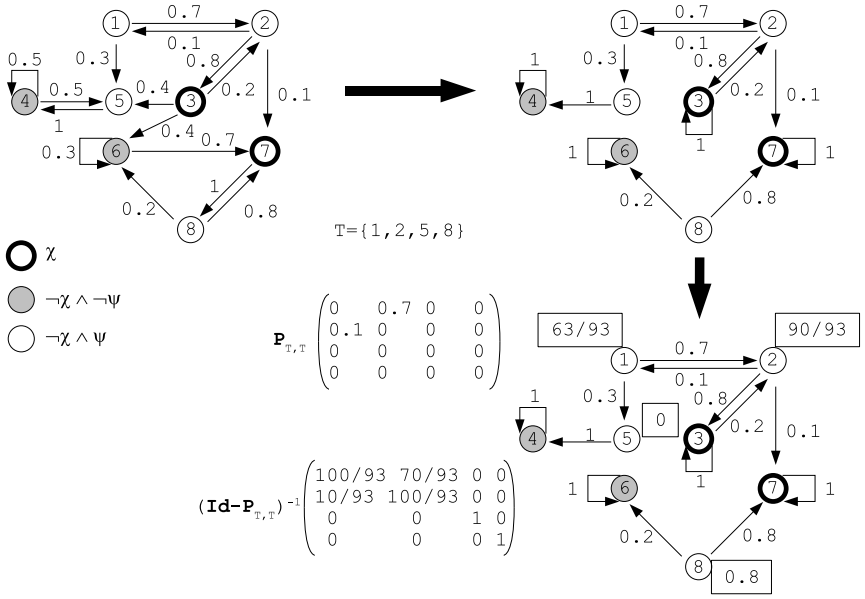

FIGURE 2.4 – Calcul de $P_{\bowtie a}\psi\mathcal{U}\chi$

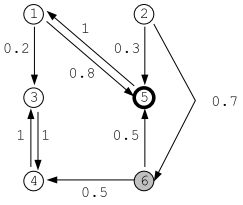

FIGURE 2.5 – Cas d'une c.f.c. terminale $\neg\chi \wedge \psi$

Nous allons démontrer que la vérification du fragment qualitatif ne dépend pas des valeurs exactes de $p_{i,j}$ mais uniquement du fait que $p_{i,j}$ soit ou non égal à 0 (on a aussi par la formule $p_{i,j} = 1 - \sum_{j' \neq j} p_{i,j'}$ connaissance du fait que $p_{i,j}$ soit ou non égal à 1). Nous analysons donc le graphe $G(\mathbf{P})$ associé à la chaîne et défini à la section 1.2.

Nous détaillons la vérification des formules $P_{=1}\psi\mathcal{U}\chi$ et $P_{=0}\psi\mathcal{U}\chi$. Tout d'abord la réponse est immédiate pour les états s tels que $s \models \chi \vee (\neg\chi \wedge \neg\psi)$. Afin de vérifier les deux formules pour les états s tels que $s \models \neg\chi \wedge \psi$, on transforme le graphe $G(\mathbf{P})$ en supprimant les arcs sortants des s tels que $s \models \chi \vee (\neg\chi \wedge \neg\psi)$ pour obtenir un graphe G'.

On rappelle alors l'observation suivante. La probabilité qu'un chemin infini de la chaîne rencontre les états s tels que $s \models \chi \vee (\neg\chi \wedge \neg\psi)$ ou termine dans une autre c.f.c. terminale de G' (donc aussi de G) est égale à 1. Par conséquent,

- $s \models P_{=1}\psi\mathcal{U}\chi$ ssi les c.f.c. terminales de G' accessibles depuis s sont incluses dans les états s' tels que $s \models \chi$.
- $s \models P_{=0}\psi\mathcal{U}\chi$ ssi les c.f.c. terminales de G' accessibles depuis s sont toutes différentes des états s' tels que $s \models \chi$.

Dans CTL les opérateurs d'états sont A avec pour sémantique « pour tout chemin issu de s, ... » et E avec pour sémantique « il existe un chemin issu de s tel que ... ». On peut comparer ces opérateurs avec les opérateurs du fragment qualitatif, lorsque les formules sont évaluées sur le graphe G :

- $P_{=1}\mathcal{X}\psi$ est équivalent à $A\mathcal{X}\psi$, $P_{>0}\mathcal{X}\psi$ est équivalent à $E\mathcal{X}\psi$ et $P_{>0}\psi\mathcal{U}\chi$ est équivalent à $E\psi\mathcal{U}\chi$. Les deux premières équivalences sont évidentes puisqu'on examine les arcs sortants de $s \xrightarrow{p_{s,s'}} s'$ (en nombre fini) tels que $p_{s,s'} > 0$ et $\sum_{s'} p_{s,s'} = 1$. La troisième équivalence provient du fait que si un chemin $\sigma = s_0, s_1, \ldots$ vérifie $\psi\mathcal{U}\chi$ alors il existe un préfixe fini de σ, $s_0, s_1, \ldots, s_n$, tels que tous les chemins issus de $s_0, s_1, \ldots, s_n$ vérifient $\psi\mathcal{U}\chi$. Or cet ensemble de chemins à une probabilité non nulle.
- $P_{=1}\psi\mathcal{U}\chi$ n'est pas équivalent à $A\psi\mathcal{U}\chi$. En effet dans G', s vérifie $A\psi\mathcal{U}\chi$ si toute c.f.c. (et pas seulement les composantes terminales) accessible depuis s, est soit triviale (réduite à un sommet sans boucle) soit l'un des sommets s' tels que $s' \models \chi$.

2.3 Agrégation de chaînes de Markov

Afin de démontrer la correction de l'algorithme de vérification de PLTL, nous rappelons les notions d'agrégation dans les chaînes de Markov. L'agrégation de chaînes de Markov finies est une méthode efficace lorsqu'on a affaire à de grandes chaînes [KS 60]. Son principe est simple : substituer à une chaîne, une chaîne « équivalente » où chaque état de la chaîne agrégée est un ensemble d'états de la chaîne originale. Il y a différentes versions de l'agrégation selon que la condition d'agrégation est valide pour toute distribution initiale (*agrégation forte*) ou pour au moins une distribution (*agrégation faible*). Nous introduisons simultanément l'agrégation pour les DTMC et les CTMC. Nous notons π_0 la distribution initiale de la chaîne et X_n (resp. X_t) la variable aléatoire décrivant l'état de la DTMC (resp. CTMC) à l'instant n (resp. t) (variables appelées Y au premier chapitre). $\mathbf{P}$ est la matrice de transition de la DTMC et $\mathbf{Q}$ est le générateur infinitésimal de la CTMC.

Définition 38 *Soient $\mathcal{M}$ une* DTMC *(resp. une* CTMC*) et $\{X_n\}_{n\in\mathbb{N}}$ (resp. $\{X_t\}_{t\in\mathbb{R}^+}$) la famille de variables aléatoires associées. Soit $\{S_i\}_{i\in I}$ une partition de l'espace d'états. Définissons Y_n pour $n \in \mathbb{N}$ (resp. Y_t pour $t \in \mathbb{R}^+$) la variable aléatoire $Y_n = i$ ssi $X_n \in S_i$ (resp. $Y_t = i$ ssi $X_t \in S_i$). Alors :*

- $\mathbf{P}$ *(resp.* $\mathbf{Q}$*) est* fortement agrégeable *selon* $\{S_i\}_{i\in I}$
  ssi il existe une matrice de transition $\mathbf{P}^{lp}$ *(resp. un générateur infinitésimal* $\mathbf{Q}^{lp}$*) t.q*
  $\forall\pi_0$ $\{Y_n\}_{n\in\mathbb{N}}$ *(resp.* $\{Y_t\}_{t\in\mathbb{R}^+}$*) est une* DTMC *(resp.* CTMC*)*
  de matrice de transition $\mathbf{P}^{lp}$ *(resp. de générateur infinitésimal* $\mathbf{Q}^{lp}$*).*

– **P** *(resp.* **Q***) est* faiblement agrégeable *selon* $\{S_i\}_{i\in I}$
ssi $\exists \pi_0$ $\{Y_n\}_{n\in\mathbb{N}}$ *(resp.* $\{Y_t\}_{t\in\mathbb{R}^+}$*) est une* DTMC *(resp.* CTMC*).*

Alors qu'une caractérisation de l'agrégation forte par examen de la matrice de transition ou du générateur infinitésimal est facile, la recherche d'une agrégation faible est bien plus difficile [Ledoux 96]. Aussi, nous introduisons l'agrégation exacte, un cas simple d'agrégation faible.

Définition 39 *Soient* $\mathcal{M}$ *une* DTMC *(resp. une* CTMC*) et* $\{X_n\}_{n\in\mathbb{N}}$ *(resp.* $\{X_t\}_{n\in\mathbb{R}^+}$*) la famille de variables aléatoires associées. Soit* $\{S_i\}_{i\in I}$ *une partition de l'espace d'états. Définissons* Y_n *pour* $n \in \mathbb{N}$ *(resp.* Y_t *pour* $t \in \mathbb{R}^+$ *) la variable aléatoire* $Y_n = i$ *ssi* $X_n \in S_i$ *(resp.* $Y_t = i$ *ssi* $X_t \in S_i$*). Alors :*

– *Une distribution initiale* π_0 *est équiprobable vis à vis de* $\{S_i\}_{i\in I}$
si $\forall i \in I, \forall s, s' \in S_i, \pi_0(s) = \pi_0(s')$.
– **P** *(resp.* **Q***) est* exactement agrégable *selon* $\{S_i\}_{i\in I}$
ssi il existe une matrice de transition $\mathbf{P}^{lp}$ *(resp. un générateur infinitésimal* $\mathbf{Q}^{lp}$*) t.q*
$\forall \pi_0$ *équiprobable* $\{Y_n\}_{n\in\mathbb{N}}$ *(resp.* $\{Y_t\}_{t\in\mathbb{R}^+}$*) est une* DTMC *(resp.* CTMC*)*
de matrice de transition $\mathbf{P}^{lp}$ *(resp. de générateur infinitésimal* $\mathbf{Q}^{lp}$*)*
et π_n *(resp.* π_t*) est équidistribuée.*

L'agrégation exacte et forte ont des caractérisations simples [PJSCH 84] rappelées dans la proposition suivante.

Proposition 40 *Soient* $\mathcal{M}$ *une* DTMC *(resp. une* CTMC*) et* **P** *(resp.* **Q***) la matrice de transition associée (resp. le générateur infinitésimal associé). Alors :*

– **P** *(resp.* **Q***) est fortement agrégeable selon* $\{S_i\}_{i\in I}$ *ssi*
$\forall i, j \in I\ \forall s, s' \in S_i\ \sum_{s''\in S_j} \mathbf{P}[s, s''] = \sum_{s''\in S_j} \mathbf{P}[s', s'']$
(resp. $\sum_{s''\in S_j} \mathbf{Q}[s, s''] = \sum_{s''\in S_j} \mathbf{Q}[s', s'']$*)*
– **P** *(resp.* **Q***) est exactement agrégeable selon* $\{S_i\}_{i\in I}$ *ssi*
$\forall i, j \in I\ \forall s, s' \in S_i\ \sum_{s''\in S_j} \mathbf{P}[s'', s] = \sum_{s''\in S_j} \mathbf{P}[s'', s']$
(resp. $\sum_{s''\in S_j} \mathbf{Q}[s'', s] = \sum_{s''\in S_j} \mathbf{Q}[s'', s']$*)*

Preuve
Nous faisons la preuve du premier point et laissons au lecteur le soin d'établir le deuxième point.

Supposons la condition remplie, soit π_n la distribution de X_n à l'instant n.
Définissons $\mathbf{P}^{lp}[i, j] = \sum_{s'\in S_j} \mathbf{P}[s, s']$ pour un $s \in S_i$ quelconque (bien définie d'après la condition).
Alors :
$\sum_{s\in S_i} \pi_{n+1}(s) = \sum_{s\in S_i} \sum_j \sum_{s'\in S_j} \pi_n(s')\mathbf{P}[s', s] =$
$\sum_j \sum_{s'\in S_j} \pi_n(s') \sum_{s\in S_i} \mathbf{P}[s', s] = \sum_j (\sum_{s'\in S_j} \pi_n(s'))\mathbf{P}^{lp}[j, i]$
Ce qui établit la condition suffisante.

Supposons maintenant que la condition ne soit pas remplie,
$\exists i, j \in I\ \exists s, s' \in S_i\ \sum_{s''\in S_j} \mathbf{P}[s, s''] \neq \sum_{s''\in S_j} \mathbf{P}[s', s'']$
Soient les deux distributions initiales $\pi_{0,s}$ et $\pi_{0,s'}$ concentrées en s et en s'. Ces deux distributions initiales conduisent au même Y_0. Alors :
$\sum_{s''\in S_j} \pi_{1,s}(s'') = \sum_{s''\in S_j} \mathbf{P}[s, s''] \neq \sum_{s''\in S_j} \mathbf{P}[s', s''] = \sum_{s''\in S_j} \pi_{1,s'}(s')$
Ce qui prouve que la matrice $\mathbf{P}^{lp}$ ne peut exister.

c.q.f.d. ◊◊◊

La figure 2.6 illustre le concept d'agrégation forte dans le cas d'une DTMC. Le corollaire suivant établit une condition suffisante d'agrégation exacte.

Corollaire 41 *Soient* $\mathcal{M}$ *une* DTMC *(resp. une* CTMC*) et* **P** *(resp.* **Q***) la matrice de transition associée (resp. le générateur infinitésimal associé). Alors* **P** *(resp.* **Q***) est exactement agrégeable selon* $\{S_i\}_{i\in I}$ *si :*

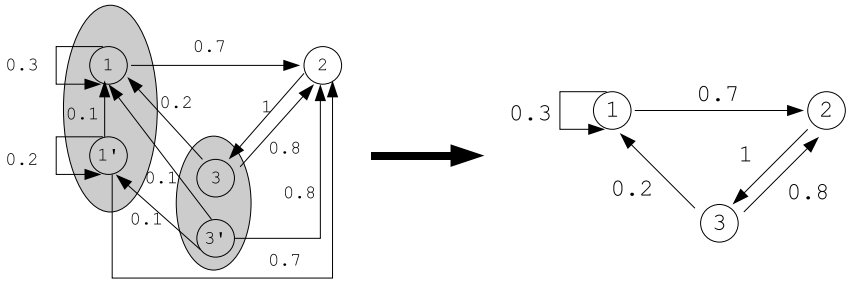

FIGURE 2.6 – Un exemple d'agrégation forte dans une DTMC

1. $\forall i \neq j \in I, \forall s, s' \in S_i, \sum_{s'' \in S_j} \mathbf{P}[s'', s] = \sum_{s'' \in S_j} \mathbf{P}[s'', s']$
   (resp. $\sum_{s'' \in S_j} \mathbf{Q}[s'', s] = \sum_{s'' \in S_j} \mathbf{Q}[s'', s']$*)*
2. $\forall i \in I, \forall s, s' \in S_i, \sum_{s'' \neq s \in S_i} \mathbf{P}[s'', s] = \sum_{s'' \neq s' \in S_i} \mathbf{P}[s'', s']$
   (resp. $\sum_{s'' \neq s \in S_i} \mathbf{Q}[s'', s] = \sum_{s'' \neq s' \in S_i} \mathbf{Q}[s'', s']$*)*
3. $\forall i \in I, \forall s, s' \in S_i, \mathbf{P}[s, s] = \mathbf{P}[s', s']$ *(resp.* $\mathbf{Q}[s, s] = \mathbf{Q}[s', s']$*)*

Quand l'agrégation forte est satisfaite la matrice de transition (resp. le générateur infinitésimal) de la chaîne agrégée peut être directement calculée à partir de la matrice de transition (resp. du générateur infinitésimal) de la chaîne originelle comme l'indique la proposition suivante (conséquence immédiate de la preuve de la proposition 40).

Proposition 42 *Soit $\mathcal{M}$ une* DTMC *(resp. une* CTMC*) qui est fortement agrégeable selon une partition de l'espace d'états $\{S_i\}_{i \in I}$. Soit $\mathbf{P}^{lp}$ (resp. $\mathbf{Q}^{lp}$) la matrice de transition (resp. le générateur infinitésimal) associée avec la chaîne agrégée, alors :*

$$\forall i, j \in I, \forall s \in S_i, \mathbf{P}^{lp}[i, j] = \sum_{s' \in S_j} \mathbf{P}[s, s'] \text{ (resp. } \mathbf{Q}^{lp}[i, j] = \sum_{s' \in S_j} \mathbf{Q}[s, s']\text{)}$$

Comme pour l'agrégation forte, en cas d'agrégation exacte la matrice de transition (resp. le générateur infinitésimal) de la chaîne agrégée peut être directement calculée à partir de la matrice de transition (resp. du générateur infinitésimal) de la chaîne originelle. Remarquons que démarrant avec une distribution initiale équidistribuée sur les états de chaque sous-ensemble de la partition, la distribution à tout instant est équidistribuée. Par conséquent, si la DTMC (resp. la CTMC) est ergodique, sa distribution stationnaire est équidistribuée entre les états de chaque sous-ensemble de la partition. Autrement dit, connaissant la matrice de transition (resp. le générateur infinitésimal) de la chaîne agrégée, on peut calculer sa distribution stationnaire, et déduire (par équidistribution *locale*) la distribution stationnaire de la chaîne originelle. Il faut souligner que cette dernière étape est impossible avec l'agrégation forte qui ne garantit pas l'équiprobabilité des états au sein d'un agrégat.

Proposition 43 *Soit $\mathcal{M}$ une* DTMC *(resp. une* CTMC*) qui est exactement agrégeable selon une partition de l'espace d'états $\{S_i\}_{i \in I}$. Soit $\mathbf{P}^{lp}$ (resp. $\mathbf{Q}^{lp}$) la matrice de transition (resp. le générateur infinitésimal) associée avec la chaîne agrégée, alors :*

- $\forall i, j \in I, \forall s \in S_j$ $\mathbf{P}^{lp}[i, j] = (\sum_{s' \in S_i} \mathbf{P}[s', s]) \times (|S_j|/|S_i|)$
  (resp. $\mathbf{Q}^{lp}[i, j] = (\sum_{s' \in S_i} \mathbf{Q}[s', s]) \times (|S_j|/|S_i|)$*)*
- *Si* $\forall i \in I, \forall s, s' \in S_i, \pi_0(s) = \pi_0(s')$ *alors*
  $\forall n \in \mathbb{N}$ *(resp.* $\forall t \in \mathbb{R}^+$*),* $\forall i \in I, \forall s, s' \in S_i$, $\pi_n(s) = \pi_n(s')$ *(resp.* $\pi_t(s) = \pi_t(s')$*),*
  où π_n (resp. π_t) est la distribution de probabilité à l'instant n (resp. t)
- *Si* $\mathbf{P}$ *(resp.* $\mathbf{Q}$*) est ergodique et π est sa distribution stationnaire alors*
  $\forall i \in I, \forall s, s' \in S_i, \pi(s) = \pi(s')$

2.4 Vérification de PLTL [COU 95]

Etant données une DTMC $\mathcal{M}$ et une formule ϕ de PLTL, on remarque que ϕ est soit une proposition atomique, soit $P_{\bowtie a}\varphi$ où φ est une formule de chemin obtenue à partir des opérateurs $\mathcal{X}$,$\mathcal{U}$ et des propositions atomiques. Dans le premier cas, la vérification est triviale. Aussi nous allons détailler le deuxième cas.

Comme précédemment, le principe de cette vérification consiste à évaluer les sous-formules de φ en remontant l'arbre syntaxique de la formule. Cependant, après chaque évaluation, l'algorithme transforme *à la fois la* DTMC *et la formule* de telle façon que la formule finale devienne une proposition atomique qui s'évalue immédiatement. La transformation de la formule substitue à une sous-formule φ' une nouvelle proposition atomique notée $[\varphi']$.

La transformation de la DTMC est plus complexe. Nous la décrivons dans le cas le plus difficile d'une sous-formule $\varphi' \equiv \psi\mathcal{U}\chi$. Chaque état s t.q. $0 < \Pr(\sigma \models \varphi' \mid s_0 = s) < 1$ (cette probabilité étant calculée dans la DTMC courante, dite chaîne originelle, par l'algorithme de PCTL) est dupliqué en deux états s^y étiqueté par $[\varphi']$ et les propositions atomiques satisfaites par s et s^n étiqueté uniquement par les propositions atomiques satisfaites par s. Les autres états sont étiquetés de manière similaire selon la valeur de cette probabilité (0 or 1). On note S_o l'ensemble des états non dupliqués.

La spécification des probabilités de transition entre états se fait ainsi :

- Les probabilités entre états de la chaîne originelle sont inchangés.
- Pour les états dupliqués, notons $py(s) = \Pr(\sigma \models \varphi' \mid s_0 = s)$ et $pn(s) = 1 - py(s)$. La probabilité de transition d'un état s' de la chaîne originelle vers s^y (resp. s^n) est celle de s' vers s dans la chaîne originelle multipliée par $py(s)$ (resp. $pn(s)$).
- Il y a uniquement des transitions de s^y (resp. s^n) vers des états s'^y (resp. s'^n) ou vers des états s' de la chaîne originelle t.q. $py(s') = 1$ (resp. $pn(s') = 1$). Les probabilités associées sont définies par $\mathbf{P}'[s^y, s'^y] = \mathbf{P}[s, s']py(s')/py(s)$ et $\mathbf{P}'[s^y, s'] = \mathbf{P}[s, s']/py(s)$ et de manière similaire pour les états s^n.

Afin de compléter la spécification de la transformation, il faut définir la probabilité de démarrer dans l'état s^y (resp. s^n) sachant que l'on démarre dans l'état s. Cette probabilité conditionnelle est $py(s)$ (resp. $pn(s)$). Par conséquent, $\pi'_0(s^y) = py(s)\pi_0(s)$ et $\pi'_0(s^n) = pn(s)\pi_0(s)$.

Observons que $\mathbf{P}'$ est bien une matrice de transition. Nous le démontrons uniquement pour un cas significatif.

$\sum_{s' \in S_o} \mathbf{P}'[s^y, s'] + \sum_{s' \in S \setminus S_o} \mathbf{P}'[s^y, s'^y] = \frac{1}{py(s)} \left(\sum_{s' \in S_o, py(s')=1} \mathbf{P}[s, s'] + \sum_{s' \in S \setminus S_o} \mathbf{P}[s, s']py(s') \right)$

Or en examinant un pas de la chaîne, on reconnaît que l'expression entre parenthèses est la probabilité $py(s)$.

Nous illustrons la transformation de la chaîne sur la figure 2.7 pour la sous-formule $\psi\mathcal{U}\chi$.

La correction de cette construction s'établit à partir des lemmes suivants.

Notations. On note $\mathcal{M}'$ la chaîne transformée. Définissons la fonction d'abstraction *abs* des états de $\mathcal{M}'$ t.q. $abs(s^y) = abs(s^n) = s$ et $abs(s) = s$ pour tout $s \in S_o$. Définissons le processus stochastique $\mathcal{M}^{abs}$ dont l'espace d'états est celui de $\mathcal{M}$ obtenu par l'abstraction *abs* à partir de $\mathcal{M}'$. Le lemme suivant est la clef de la correction de l'algorithme.

Lemme 44 *Le processus stochastique $\mathcal{M}^{abs}$ est une agrégation faible du processus $\mathcal{M}'$ (relativement à la distribution initiale π'_0) et il est identique à la chaîne de Markov $\mathcal{M}$.*

Preuve

Notons π_n (resp. π'_n) la distribution de $\mathcal{M}$ (resp. $\mathcal{M}'$) à l'instant n. Nous allons démontrer par récurrence sur n que :

$\forall s \in S_o\ \pi_n(s) = \pi'_n(s)$ et $\forall s \in S \setminus S_o\ \pi'_n(s^y) = \pi_n(s)py(s) \wedge \pi'_n(s^n) = \pi_n(s)pn(s)$

Pour $n = 0$, c'est la définition de π'_0. Supposons les équations vérifiées pour n. Démontrons-les pour $n+1$. Nous traitons ici uniquement le cas d'un état s^y et laissons au lecteur le soin de traiter les autres cas.

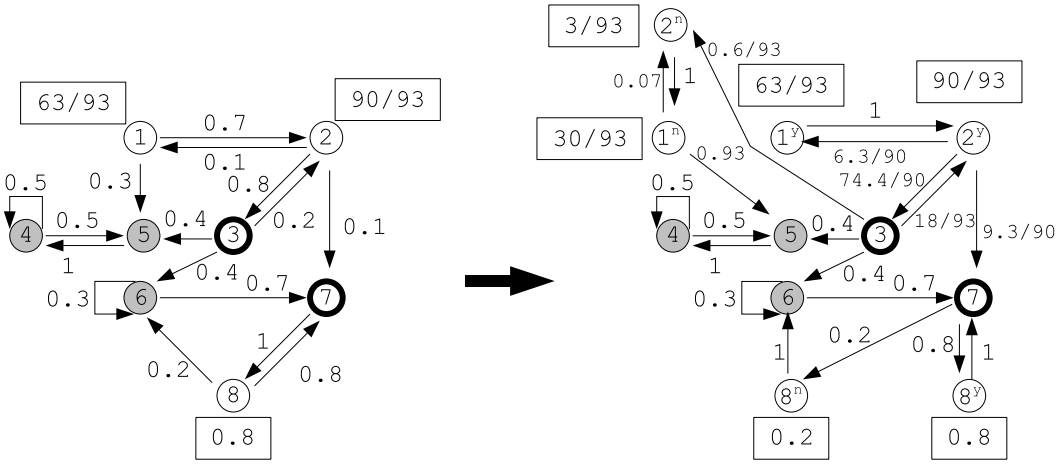

FIGURE 2.7 – Transformation de chaîne pour PLTL

$\pi'_{n+1}(s^y) = \sum_{s' \in S_o} \pi'_n(s')\mathbf{P}'[s, s^y] + \sum_{s'^y | s' \in S \setminus S_o} \pi'_n(s'^y)\mathbf{P}'[s'^y, s^y]$
$= \sum_{s' \in S_o} \pi_n(s')\mathbf{P}[s', s]py(s) + \sum_{s'^y | s' \in S \setminus S_o} \pi_n(s')py(s')\mathbf{P}'[s', s]\frac{py(s)}{py(s')}$
$= py(s)\left(\sum_{s' \in S_o} \pi_n(s')\mathbf{P}[s', s] + \sum_{s' \in S \setminus S_o} \pi_n(s')\mathbf{P}'[s', s]\right) = py(s)\pi_{n+1}(s)$

Le résultat est alors immédiat puisque dans $\mathcal{M}^{abs}$, $\forall s \in S \setminus S_o$ $\pi_n^{abs}(s) = \pi'_n(s^y) + \pi'_n(s^n)$.

c.q.f.d. ◊◊◊

Un chemin est dit *normal* s'il se termine dans une c.f.c. terminale qui contient un état de S_o et visite infiniment souvent les états de cette c.f.c.

Lemme 45 *Toute c.f.c. terminale de $\mathcal{M}$ et de $\mathcal{M}'$ contient un état de S_o. Par conséquent, l'ensemble des chemins normaux est de mesure 1 dans $\mathcal{M}$ et dans $\mathcal{M}'$.*

Preuve
Rappelons qu'un chemin aléatoire a une probabilité 1 de rencontrer une c.f.c. terminale et visiter ses états infiniment souvent. Examinons les différents cas pour une c.f.c. terminale dans $\mathcal{M}$ ou $\mathcal{M}'$.

- Il existe un état de la c.f.c. vérifiant χ ou vérifiant $\neg\chi \wedge \neg\psi$. Cet état appartient à S_o.
- Tous les états de la c.f.c. vérifient $\neg\chi \wedge \psi$. Dans $\mathcal{M}$, cela conduit à $pn(s) = 1$ pour un état s quelconque de cette c.f.c. Supposons que dans $\mathcal{M}'$, la c.f.c. (disons C) ne contienne que des états dupliqués. Sélectionnons l'un de ces états, dupliqué à partir de s.
  1. Cet état est s^y. Dans $\mathcal{M}$, il y a un chemin de s vers un état s' vérifiant χ et dont les états intermédiaires vérifient $\neg\chi \wedge \psi$. Ce chemin donne lieu à un chemin dans $\mathcal{M}'$ de s^y vers s'. Par conséquent $s' \in C$, d'où une contradiction.
  2. Cet état est s^n. Dans $\mathcal{M}$, il y a (1) soit un chemin de s vers un état s' vérifiant $\neg\chi \wedge \neg\psi$ et dont les états intermédiaires vérifient $\neg\chi \wedge \psi$, (2) soit un chemin de s vers un état s' appartenant à une c.f.c. terminale dont tous les états vérifient $\neg\chi \wedge \psi$ et tel que les états intermédiaires du chemin vérifient $\neg\chi \wedge \psi$. Dans les deux cas, ce chemin donne lieu à un chemin dans $\mathcal{M}'$ de s^n vers s'. Par conséquent $s' \in C$, d'où une contradiction.

c.q.f.d. ◊◊◊

Soit φ'' une sous-formule de φ où apparaît φ'. Notons $\varphi''(\varphi' \leftarrow [\varphi'])$, la formule φ'' dans laquelle φ' a été remplacée par la proposition atomique $[\varphi']$.

Lemme 46 *Soit une sous-formule φ'' de φ où apparaît φ'. On a pour tout chemin normal σ, $\sigma \models \varphi''(\varphi' \leftarrow [\varphi']) \Leftrightarrow \varphi''$. Par conséquent, soit σ un chemin aléatoire de $\mathcal{M}'$, $\Pr(\sigma \models \varphi''(\varphi' \leftarrow [\varphi']) \Leftrightarrow \varphi'') = 1$.*

Preuve
On établit la preuve par induction sur la taille de φ''.

Le cas de base correspond à $\varphi'' = \varphi'$. Supposons que $\sigma \models \varphi'$. Cela signifie qu'il existe un préfixe de σ t.q. $\neg\chi \wedge \psi$ soit vérifié par les états intermédiaires et que χ soit vérifié sur le dernier état. Ce chemin se « projette » par abstraction sur un chemin de $\mathcal{M}$. Par conséquent on observe qu'aucun état de ce chemin n'appartient à S_o avec $py(s) = 0$. Démontrons que pour tout état du préfixe que soit cet état appartient à S_o, disons s, et $py(s) = 1$, soit cet état est de la forme s^y. Supposons que ce ne soit pas le cas et considérons le dernier état du préfixe qui ne vérifie pas cette condition. L'état en question ne peut être le dernier état qui vérifie χ. D'après l'observation précédente, cet état est de la forme s^n mais (1) soit son successeur appartient à S_o, disons s, et $py(s) = 1$, (2) soit son successeur est de la forme s^y. Dans les deux cas, ceci est en contradiction avec la construction de $\mathcal{M}'$. Donc le premier état du chemin vérifie $[\varphi']$.

Supposons que $\sigma \models [\varphi']$. Le premier état est soit un état qui appartient à S_o, disons s, et $py(s) = 1$, soit un état de la forme s^y. D'un état de la forme s^y on ne peut atteindre (en un pas) qu'un état qui appartient à S_o, disons s, et $py(s) = 1$ ou qu'un état de la forme s^y. Puisque le chemin est normal, il existe donc un préfixe fini de σ dont les états intermédiaires sont de la forme s^y (et donc vérifient ψ) et le dernier état appartient S_o, disons s alors $py(s) = 1$. Si $s \models \chi$ alors $\sigma \models \varphi'$. Sinon $s \models \psi$ et tout successeur s' de s appartient à S_o avec $py(s') = 1$. On itère le raisonnement et soit on obtient un préfixe fini de σ témoin de la satisfaction de φ', soit une c.f.c. terminale de $\mathcal{M}'$ dont tous les états s appartiennent à S_o avec $py(s) = 1$ mais tels que $s \models \neg\chi$. En prenant dans $\mathcal{M}$ n'importe quel chemin fini issu de s dont les états intermédiaires satisfont ψ et dont le dernier état s' satisfait χ, on obtient que s appartient à cette c.f.c. terminale, d'où une contradiction puisque σ visite tous les états de la c.f.c.

Pour le pas d'induction, on observe d'abord qu'un suffixe d'un chemin normal est un chemin normal. Nous ne développons la preuve que pour le cas $\varphi'' \equiv \theta\mathcal{U}\theta'$. Soit $\sigma = s_0, s_1, \ldots$ un chemin normal,

$$\begin{array}{c}
\sigma \models \varphi'' \\
\textit{ssi} \\
\text{il existe } i \text{ t.q. } s_i, s_{i+1}, \ldots \models \theta' \text{ et pour tout } j < i,\ s_j, s_{j+1}, \ldots \models \theta \\
\textit{ssi en raison de l'hypothèse d'induction et de l'observation précédente} \\
\text{il existe } i \text{ t.q. } s_i, s_{i+1}, \ldots \models \theta'(\varphi' \leftarrow [\varphi']) \text{ et pour tout } j < i,\ s_i, s_{j+1}, \ldots \models \theta(\varphi' \leftarrow [\varphi']) \\
\textit{ssi} \\
\sigma \models \varphi''(\varphi' \leftarrow [\varphi'])
\end{array}$$

c.q.f.d. $\Diamond\Diamond\Diamond$

Notons que le lemme précédent s'applique à $\varphi'' = \varphi$. Nous pouvons maintenant établir la correction de l'algorithme.

Théorème 47 *Soit σ (resp. σ') un chemin aléatoire de $\mathcal{M}$ (resp. $\mathcal{M}'$). Alors :*

$$\Pr_{\mathcal{M}}(\sigma \models \varphi) = \Pr_{\mathcal{M}'}(\sigma' \models \varphi(\varphi' \leftarrow [\varphi']))$$

Preuve
$\Pr_{\mathcal{M}}(\sigma \models \varphi) = \Pr_{\mathcal{M}^{abs}}(\sigma^{abs} \models \varphi)$
(lemme 44)
$= \Pr_{\mathcal{M}'}(\sigma' \models \varphi)$
En effet la valeur de vérité de φ d'un chemin σ' ne dépend que de son abstraction σ^{abs}.
$= \Pr_{\mathcal{M}'}(\sigma' \models \varphi \wedge \varphi(\varphi' \leftarrow [\varphi'])) = \Pr_{\mathcal{M}'}(\sigma' \models \varphi(\varphi' \leftarrow [\varphi']))$
(lemme 46)

c.q.f.d. $\Diamond\Diamond\Diamond$

Le fragment qualitatif de PLTL
Intéressons-nous maintenant au fragment qualitatif de PLTL. Celui-ci est défini par restriction des opérateurs à $P_{\bowtie 1}\varphi$ et $P_{\bowtie 0}\varphi$.

Nous allons démontrer que la vérification du fragment qualitatif ne dépend pas des valeurs exactes de $p_{i,j}$ mais uniquement du fait que $p_{i,j}$ soit ou non égal à 0 (on a aussi par la formule $p_{i,j} = 1 - \sum_{j' \neq j} p_{i,j'}$ connaissance du fait que $p_{i,j}$ soit ou non égal à 1). Nous analysons donc le graphe $G(\mathbf{P})$ associé à la chaîne et défini plus haut. Nous appliquons itérativement la construction précédente sans tenir compte des probabilités mais uniquement des arcs. Ceci est possible car la duplication dépend uniquement de $G(\mathbf{P})$. Dans le graphe expansé final, on procède comme pour le fragment qualitatif de PCTL. Une fois cette opération effectuée, s satisfait la formule $P_{=1}\varphi$ si toutes ses instances (obtenues par duplications successives) la satisfont. De même s satisfait la formule $P_{=0}\varphi$ si aucune de ses instances ne la satisfait.

2.5 Vérification de PCTL*

Etant données une DTMC et une formule ϕ de PCTL*, l'algorithme de vérification procède dans l'arbre syntaxique de la formule ϕ par évaluation successive des sous-arbres de ϕ correspondant aux formules de PLTL et en étiquetant chaque état avec les sous-formules qu'il vérifie et en substituant à la sous-formule une proposition atomique. Ainsi chaque étape de l'algorithme évalue une formule de PLTL.

Chapitre 3

Model checking de systèmes temps-réels probabilistes

Ce chapitre se divise en deux parties selon que l'on considère un temps discret ou un temps dense.

3.1 Systèmes probabilistes avec durées [LS 05]

Un système probabiliste avec durée est proche d'une DTMC. La seule différence réside dans la visite d'un état qui a une durée fixe entière dépendant de l'état.

Définition 48 *Un système probabiliste avec durées $\mathcal{A} = (S, \nu, d, next)$ est défini par :*
- *S, l'ensemble fini des états ;*
- *$\nu : S \mapsto 2^{\mathcal{P}}$ définit l'ensemble des propriétés satisfaites par les états ;*
- *$d : S \mapsto \mathbb{N}$ désigne la durée de la visite en un état ;*
- *$next : S \mapsto [0,1]^S$ désigne le successeur (aléatoire) d'un état avec $next(s)$ une distribution de probabilité, i.e. $\sum_{s' \in S} next(s)(s') = 1$.*

Dans la suite, $next(s, s')$ est une notation alternative pour $next(s)(s')$. Un système est *fortement non Zénon* s'il n'existe pas de suite d'états $s_0, \ldots, s_n$ avec $next(s_i)(s_{i+1}) > 0$, $s_0 = s_n$ et $d(s_i) = 0$ pour tout $i < n$. Comme son nom l'indique le caractère fortement non Zénon garantit que le processus diverge temporellement avec probabilité 1. D'autres critères plus fins pourraient être envisagés.

La sémantique (en temps discret) du processus stochastique se décline selon deux points de vue : la sémantique *de saut* et la sémantique *continue*.

Dans la sémantique de saut, la durée de visite s'interprète comme une durée de transition indivisible. Aussi une exécution du système est une suite infinie $\sigma = (s_0, \tau_0), (s_1, \tau_1), \ldots$ avec $\tau_0 = 0$ et pour tout i, $\tau_{i+1} = \tau_i + d(s_i)$ et $next(s_i)(s_{i+1}) > 0$. On parle de sémantique de saut car on « saute » certains instants discrets du temps.

Dans la sémantique continue, la durée s'interprète comme une durée de transition divisible en pas de durée unitaire ou nulle. Autrement dit, le système s'interprète préalablement comme un système probabiliste avec des durées de transition égales à 0 ou 1. Aussi l'ensemble des *configurations* du système est définie par l'ensemble :

$$\Omega = \{(s, i) \mid s \in S \wedge 0 < i < d(s)\} \cup \Omega = \{(s, 0) \mid s \in S\}$$

Les transitions (probabilistes) sont définies par la fonction *next* suivante :
- Si $d(s) = 0$ alors $next(s, 0)(s', 0) = next(s)(s')$ (et 0 ailleurs) avec une durée de transition nulle.

– Si $d(s) > 0$ alors $next(s, d(s) - 1)(s', 0) = next(s)(s')$ (et 0 ailleurs) avec une durée de transition égale à 1.
– $\forall 0 \leq i < d(s) - 1$ $next(s, i)(s, i + 1) = 1$ (et 0 ailleurs) avec une durée de transition égale à 1.

Observons que ce nouveau système peut avoir une taille exponentielle en fonction de la taille du système initial. Ceci est dû au « dépliage » des durées de visite codées en binaire. Les séquences d'exécution du système original en sémantique continue sont les séquences d'exécution du système déplié.

3.2 Logiques temporelles pour les systèmes probabilistes avec durées

Nous développerons une méthode de model checking pour une logique étendue adaptée aux systèmes temps-réels. Aussi nous introduisons maintenant une version « probabiliste » de la logique TCTL [ACD 93] que nous désignerons sous le nom de PTCTL. La syntaxe de cette logique est définie inductivement à l'aide de formules d'état et de chemin.

Définition 49 *Soit $\mathcal{P}$, un ensemble de propositions atomiques.*
Une formule d'état de PTCTL *(relative à $\mathcal{P}$) est définie inductivement par :*
E_1 *: Si $\phi \in \mathcal{P}$ alors ϕ est une formule d'état de* PTCTL *;*
E_2 *: Si ϕ et ψ sont des formules d'état de* PTCTL *alors $\neg\phi$ et $\phi \wedge \psi$ sont des formules de* PTCTL *;*
E_3 *: Si φ est une formule de chemin de* PTCTL*, $a \in [0, 1]$ est un rationnel, $\bowtie \in \{=, \neq, <, \leq, >, \geq\}$ alors $P_{\bowtie a}\varphi$ est une formule d'état de* PTCTL*.*
Une formule de chemin de PTCTL *(relative à $\mathcal{P}$) est définie inductivement par :*
C *: Si φ et θ sont des formules d'état de* PTCTL*, d est un entier, $\sim \in \{=, \leq, \geq\}$ alors $\varphi \mathcal{U}_{\sim d} \theta$ et $\mathcal{X}\varphi$ sont des formules de chemin de* PTCTL*.*

Etant donnée une exécution infinie σ, on désigne par $\sigma(i)$ la $i$ème configuration de σ et $Time(\sigma, i)$ le temps d'atteinte de cette configuration. La satisfaction présentée ci-dessous est valable à la fois pour la sémantique de saut (les configurations sont les états) et la sémantique continue (les configurations sont des paires (état, durée) et les propriétés atomiques satisfaites par la configuration sont celles satisfaites par l'état).

Définition 50 *Soit $\mathcal{A}$ un système probabiliste, s une configuration du système et σ une exécution infinie.*
La satisfaction d'une formule d'état ϕ par s est définie inductivement par :
– *Si $\phi \in \mathcal{P}$ alors $\mathcal{A}, s \models \phi$ ssi ϕ étiquette s ;*
– *Si $\phi \equiv \neg\psi$ alors $\mathcal{A}, s \models \phi$ ssi $\mathcal{A}, s \not\models \psi$;*
– *$\phi \equiv \psi_1 \wedge \psi_2$ alors $\mathcal{A}, s \models \phi$ ssi $\mathcal{A}, s \models \psi_1$ et $\mathcal{A}, s \models \psi_2$;*
– *Si $\phi \equiv P_{\bowtie a}\varphi$ alors $\mathcal{A}, s \models \phi$ ssi $\Pr(\{\sigma \models \varphi\} \mid \sigma$ démarre en $s) \bowtie a$.*
La satisfaction d'une formule de chemin φ par σ est définie inductivement par :
– *Si $\varphi \equiv \mathcal{X}\theta$ alors $\sigma \models \varphi$ ssi $\sigma(1) \models \theta$;*
– *Si $\varphi \equiv \theta_1 \mathcal{U}_{\sim d} \theta_2$ alors $\sigma \models \varphi$ ssi $\exists i \in \mathbb{N}$ $Time(\sigma, i) \sim d$, $\sigma(i) \models \theta_2$ et $\forall i' < i$ $\sigma(i') \models \theta_1$.*

Remarquons que dans le cas d'un $\mathcal{U}_{=c}$ la formule peut être non satisfaite par l'absence de configuration à l'instant c.

Nous étudierons aussi le fragment PTCTL$[\leq, \geq]$ obtenu en interdisant les tests d'égalité sur les durées et les fragments qualitatifs qui imposent que les seuils des probabilités soient uniquement 0 et 1.

3.3 Algorithmes de vérification pour systèmes probabilistes avec durées

3.3.1 Vérification de formules de PTCTL

Les algorithmes que nous décrivons ici sont des algorithmes « bottom-up » qui étiquettent les états ou les configurations du système en partant des sous-formules les plus internes et en remontant l'arbre syntaxique de la formule. Dans toute cette partie, nous nous concentrons sur les formules d'état faisant apparaître le $\mathcal{U}$, les autres cas (relativement faciles) étant laissés en exercice.

Nous indiquons d'abord comment effectuer la vérification dans le cas de la sémantique de saut. Il s'agit dans tous les cas de comparer avec un seuil la probabilité de satisfaction d'une formule par un chemin aléatoire. L'algorithme 1 effectue le calcul de cette probabilité pour les formules $\varphi \mathcal{U}_{\leq c} \psi$, $\varphi \mathcal{U}_{=c} \psi$ et $\varphi \mathcal{U}_{\geq c} \psi$ où l'on suppose que φ et ψ étiquettent les états. Il utilise pour cela une technique de programmation dynamique en calculant de manière incrémentale les probabilités pour les formules où i (avec $0 \leq i \leq c$) est substitué à c.

Afin de gérer les durées nulles, le parcours des états dans les boucles est effectué selon un tri topologique qui garantit que si $d(s) = 0$ et $next(s, s') > 0$ alors s' est examiné avant s.

Algorithme 1 : Evaluation de PTCTL dans le cadre de la sémantique de saut

Data : $T[\mathbb{N}, S]$ un tableau contenant les calculs intermédiaires
`Calculinfeq`(φ, ψ, c)
Input : φ, ψ, c, les termes de la formule $\varphi \mathcal{U}_{\leq c} \psi$
Data : i un indice, s, s' des états
for $i \leftarrow 0$ **to** c **do**
  for $s \in S$ **do**
    if $s \models \psi$ **then** $T[s, i] \leftarrow 1$
    else if $(s \not\models \varphi) \vee (i < d(s))$ **then** $T[s, i] \leftarrow 0$
    else $T[s, i] \leftarrow \sum_{s' \in S'} next(s, s') T[s', i - d(s)]$
  end
end

`Calculeq`(φ, ψ, c)
Input : φ, ψ, c, les termes de la formule $\varphi \mathcal{U}_{=c} \psi$
Data : i un indice, s, s' des états
for $i \leftarrow 0$ **to** c **do**
  for $s \in S$ **do**
    if $i = 0 \wedge s \models \psi$ **then** $T[s, i] \leftarrow 1$
    else if $(s \not\models \varphi) \vee (i < d(s))$ **then** $T[s, i] \leftarrow 0$
    else $T[s, i] \leftarrow \sum_{s' \in S'} next(s, s') T[s', i - d(s)]$
  end
end

`Calculsupeq`(φ, ψ, c)
Input : φ, ψ, c, les termes de la formule $\varphi \mathcal{U}_{\geq c} \psi$
Data : i un indice, s, s' des états
for $i \leftarrow 0$ **to** c **do**
  for $s \in S$ **do**
    if $i = 0$ **then** $T[s, i] \leftarrow \Pr(\sigma \models \varphi \mathcal{U} \psi \mid \sigma_0 = s)$; `// cf section 2.2`
    else if $s \not\models \varphi$ **then** $T[s, i] \leftarrow 0$
    else $T[s, i] \leftarrow \sum_{s' \in S'} next(s, s') T[s', \max(i - d(s), 0)]$
  end
end

Nous établissons la correction de l'algorithme 1.

$\theta \equiv \varphi \mathcal{U}_{\leq i} \psi$**.** Si un état s satisfait ψ alors tout chemin issu de s satisfait θ. Sinon s doit satisfaire φ, le prochain changement d'état a lieu en au plus tard i unités de temps et l'état atteint doit satisfaire $\varphi \mathcal{U}_{\leq i-d(s)} \psi$.

$\theta \equiv \varphi \mathcal{U}_{=i} \psi$**.** Si un état s satisfait ψ et $i = 0$ alors tout chemin issu de s satisfait θ. Sinon s doit satisfaire φ, le prochain changement d'état a lieu en au plus tard i unités de temps et l'état atteint doit satisfaire $\varphi \mathcal{U}_{=i-d(s)} \psi$.

$\theta \equiv \varphi \mathcal{U}_{\geq i} \psi$**.** Si $i = 0$ alors la durée des séjours dans les états n'est plus significative et le calcul s'effectue dans la DTMC obtenue en oubliant les durées. Sinon s doit satisfaire φ et l'état atteint doit satisfaire $\varphi \mathcal{U}_{\geq \max(0,i-d(s))} \psi$.

Etudions la complexité de l'algorithme 1. Les boucles sont indicées par les états de S et par un index allant de 0 à c. Par conséquent, on a affaire un algorithme pseudo-polynomial au sens où il est polynomial si c est décrit en unaire ou si l'algorithme est spécialisé pour des valeurs de c inférieures à une constante prédéfinie. Dans le cas général, on a affaire à un algorithme polynomial vis à vis de la taille du système et en EXPTIME vis à vis de la taille de la formule.

Si on adopte la sémantique continue alors l'algorithme 1 peut être appliqué au système déplié avec durées 0 ou 1. Cependant cette transformation conduit à un algorithme en EXPTIME à la fois vis à vis de la taille de la formule mais aussi vis à vis de la taille du système.

3.3.2 Vérification de formules de PTCTL$[\leq, \geq]$

Dans cette section, nous montrons comment éviter la construction du système déplié lors de la vérification de formules de PTCTL$[\leq, \geq]$ dans le cadre de la sémantique continue. L'idée principale consiste à maintenir un ensemble d'intervalles pour un état s et une sous-formule θ de la formule à vérifier, noté $Sat[s, \theta]$ tel que $(s, i) \models \theta$ ssi $i \in Sat[s, \theta]$.

Supposons que nous désirions calculer $Sat[s, P_{\bowtie a} \varphi \mathcal{U}_{\sim c} \psi]$ avec $\sim \in \{\leq, \geq\}$ sachant que nous connaissons $Sat[s, \varphi]$ et $Sat[s, \psi]$.

Spécification d'intervalles. Nous construisons d'abord un ensemble d'intervalles disjoints, noté $Int(s)$ pour chaque état s défini uniquement par les règles suivantes :

- $\bigcup_{I \in Int(s)} I = \bigcup_{I \in Sat[s,\varphi]} I \cup \bigcup_{I \in Sat[s,\psi]} I$
- Les intervalles sont homogènes par rapport à la satisfaction de φ et ψ. Au sein d'un intervalle, l'une des trois formules $\varphi \wedge \psi$, $\varphi \wedge \neg\psi$ $\neg\varphi \wedge \psi$ est satisfaite par toutes les configurations.
- Si $\max(d(s)-1, 0)$ appartient à $Int(s)$ alors $[\max(d(s)-1, 0), \max(d(s)-1, 0)]$ est un intervalle de $Int(s)$.
- Si 0 appartient à $Int(s)$ alors $[0, 0]$ est un intervalle de $Int(s)$.

En complétant par les intervalles « complémentaires » des intervalles de $Sat[s, \varphi]$ et $Sat[s, \psi]$, puis en ordonnant les extrémités des sommets de tous ces intervalles pour former les intervalles de $Int(s)$, on déduit que le nombre d'intervalles de $Int(s)$ est inférieur ou égal à $2(|Sat[s, \varphi]| + |Sat[s, \psi]|) + 3$.

Spécification d'un système probabiliste sur les intervalles. Les états de ce système sont :

- les paires $(s, [a, b]^-)$, $(s, [a, b]^+)$ avec $[a, b] \in Int(s)$ et $a \neq b$,
- les paires $(s, [a, a])$ avec $[a, a] \in Int(s)$,
- un état puits $\perp$.

La fonction de transition est définie par :

- Soit $conf = (s, [\max(d(s) - 1, 0), \max(d(s) - 1, 0)])$, un état. La durée de séjour dans cet état est $\min(d(s), 1)$. La distribution se répartit ainsi : $next(conf)(s', [0, 0]) = next(s)(s')$ lorsque $(s', [0, 0])$ est un état du système et $next(conf, \perp)$ est la probabilité restante.
- Soit $conf = (s, [a, b]^-)$, un état. Alors la durée de séjour dans $conf$ est égale à $b - a$ et conduit avec probabilité 1 à l'état $(s, [a, b]^+)$.
- Soit $conf = (s, [a, b]^+)$ ou $conf = (s, [b, b])$ (avec $b \neq \max(d(s) - 1, 0)$) un état. S'il y a un état $(s, [b + 1, c]^-)$ ou un état $(s, [b + 1, b + 1])$ alors la durée de séjour dans $conf$ est égale à

1 et conduit avec probabilité 1 à l'état $(s, [b+1, c]^-)$ ou $(s, [b+1, b+1])$. Sinon la durée de séjour est nulle et conduit avec probabilité 1 à $\bot$

– $\bot$ est un états puits de durée de séjour 1 et qui conduit à lui-même avec probabilité 1.

Les états standards sont étiquetés en fonction de leur appartenance à $Sat[s, \varphi]$ et $Sat[s, \psi]$. $\bot$ est étiqueté par $\neg\varphi \wedge \neg\psi$.

Première observation. D'après la construction de ce système, disons $\mathcal{A}'$:

– La probabilité dans $\mathcal{A}'$ d'un chemin issu de $(s, [a, a])$ de satisfaire $\varphi\mathcal{U}_{\sim c}\psi$ est égale la probabilité d'un chemin issu de (s, a) de satisfaire $\varphi\mathcal{U}_{\sim c}\psi$ dans $\mathcal{A}$ (en sémantique continue).

– La probabilité dans $\mathcal{A}'$ d'un chemin issu de $(s, [a, b]^-)$ de satisfaire $\varphi\mathcal{U}_{\sim c}\psi$ est égale la probabilité d'un chemin issu de (s, a) de satisfaire $\varphi\mathcal{U}_{\sim c}\psi$ dans $\mathcal{A}$.

– La probabilité dans $\mathcal{A}'$ d'un chemin issu de $(s, [a, b]^+)$ de satisfaire $\varphi\mathcal{U}_{\sim c}\psi$ est égale la probabilité d'un chemin issu de (s, b) de satisfaire $\varphi\mathcal{U}_{\sim c}\psi$ dans $\mathcal{A}$.

Cette observation est justifiée par le fait que si $\sim$ est $\leq$ alors un chemin fini qui satisfait la formule dans $\mathcal{A}$ peut toujours être arrêté au début du dernier « intervalle » qui recouvre le chemin et si $\sim$ est $\geq$ alors un chemin fini qui satisfait la formule dans $\mathcal{A}$ peut toujours être prolongé jusqu'à la fin du dernier « intervalle » qui recouvre le chemin. Ceci ne modifie pas les calculs puisqu'on se déplace à l'intérieur d'un intervalle avec probabilité 1.

Deuxième observation. A l'intérieur d'un intervalle, les chemins atteignent la borne supérieure de l'intervalle avec probabilité 1. Intéressons-nous à une configuration $(s, b-i)$ avec $b-i \in [a, b[$ et $[a, b] \in Int(s)$. Il y a plusieurs cas à considérer :

– ψ est satisfait dans l'intervalle et $\sim$ est $\leq$ ou $\sim c$ est ≥ 0. Par conséquent, tous les chemins issus d'une configuration de l'intervalle satisfont la formule.

– ψ n'est pas satisfait dans l'intervalle et $\sim$ est $\leq$. Par conséquent, la probabilité qu'un chemin issu de $(s, b-i)$ satisfasse $\varphi\mathcal{U}_{\leq c}\psi$ est égale à la probabilité qu'un chemin issu de (s, b) satisfasse $\varphi\mathcal{U}_{\leq c-i}\psi$ pour $i < c$ et est égale à 0 pour $i \geq c$.

– $\varphi \wedge \psi$ est satisfait dans l'intervalle et $\sim$ est $\geq$. Par conséquent, la probabilité qu'un chemin issu de $(s, b-i)$ satisfasse $\varphi\mathcal{U}_{\geq c}\psi$ est égale à la probabilité qu'un chemin issu de (s, b) satisfasse $\varphi\mathcal{U}_{\geq c-i}\psi$ pour $i < c$ et est égale à 1 pour $i \geq c$.

– $\varphi \wedge \neg\psi$ est satisfait dans l'intervalle et $\sim$ est $\geq$. Par conséquent, la probabilité qu'un chemin issu de $(s, b-i)$ satisfasse $\varphi\mathcal{U}_{\geq c}\psi$ est égale à la probabilité qu'un chemin issu de (s, b) satisfasse $\varphi\mathcal{U}_{\geq c-i}\psi$ pour $i < c$ et est égale à la probabilité qu'un chemin issu de (s, b) satisfasse $\varphi\mathcal{U}_{\geq 0}\psi$ pour $i \geq c$.

– $\neg\varphi \wedge \psi$ est satisfait dans l'intervalle et $\sim$ est $\geq$ avec $c > 0$. Par conséquent, aucun chemin issu d'une configuration de l'intervalle ne satisfait la formule.

Nous pouvons donc déterminer les $Sat[s, P_{\bowtie p}\varphi\mathcal{U}_{\sim c}\psi]$ en temps polynomial en fonction de la taille des $Sat[s, \varphi]$, des $Sat[s, \psi]$ et de c. Cependant la taille des intervalles pourrait croître exponentiellement. En raffinant l'analyse précédente, montrons qu'il n'en est rien.

Considérons d'abord le cas d'une formule $P_{\bowtie p}\varphi\mathcal{U}_{\leq c}\psi$. Pour un état s donné toutes les configurations des intervalles de $Sat[s, \psi]$ donnent lieu à une probabilité 1. On intersecte ensuite les intervalles $Sat[s, \varphi]$ avec le complémentaire de $Sat[s, \psi]$. Considérons les intervalles ainsi obtenus qui précèdent et sont contigus avec un intervalle $Sat[s, \psi]$; tronquons les éventuellement aux c derniers élements pour prolonger (en arrière) un intervalle de $Sat[s, \psi]$ avec encore une probabilité 1. Enfin considérons le dernier intervalle ainsi obtenu à condition qu'il soit au delà du dernier intervalle de $Sat[s, \psi]$ et contienne la dernière configuration de s. A l'intérieur de cet intervalle la probabilité de satisfaire $\varphi\mathcal{U}_{\leq c}\psi$ croît et donc franchit une seule fois le seuil à comparer. Par conséquent, il y a au plus $|Sat[s, \psi]| + 2$ intervalles dans $Sat[\varphi\mathcal{U}_{\leq c}\psi]$.

Considérons maintenant le cas d'une formule $P_{\bowtie p}\varphi\mathcal{U}_{\geq c}\psi$. Soit un intervalle non terminal de $Sat[s, \varphi]$. S'il n'existe pas de configuration qui satisfait ψ et atteignable sans quitter l'intervalle excepté éventuellement pour le dernier état, alors la probabilité de satisfaire la formule est nulle à partir de cet intervalle. Sinon en prenant le plus grand état qui vérifie ses conditions alors l'intervalle se divise (éventuellement) en deux sous-intervalles l'un pour lequel la probabilité de satisfaction est 1, l'autre pour lequel elle est nulle. Soit maintenant l'intervalle terminal de $Sat[s, \varphi]$. S'il ne contient pas la dernière configuration de s alors son cas est identique au cas précédent. Sinon il se

divise toujours en deux sous-intervalles mais sur le deuxième sous intervalle la probabilité décroît et donc franchit une seule fois le seuil à comparer. Par conséquent, il y a au plus $|Sat[s,\varphi]|+2$ intervalles dans $Sat[P_{\bowtie p}\varphi\mathcal{U}_{\geq c}\psi]$.

En majorant grossièrement, on obtient $|Sat[P_{\bowtie p}\varphi\mathcal{U}_{\geq c}\psi]| \leq |Sat[s,\psi]| + |Sat[s,\varphi]| + 2$. Cette dernière inégalité vérifiée aussi pour les autres opérateurs garantit que le nombre d'intervalles par état est proportionnel à la taille de la formule. On retrouve donc la complexité de la sémantique par saut lorsqu'on élimine l'égalité pour l'opérateur $\mathcal{U}_{\sim c}$.

3.3.3 Vérification de formules du fragment qualitatif de PTCTL

Nous allons réduire la vérification du fragment qualitatif de PTCTL à la vérification de TCTL pour les systèmes de transitions à durée (voir [LMS 06]). Aussi nous étudions d'abord ces systèmes.

Définition 51 *Un système de transitions avec durées $\mathcal{A} = (S, \nu, d, next)$ est défini par :*
- *S, l'ensemble fini des états ;*
- *$\nu : S \mapsto 2^{\mathcal{P}}$ définit l'ensemble des propriétés satisfaites par les états ;*
- *$d : S \mapsto \mathbb{N}$ désigne la durée de la visite en un état ;*
- *$next : S \mapsto 2^S$ désigne l'ensemble des successeurs possibles d'un état. On notera $s \to s'$ ssi $s' \in next(s)$.*

Définition 52 *Soit $\mathcal{P}$, un ensemble de propositions atomiques.*
Une formule d'état de TCTL *(relative à $\mathcal{P}$) est définie inductivement par :*
- *E_1 : Si $\phi \in \mathcal{P}$ alors ϕ est une formule d'état de* TCTL *;*
- *E_2 : Si ϕ et ψ sont des formules d'état de* TCTL *alors $\neg\phi$ et $\phi \wedge \psi$ sont des formules de* TCTL *;*
- *E_3 : Si φ est une formule de chemin de* TCTL*, alors $A\varphi$ et $E\varphi$ sont des formules d'état de* TCTL*.*

Une formule de chemin de TCTL *(relative à $\mathcal{P}$) est définie inductivement par :*
- *C : Si φ et θ sont des formules d'état de* TCTL*, d est un entier, $\sim \in \{=, \leq, \geq\}$ alors $\varphi\mathcal{U}_{\sim d}\theta$ et $\mathcal{X}\varphi$ sont des formules de chemin de* TCTL*.*

Etant donnée une exécution infinie σ, on désigne par $\sigma(i)$ la $i$ème configuration de σ et $Time(\sigma, i)$ le temps d'atteinte de cette configuration. La satisfaction présentée ci-dessous est valable à la fois pour la sémantique de saut (les configurations sont les états) et la sémantique continue (les configurations sont des paires états, durée et les propriétés atomiques satisfaites par la configuration sont celles satisfaites par l'état).

Définition 53 *Soit $\mathcal{A}$ un système de transitions avec durées, s une configuration du système et σ une exécution infinie.*
La satisfaction d'une formule d'état ϕ par s est définie inductivement par :
- *Si $\phi \in \mathcal{P}$ alors $\mathcal{A}, s \models \phi$ ssi ϕ étiquette s ;*
- *Si $\phi \equiv \neg\psi$ alors $\mathcal{A}, s \models \phi$ ssi $\mathcal{A}, s \not\models \psi$;*
- *$\phi \equiv \psi_1 \wedge \psi_2$ alors $\mathcal{A}, s \models \phi$ ssi $\mathcal{A}, s \models \psi_1$ et $\mathcal{A}, s \models \psi_2$;*
- *Si $\phi \equiv A\varphi$ alors $\mathcal{A}, s \models \phi$ ssi pour tout séquence σ issue de s on a $\sigma \models \varphi$. Si $\phi \equiv E\varphi$ alors $\mathcal{A}, s \models \phi$ ssi pour il existe une séquence σ issue de s telle que $\sigma \models \varphi$.*

La satisfaction d'une formule de chemin φ par σ est définie inductivement par :
- *Si $\varphi \equiv \mathcal{X}\theta$ alors $\sigma \models \varphi$ ssi $\sigma(1) \models \theta$;*
- *Si $\varphi \equiv \theta_1\mathcal{U}_{\sim d}\theta_2$ alors $\sigma \models \varphi$ ssi $\exists i \in \mathbb{N}\ Time(\sigma, i) \sim d$, $\sigma(i) \models \theta_2$ et $\forall i' < i\ \sigma(i') \models \theta_1$.*

Vérification de formules TCTL$[\leq, \geq]$ avec sémantique de saut

Nous étudions d'abord la vérification des formules de TCTL$[\leq, \geq]$ dans le cadre de la sémantique par sauts. A l'instar de CTL, l'algorithme effectue une évaluation « bottom-up » des sous-formules

d'états et substitue aux sous-formules de propositions d'état. Nous proposons des algorithmes pour vérifier $Ep\mathcal{U}_{\leq c}q, Ep\mathcal{U}_{\geq c}q, Ap\mathcal{U}_{\leq c}q, Ap\mathcal{U}_{\geq c}q$ où p, q sont des propriétés atomiques.

Cas $Ep\mathcal{U}_{\leq c}q$. On construit le graphe restreint aux états qui satisfont $p \vee q$. Puis pour chaque état s, on calcule le plus court chemin de s à un état satisfaisant q. Ceci se fait en temps polynomial en fonction de la taille du graphe (avec par exemple l'algorithme de Dijkstra).

Cas $Ep\mathcal{U}_{\geq c}q$. On commence par se retreindre aux sommets vérifiant $p \wedge Ep\mathcal{U}q$ (calculables en temps polynomial par l'algorithme de vérification de CTL) et dans ce sous-graphe, on étiquette les sommets des c.f.c. contenant un arc de durée non nulle par une nouvelle proposition atomique, disons r. Ceci se fait en temps polynomial après application de l'algorithme de Tarjan. On considère le graphe acyclique des c.f.c. étiquetées par q ssi l'un des sommets est étiqueté par q et on complète ce graphe par les états satisfaisant $\neg p \wedge q$ et les arcs entrants dans ces états depuis les états du graphe des c.f.c. Ceci nous donne encore un graphe acyclique.

Dans ce graphe, il existe un chemin σ issu de s qui satisfait $p\mathcal{U}_{\geq c}q$ ssi (1) il existe un chemin issu de s qui satisfait $p\mathcal{U}r$ ou (2) il existe un chemin issu de s qui satisfait $p\mathcal{U}_{\geq c}q$. Le premier cas se traite avec l'algorithme pour CTL. Le deuxième cas se traite par un tri topologique des sommets puis par un algorithme standard de programmation dynamique laissé aux bons soins du lecteur.

Cas $Ap\mathcal{U}_{\leq c}q$. On observe d'abord que $Ap\mathcal{U}_{\leq c}q \equiv A\mathcal{F}_{\leq c}q \wedge \neg E\neg q\mathcal{U}(\neg p \wedge \neg q)$. Il nous reste donc à vérifier $A\mathcal{F}_{\leq c}q$. Dans le graphe restreint aux sommets vérifiant $\neg q$, on étiquette par r, les sommets des c.f.c. comportant au moins un arc (et donc un circuit). Puis on applique l'équivalence $A\mathcal{F}_{\leq c}q \equiv \neg E\neg q\mathcal{U}_{>c}\mathbf{true} \wedge \neg E\neg q\mathcal{U}r$ pour en déduire un algorithme en temps polynomial.

Cas $Ap\mathcal{U}_{\geq c}q$. Le sous-cas $c = 0$ est une formule de CTL. Donc on suppose que $c > 0$. On observe alors que $Ap\mathcal{U}_{\geq c}q \equiv A\mathcal{G}_{<c}(p \wedge Ap\mathcal{U}_{>0}q)$. Sachant que $A\mathcal{G}_{<c}\varphi \equiv \neg E\mathcal{F}_{<c}\neg\varphi$, il ne reste plus qu'à traiter l'opérateur $A\varphi\mathcal{U}_{>0}\psi$. Un algorithme pour cet opérateur consiste à dupliquer chaque état s en deux états s_0 et s_1. Une transition de durée nulle de s à s' donne lieu à une transition de s_0 à s'_0 et à une transition de s_1 à s'_1. Une transition de durée non nulle de s à s' donne lieu à une transition de s_0 à s'_1 et à une transition de s_1 à s'_1. On étiquette les états s_1 avec une propriété r et on applique l'algorithme de CTL pour vérifier $A\varphi\mathcal{U}(\psi \wedge r)$. Un état s est étiqueté par $A\varphi\mathcal{U}_{>0}\psi$ ssi l'état s_0 est étiqueté par $A\varphi\mathcal{U}(\psi \wedge r)$.

Par conséquent, la vérification de TCTL$[\leq, \geq]$ dans le cadre de la sémantique par sauts se fait en temps polynomial. Puisque TCTL est une extension de CTL et que le problème de la vérification de formules de CTL est PTIME-complet, on conclut que le problème de la vérification de TCTL$[\leq, \geq]$ est PTIME-complet.

Vérification de formules TCTL avec sémantique de saut

La proposition suivante indique qu'il y a peu d'espoir d'obtenir un algorithme en temps polynomial pour TCTL.

Proposition 54 *La vérification de la formule $E\mathcal{F}_{=c}p$ pour la sémantique de saut est un problème NP-difficile.*

Preuve
La variante suivante du problème du sac à dos est NP-complète. Etant donnés n poids $b_1, \ldots, b_n$ et une capacité c existe-t-il un sous-ensemble $I \subseteq \{1, \ldots, n\}$ tel que $\sum_{i \in I} b_i = c$?

La réduction du problème se fait ainsi.
L'ensemble des états est défini par $\{s_0, \ldots, s_n\} \cup \{r_1^-, r_1^+, \ldots, r_n^-, r_n^+\}$. Seul l'état s_n est étiqueté par p. Les transitions sont les suivantes :

- Pour tout $0 \leq i < n$, $s_i \xrightarrow{0} r_{i+1}^-$ et $s_i \xrightarrow{0} r_{i+1}^+$;
- Pour tout $0 < i \leq n$, $r_i^- \xrightarrow{0} s_i$ et $r_i^+ \xrightarrow{b_i} s_i$.

On laisse au lecteur le soin de prouver que $s_0 \models E\mathcal{F}_{=c}p$ ssi le problème du sac à dos a une solution.

c.q.f.d. ◊◊◊

Les deux propositions suivantes sont la clef de la vérification des formules avec test d'égalité.

Proposition 55 *La vérification de la formule $Ep\mathcal{U}_{=c}q$ pour la sémantique de saut est un problème dans NP.*

Preuve
Soit s_0, l'état pour lequel on veut vérifier la formule. On observe d'abord que la méthode qui consiste à deviner un chemin issu de s_0 et à vérifier la formule ne fonctionne pas car la longueur du chemin est supérieure plus à $c|S|$ alors que la taille de la formule est de l'ordre de $\log(c)$.

On procède de manière plus intelligente en devinant un vecteur d'occurrences de transitions $\mathbf{v}$ et un état s_f qui vérifie les conditions suivantes :

- Pour tout état $s \notin \{s_0, s_f\}$, le nombre de transitions entrantes est égal au nombre de transitions sortantes. Si $s_0 = s_f$ alors la propriété est aussi vérifiée pour s_0. Sinon le nombre de transitions sortantes de s_0 est égal au nombre de transitions entrantes plus un et le nombre de transitions sortantes de s_f est égal au nombre de transitions entrantes moins un.
- Le sous-graphe induit par les transitions est connexe.
- La somme des durées des arcs est égale à c.
- L'état s_f vérifie q et tout état qui a un arc sortant vérifie p.

Le deux premières conditions assurent que l'on peut fabriquer un chemin par le théorème d'Euler. Les deux dernières conditions assurent que le chemin vérifie la formule. Puisque les composantes du vecteur sont inférieures ou égales à $c|S|$ la prédiction et sa vérification se font en temps polynomial.

c.q.f.d. ◊◊◊

Proposition 56 *La vérification de la formule $Ap\mathcal{U}_{=c}q$ pour la sémantique de saut est un problème dans coNP.*

Preuve
On observe que $Ap\mathcal{U}_{=c}q \equiv Ap\mathcal{U}_{\geq c}q \wedge \neg E\mathcal{G}_{=c}\neg q$. Il suffit donc de concevoir une procédure dans NP pour $E\mathcal{G}_{=c}p'$. Ceci se fait de manière similaire à la preuve précédente en notant qu'il y a trois cas possibles de chemin : celui qui évite l'instant c et celui qui rencontre l'instant c un nombre fini de fois et celui qui reste indéfiniment à l'instant c.

c.q.f.d. ◊◊◊

En appliquant la méthode « bottom-up », on obtient un algorithme dans $\Delta_2^p = P^{NP}$. Rappelons que P^{NP} est la classe de complexité des problèmes qui se résolvent par un algorithme en temps polynomial avec des appels à un oracle NP. En fait, le problème de vérification de TCTL pour la sémantique de saut est Δ_2^p-complet.

Vérification de formules TCTL[$\leq, \geq$] avec sémantique continue

On applique la technique des intervalles de satisfaction déjà vue précédemment. Nous allons simplement l'illustrer pour une formule $E\varphi\mathcal{U}_{\leq c}\psi$ sachant que nous connaissons $Sat[s, \varphi]$ et $Sat[s, \psi]$. Pour chaque configuration, nous calculons (symboliquement) la plus courte durée d'un chemin (s'il en existe) issu de la configuration satisfaisant $\varphi\mathcal{U}\psi$ (que nous comparerons à c).

Spécification d'intervalles. Nous construisons d'abord un ensemble d'intervalles disjoints, noté $Int(s)$ pour chaque état s défini uniquement par les règles suivantes :

- $\bigcup_{I \in Int(s)} I = \bigcup_{I \in Sat[s,\varphi]} I \cup \bigcup_{I \in Sat[s,\psi]} I$
- Les intervalles sont homogènes par rapport à la satisfaction de φ et ψ. Au sein d'un intervalle, l'une des trois formules $\varphi \wedge \psi$, $\varphi \wedge \neg\psi$ $\neg\varphi \wedge \psi$ est satisfaite par toutes les configurations.
- Si $\max(d(s)-1, 0)$ appartient à $Int(s)$ alors $[\max(d(s)-1, 0), \max(d(s)-1, 0)]$ est un intervalle de $Int(s)$.
- Si 0 appartient à $Int(s)$ alors $[0, 0]$ est un intervalle de $Int(s)$.

Comme vu précédemment, le nombre d'intervalles de $Int(s)$ est inférieur ou égal à $2(|Sat[s,\varphi]| + |Sat[s,\psi]|) + 3$.

Spécification d'un système de transitions avec durées. Les états de ce système sont :
- les paires $(s, [a,b]^-)$, $(s, [a,b]^+)$ avec $[a,b] \in Int(s)$ et $a \neq b$,
- les paires $(s, [a,a])$ avec $[a,a] \in Int(s)$.

La fonction de transition est définie par :
- Soit $conf = (s, [\max(d(s)-1, 0), \max(d(s)-1, 0)])$, un état. La durée de séjour dans cet état est $\min(d(s), 1)$. Alors $next(conf) = \{(s', [0,0]) \mid s' \in next(s)$ et $(s', [0,0])$ est un état$\}$.
- Soit $conf = (s, [a,b]^-)$, un état. Alors la durée de séjour dans $conf$ est égale à $b - a$ et $next(conf) = \{(s, [a,b]^+)\}$.
- Soit $conf = (s, [a,b]^+)$ ou $conf = (s, [b,b])$ (avec $b \neq \max(d(s)-1, 0)$) un état. S'il y a un état $(s, [b+1, c]^-)$ alors la durée de séjour dans $conf$ est égale à 1 et $next(conf) = \{(s, [b+1, c]^-)\}$. Sinon la durée de séjour est nulle et $next(conf) = \emptyset$.

Les états sont étiquetés en fonction de leur appartenance à $Sat[s,\varphi]$ et $Sat[s,\psi]$.

Première observation. D'après la construction de ce système disons $\mathcal{A}'$:
- La durée d'un (éventuel) plus court chemin témoin de $\varphi \mathcal{U}_{\leq c} \psi$ issu de $(s, [a,a])$ est égale à la durée d'un (éventuel) plus court chemin témoin issu de (s,a) dans $\mathcal{A}$ (en sémantique continue).
- La durée d'un (éventuel) plus court chemin témoin issu de $(s, [a,b]^-)$ est égale à la durée d'un (éventuel) plus court chemin témoin issu de (s,a) dans $\mathcal{A}$.
- La durée d'un (éventuel) plus court chemin témoin issu de $(s, [a,b]^+)$ est égale à la durée d'un (éventuel) plus court chemin témoin issu de (s,b) dans $\mathcal{A}$.

Cette observation est justifiée par le fait qu'un chemin fini qui satisfait la formule dans $\mathcal{A}$ peut toujours être arrêté au début du dernier « intervalle » qui recouvre le chemin.

Deuxième observation. Intéressons-nous à une configuration $b - i \in [a,b[$ avec $[a,b] \in Int(s)$. Il y a plusieurs cas à considérer :
- ψ est satisfait dans l'intervalle. Par conséquent, la durée à calculer est nulle.
- ψ n'est pas satisfait dans l'intervalle. Par conséquent, la durée à calculer est égale à la durée associée à (s,b) augmentée de i. L'intervalle est donc éventuellement scindé en deux $[a,\alpha]$ et $[\alpha+1, b]$, le calcul de α d'effectuant en temps polynomial en fonction de $\log(c)$.

Nous pouvons donc déterminer les $Sat[s, \varphi \mathcal{U}_{\sim c} \psi]$ en temps polynomial en fonction de la taille des $Sat[s,\varphi]$, des $Sat[s,\psi]$ et de $\log(c)$. Cependant la taille des intervalles pourrait croître exponentiellement. En raffinant l'analyse précédente, montrons qu'il n'en est rien.

Pour un état s donné toutes les configurations des intervalles de $Sat[s,\psi]$ satisfont la formule. On intersecte ensuite les intervalles $Sat[s,\varphi]$ avec le complémentaire de $Sat[s,\psi]$. Considérons les intervalles ainsi obtenus qui précèdent et sont contigus avec un intervalle $Sat[s,\psi]$; tronquons les éventuellement aux c derniers élements pour prolonger (en arrière) un intervalle de $Sat[s,\psi]$ Enfin considérons le dernier intervalle ainsi obtenu à condition qu'il soit au delà du dernier intervalle de $Sat[s,\psi]$ et contienne la dernière configuration de s. A l'intérieur de cet intervalle la durée du plus court chemin témoin décroît et donc franchit une seule fois le seuil à comparer. Par conséquent, il y a au plus $|Sat[s,\psi]| + 2$ intervalles dans $Sat[\varphi \mathcal{U}_{\leq c} \psi]$.

En conclusion, nous avons obtenu un algorithme en PTIME.

Vérification de formules TCTL avec sémantique continue

L'évaluation la plus naïve consiste à construire le graphe des configurations, puis d'appliquer la technique « bottom-up » sur le graphe des configurations en étiquetant les sous-formules. Les algorithmes associés aux opérateurs s'exécutent tous en temps polynomial par rapport à la taille du graphe et exponentiel par rapport à la taille de la formule (dans le cas d'un test d'égalité sur la durée). On obtient donc un algorithme dans EXPTIME.

Cependant cet algorithme peut être optimisé comme suit. On démontre d'abord que les A peuvent être éliminés dans la formule (en utilisant aussi l'opérateur modal $\mathcal{G}$). Puis on définit une fonction $Sat((s,i), \varphi)$ qui renvoie la valeur de vérité de φ pour la configuration (s,i)). Cette

fonction appelle une fonction spécialisée en fonction de l'opérateur le plus externe de φ. Décrivons le fonctionnement de l'une de ces fonctions $Sat_{E\mathcal{U}_=}((s,i),\theta,\psi,c)$ qui renvoie la valeur de vérité de $E\theta\mathcal{U}_{=c}\psi$ pour la configuration (s,i)).

Cette fonction cherche un chemin du durée c ainsi :

- Supposons $c=0$. Elle appelle $Sat((s,i),\psi)$ Si cet appel renvoie vrai alors elle renvoie vrai. Sinon elle appelle $Sat((s,i),\theta)$. Si cet appel renvoie faux alors elle renvoie faux. Sinon si $i=0$ et $d(s)=0$ elle explore les configurations accessibles depuis (s,i) par un echemin de durée 0. Ceci se fait en temps linéaire par un parcours du système original. Pour chaque configuration trouvée, appelle $Sat((s,i),\psi)$. Si l'un des appels renvoie vrai, la fonction renvoie vrai elle renvoie vrai. Sinon elle renvoie faux.
- Supposons $c=1$. Elle appelle $Sat((s,i),\theta)$. Si cet appel renvoie faux alors elle renvoie faux. Sinon elle explore les configurations accessibles depuis (s,i) par un chemin de durée 1. Ceci se fait en temps linéaire par un parcours du système original. Pour chaque configuration trouvée, appelle $Sat((s,i),\psi)$. Si l'un des appels renvoie vrai, la fonction renvoie vrai elle renvoie vrai. Sinon elle renvoie faux.
- Supposons $c>1$. La fonction effectue une boucle sur l'ensemble des configurations du système. Soit (s',i') la configuration courante. La procédure cherche un chemin qui passe en son « milieu » par (s',i'). Elle appelle donc une procédure spécialisée $Reach((s,i),(s',i'),\theta,\lfloor c/2\rfloor)$ qui cherche (avec la même technique dichotomique) un chemin de longueur $\lfloor c/2\rfloor$ de (s,i) à (s',i') tels que tous les états satisfont θ.
  Si l'appel renvoie vrai alors elle appelle $Sat_{E\mathcal{U}_=}((s',i'),\theta,\psi,\lceil c/2\rceil)$ et renvoie vrai si ce deuxième appel renvoie aussi vrai. Dans le cas contraire, elle passe à la configuration suivante. Si elle a examiné sans succès toutes les configurations alors elle renvoie faux.

Chaque appel occupe un espace polynomial et il y a au plus $O(\log(c))$ appels dans la pile. On obtient ainsi un algorithme dans PSPACE (le lecteur attentif aura reconnu une généralisation de la technique de Savitch). Cet algorithme est optimal car on démontre que le problème est PSPACE-complet.

Réduction du fragment qualitatif de PTCTL à TCTL

Dans la section 2.2, nous avons déjà discuté des ressemblances et des différences entre la vérification du fragment qualitatif de PCTL pour une DTMC et la vérification de CTL sur le graphe de la DTMC. Cette comparaison reste valable dans le cadre des systèmes avec durées. Nous les synthétisons ici et nous les étendons avec les durées. Soit $\mathcal{A}$, un système probabiliste avec durées, soit $\mathcal{A}'$ le système de transitions avec durée obtenu par $s'\in next(s)$ ssi $\nu(s)(s')>0$. Alors :

- $P_{=1}\mathcal{X}\psi$ est équivalent à $A\mathcal{X}\psi$, $P_{>0}\mathcal{X}\psi$ est équivalent à $E\mathcal{X}\psi$ et $P_{>0}\psi\mathcal{U}_{\sim c}\chi$ est équivalent à $E\psi\mathcal{U}_{\sim c}\chi$.
- $P_{=1}\psi\mathcal{U}_{\sim c}\chi$ n'est pas nécessairement équivalent à $A\psi\mathcal{U}_{\ c}\chi$ mais dans le cas d'un « until » borné ($\sim\in\{\leq,=\}$), l'équivalence est justifiée car le nombre de chemins issus d'un sommet de durée inférieure ou égale à c est fini. Il reste donc le cas $P_{=1}\psi\mathcal{U}_{\geq c}\chi$. On affecte d'abord aux états une propriété atomique r équivalente à $P_{=1}\psi\mathcal{U}\chi$ calculée (en temps polynomial) comme dans une DTMC. La formule $P_{=1}\psi\mathcal{U}_{\geq c}\chi$ est équivalente à ce que tous les états des chemins de durée strictement inférieure à c (soit un nombre fini de chemins) vérifient ψ et que tous les états prolongeant immédiatement ces chemins vérifient $P_{=1}\psi\mathcal{U}\chi\equiv r$. Par conséquent la formule implique $A\psi\mathcal{U}_{\geq c}r$. D'autre part soit un état s qui vérifie $A\psi\mathcal{U}_{\geq c}r$ et tel qu'il existe un chemin issu de cet état dont le premier état atteint après au moins c unités de temps disons s' ne satisfait pas r. Alors de s', il existe un chemin fini tel que :
  1. le dernier état satisfait $\neg\psi$ et aucun état ne satisfait χ ce qui entraîne qu'il existe un chemin issu de s qui satisfait pas $\psi\mathcal{U}_{\geq c}r$ car aucun état de ce sous-chemin ne satisfait r ; d'où une contradiction.
  2. aucun état ne satisfait χ et le dernier état appartient à une c.f.c. terminale qui ne satisfait jamais χ. On peut donc étendre ce sous-chemin de manière arbitraire par un

sous-chemin infini dans cette c.f.c. Ce qui entraîne qu'il existe un chemin issu de s qui satisfait pas $\psi \mathcal{U}_{\geq c} r$ car aucun état de ce sous-chemin infini ne satisfait r ; d'où une contradiction.

Par conséquent la formule $P_{=1}\psi \mathcal{U}_{\geq c}\chi$ est équivalente à la formule $A\psi \mathcal{U}_{\geq c} r$.

A l'aide de cette transformation, les algorithmes pour TCTL s'appliquent avec les mêmes complexités au fragment qualitatif de PTCTL.

3.4 Systèmes probabilistes à événements temporisés [ACD 91]

On se fixe un ensemble de propositions atomiques, noté $\mathcal{P}$.

Définition 57 *Un système probabiliste à événements temporisés $\mathcal{A} = (S, \nu, \mathcal{E}, f, E, next)$ est défini par :*

- *S, l'ensemble fini des états ;*
- *$\nu : S \mapsto 2^{\mathcal{P}}$ définit l'ensemble des propriétés satisfaites par les états ;*
- *$\mathcal{E}$ désigne l'ensemble des événements du système. Pour tout $e \in \mathcal{E}$, $f(e)$ est une distribution dont le support fini est un intervalle $[l_e, u_e]$ vérifiant :*
  1. *l_e, u_e sont des entiers avec $u_e > 0$.*
  2. *Si $l_e < u_e$ alors f_e est définie par une fonction de densité non nulle sur tout l'intervalle $[l_e, u_e]$. On dit que e est un événement* de délai variable.
  3. *Si $l_e = u_e$ alors f_e est la distribution de Dirac en u_e. On dit que e est un événement* de délai fixe.
- *$E : S \mapsto 2^{\mathcal{E}} \setminus \{\emptyset\}$ associe à chaque état, l'ensemble des événements franchissables ;*
- *$next : S \times 2^{\mathcal{E}} \setminus \{\emptyset\} \times S \mapsto [0, 1]$ est une fonction définie pour les triplets (s, α, s') t.q. $\alpha \subseteq E(s)$ et t.q. $next(s, \alpha, -)$ soit une distribution de probabilité, i.e. $\sum_{s' \in S} next(s, \alpha, s') = 1$.*

Nous expliquons la sémantique du système à l'aide de l'approche de la section 1.1. Initialement ou après l'occurrence d'un événement, le système est dans une configuration (s, c) avec $s \in S$ et c une fonction qui associe à tout événement $e \in E(s)$, un délai $c(e) \leq u_e$. Un événement e est dit à délai minimal si $\forall e' \in E(s)\ c(e) \leq c(e')$. On note $min(c)$, l'ensemble des événements à délai minimal et on note le délai minimal $tmin(c) = \min(c(e) \mid e \in E(s))$.

L'occurrence du prochain « événément » du système à événements discrets a lieu après $tmin(c)$ unités de temps. Il correspond à l'occurrence simultanée des événements de $\min(c)$.

La nouvelle configuration (s', c') est obtenue par la suite d'actions suivante :

1. On effectue un tirage selon la distribution $next(s, min(c), -)$. s' est le résultat de ce tirage.
2. Si $e \in E(s')$ est un événement tel que $e \in E(s) \setminus min(c)$, alors $c'(e) = c(e) - tmin(c)$.
3. Si $e \in E(s')$ est un événement tel que soit $e \notin E(s)$ soit $e \in min(c)$, alors $c'(e)$ est obtenu par un tirage aléatoire selon la distribution f_e.

Autrement dit, pour un événement toujours possible et non apparu son délai est décrémenté du temps écoulé et pour un événement à nouveau possible son délai est tiré selon la distribution de l'événement.

Dans toute exécution infinie (au moins) un événement apparaît une infinité de fois, disons e. Notons $0 < p$ la probabilité que le délai de e soit supérieur ou égal à $1/2$. Soit k un entier quelconque fixé. Pour qu'une suite de n occurrences de e ait lieu en un temps inférieur ou égal à $k/2$, il faut qu'au moins $n - k$ occurrences parmi les n aient une délai inférieur ou égal à $1/2$, soit une probabilité majorée par : $\binom{n}{n-k}(1-p)^{n-k}$, quantité qui tend vers 0 quand n tend vers l'infini. Par conséquent, avec probabilité 1 une exécution infinie du système est non Zénon.

Dans la suite du chapitre, on désignera plus simplement ces systèmes comme des systèmes probabilistes.

3.5 Logiques temporelles pour les systèmes probabilistes à événements temporisés

Nous développerons une méthode de model checking pour PCTL (sans l'opérateur $\mathcal{X}$) mais aussi pour une logique étendue adaptée aux systèmes temps-réels. Aussi nous introduisons maintenant une version « probabiliste » de la logique TCTL [ACD 93] que nous désignerons sous le nom de PTCTL. La syntaxe de cette logique est définie inductivement à l'aide de formules d'état et de chemin. Par rapport aux précédentes versions de PTCTL cette logique ne dispose pas de l'opérateur $\mathcal{X}$. Cependant son introduction ne soulève pas de problèmes particuliers.

Définition 58 *Soit $\mathcal{P}$, un ensemble de propositions atomiques.*
Une formule d'état de PTCTL *(relative à $\mathcal{P}$) est définie inductivement par :*
E_1 : Si $\phi \in \mathcal{P}$ alors ϕ est une formule d'état de PTCTL *;*
E_2 : Si ϕ et ψ sont des formules d'état de PTCTL *alors $\neg\phi$ et $\phi \wedge \psi$ sont des formules de* PTCTL *;*
E_3 : Si φ est une formule de chemin de PTCTL*, $a \in [0,1]$ est un rationnel, $\bowtie \in \{=, \neq, <, \leq, >, \geq\}$ alors $P_{\bowtie a}\varphi$ est une formule d'état de* PTCTL*.*
Une formule de chemin de PTCTL *(relative à $\mathcal{P}$) est définie inductivement par :*
C : Si φ et θ sont des formules d'état de PTCTL*, d est un entier, $\sim \in \{=, <, \leq, >, \geq\}$ alors $\varphi \mathcal{U}_{\sim d} \theta$ est une formule de chemin de* PTCTL*.*

Etant donnée une exécution infinie σ, on désigne par $\sigma(t)$ la configuration atteinte à l'instant t par σ.

Définition 59 *Soit $\mathcal{A}$ un système probabiliste, (s,c) une configuration du système et σ une exécution infinie.*
La satisfaction d'une formule d'état ϕ par (s,c) est définie inductivement par :
- *Si $\phi \in \mathcal{P}$ alors $\mathcal{A},(s,c) \models \phi$ ssi ϕ étiquette s ;*
- *Si $\phi \equiv \neg\psi$ alors $\mathcal{A},(s,c) \models \phi$ ssi $\mathcal{A},(s,c) \not\models \psi$;*
- *$\phi \equiv \psi_1 \wedge \psi_2$ alors $\mathcal{A},(s,c) \models \phi$ ssi $\mathcal{A},(s,c) \models \psi_1$ et $\mathcal{A},(s,c) \models \psi_2$;*
- *Si $\phi \equiv P_{\bowtie a}\varphi$ alors $\mathcal{A},(s,c) \models \phi$ ssi $\Pr(\{\sigma \models \varphi\} \mid \sigma$ démarre en $(s,c)) \bowtie a$.*

La satisfaction d'une formule de chemin φ par σ est définie inductivement par :
$$\text{Si } \varphi \equiv \theta_1 \mathcal{U}_{\sim d} \theta_2 \text{ alors } \sigma \models \varphi \text{ ssi } \exists t \sim d\ \sigma(t) \models \theta_2 \text{ et } \forall t' < t\ \sigma(t') \models \theta_1 \quad .$$

3.6 Algorithme de vérification pour systèmes probabilistes avec événements temporisés

Nous ne considérons dans cette section que les fragments qualitatifs de PCTL et de PTCTL, c'est à dire ceux tels que les seuils de probabilité apparaissant dans les formules soient 0 ou 1. Afin d'alléger les notations A sera une abréviation de $P_{\geq 1}$ et E sera une abréviation de $P_{>0}$.

La première étape de l'algorithme consiste en une réécriture de l'opérateur $A\mathcal{U}_{\sim d}$ afin de ne plus avoir que des opérations de branchement E (i.e. avec probabilité non nulle). On introduit donc trois opérateurs de chemin :
- $\mathcal{G}_{\sim d}\phi$ dont la sémantique est définie par :
$$\sigma \models \mathcal{G}_{\sim d}\phi \text{ ssi } \forall t \sim d\ \sigma(t) \models \phi$$
- $\mathcal{F}_{\sim d}\phi$, l'abréviation de $\mathbf{true}\ \mathcal{U}_{\sim d}\phi$ dont la sémantique est définie par :
$$\sigma \models \mathcal{F}_{\sim d}\phi \text{ ssi } \exists t \sim d\ \sigma(t) \models \phi$$
- $\mathcal{U}^{\circ}_{\sim d}\phi$ dont la sémantique est définie par :
$$\sigma \models \theta_1 \mathcal{U}^{\circ}_{\sim d} \theta_2 \text{ ssi } \exists t \sim d\ \sigma(t) \models \theta_2 \text{ et } \forall 0 < t' < t\ \sigma(t') \models \theta_1$$
(Notez que la contrainte sur θ_1 exclut l'instant 0).

Avec ces définitions on observe que :
- $A\varphi\ \mathcal{U}_{\sim d}\ \psi \equiv \neg\big((E\mathcal{G}_{\sim d}\ \neg\psi) \vee E\neg\psi\ \mathcal{U}(\neg\varphi \wedge \neg\psi)\big)$ lorsque $\sim \in \{<, \leq\}$

– $A\varphi\ \mathcal{U}_{=d}\ \psi \equiv \neg\big((E\mathcal{G}_{=d}\ \neg\psi) \vee (E\mathcal{F}_{<d}\ \neg\varphi)\big)$
– $A\varphi\ \mathcal{U}_{\geq d}\ \psi \equiv \neg\big((E\mathcal{G}_{\geq d}\ \neg\psi) \vee (E\mathcal{F}_{<d}\ \neg\varphi) \vee E\mathcal{G}_{=d}(E\neg\psi\ \mathcal{U}\neg(\varphi \wedge \neg\psi))\big)$
– $A\varphi\ \mathcal{U}_{>d}\ \psi \equiv \neg\big((E\mathcal{G}_{>d}\ \neg\psi) \vee (E\mathcal{F}_{\leq d}\ \neg\varphi) \vee E\mathcal{G}_{=d}(E\neg\psi\ \mathcal{U}^{\circ}_{>0}\neg(\varphi \wedge \neg\psi))\big)$

Par conséquent, l'algorithme de model checking n'a besoin de traiter que les opérateurs $E\mathcal{G}_{\sim d}$, $E\mathcal{U}_{\sim d}$ et $E\mathcal{U}^{\circ}_{\sim d}$.

L'algorithme construit un graphe de classes comme dans le cas des automates temporisés. Cependant le processus stochastique associé à cette abstraction n'est plus markovien car les probabilités d'évolution à partir d'une classe dépendent des configurations au sein d'une même classe. De manière plus formelle, deux configurations (s, c) et (s, c') sont équivalentes (et appartiennent à la même classe) ssi :

1. $\forall e \in E(s)\ \lfloor c(e) \rfloor = \lfloor c(e') \rfloor$
2. On note avec $frac(x) = x - \lfloor x \rfloor$. Alors :
   $\forall e, e' \in E(s)\ frac(c(e)) \geq frac(c(e')) \Leftrightarrow frac(c'(e)) \geq frac(c'(e'))$
   et $frac(c(e)) = 0 \Leftrightarrow frac(c'(e)) = 0$

Le nombre de classes est fini mais exponentiel en fonction de la taille du système. Une classe est dite *transitoire* si l'une des horloges d'un événement est entière. Le passage d'un temps aussi petit qu'il soit au sein d'une classe transitoire fait changer la configuration de classe. Lorsque la classe n'est pas transitoire, le processus change de classe après $tminf(c) = \min(frac(c(e)) \mid e \in E(s))$ unité de temps. On note $minf(c) = \{e \in E(s) \mid frac(c(e)) = tminf(c)\}$.

Il y a dans ce graphe deux types de transition :

– Les transitions de passage de temps. Elles sont possibles lorsque les horloges de $min(c)$ ont une valeur supérieure ou égale à 1 ou lorsqu'elles n'appartiennent pas à $minf(c)$. Dans ce cas :
  1. Si la classe est transitoire on « laisse s'écouler » une petite durée (inférieure à la plus petite partie fractionnaire non nulle ou à 1 s'il n'y en a pas) ce qui conduit à une classe non transitoire. On observe qu'a contrario du graphe des classes les valeurs des délais décroissent.
  2. Si la classe n'est pas transitoire on « laisse s'écouler » le délai $tminf(c)$ ce qui conduit à une classe transitoire.
– Les transitions d'événements. Elles sont possibles lorsque les horloges de $min(c)$ ont une valeur strictement inférieure à 1 et qu'elles appartiennent à $minf(c)$. Dans ce cas :
  1. Pour chaque s' tel que $next(s, min(c), s') > 0$ on crée des arcs vers différentes classes indicées par s' décrites par les points suivants.
  2. Les parties fractionnaires des délais des événements toujours franchissables et de partie fractionnaire différente de celle de $min(c)$ dans la nouvelle classe sont dans la même relation d'ordre (incluant la comparaison à 0) et les parties entières sont inchangées. Les évenements de même partie fractionnaire que celle de $min(c)$ ont maintenant une partie fractionnaire nulle et une partie entière décrémentée d'une unité.
  3. Pour un événement e à délai variable à nouveau franchissable, on choisit une partie entière comprise entre l_e et $u_e - 1$. La partie fractionnaire du nouvel événement est « unique » et non nulle. Elle peut être placée n'importe où par rapport aux autres parties fractionnaires.
  4. Pour un événement e à délai fixe à nouveau franchissable, on choisit $c'(e) = u_e$.

L'état initial (que nous notons s_0) a des arcs vers des classes indicées par s_0 correspondant aux tirages possibles des $e \in E(s_0)$.

A une exécution σ, on associe le parcours correspondant dans le graphe des classes $\gamma_0(\sigma), \gamma_1(\sigma), \ldots$ où les $\gamma_i(\sigma)$ sont les classes successivement visitées par σ.

Notre objectif est de réduire le problème du model checking à un algorithme d'analyse du graphe des classes dans le cas de PCTL (ou d'un graphe des classes étendu dans le cas de PTCTL, voir plus loin).

Observation. Le point 1 des transitions d'événement est problématique car la façon dont la probabilités de transition $next(s, min(c), s')$ se répartit entre les différentes classes indicées par s' dépend de la configuration au sein de la classe courante. Cependant en raison des hypothèses sur les distributions associées aux événements, nous pouvons établir le lemme suivant.

Lemme 60 *Soient $\gamma_0, \gamma_1, \ldots, \gamma_n$ une suite de classes et $(s, c) \in \gamma_0$ une configuration. Notons p la probabilité pour que les $n+1$ premières classes visitées par l'exécution issue de (s, c) soient $\gamma_0, \gamma_1, \ldots, \gamma_n$. Alors :*

$$p > 0 \text{ ssi } \gamma_0, \gamma_1, \ldots, \gamma_n \text{ est un chemin dans le graphe des classes.}$$

Preuve
Cette preuve ne présente pas de difficultés. Les transitions de temps sont déterministes et par conséquent de γ_i on passe à γ_{i+1} avec probabilité 1 quelque soit la configuration de γ_i si $\gamma_i \rightarrow \gamma_{i+1}$ est un passage de temps. Notons qu'un passage de temps est exclusif d'une transition d'événements.

Quant aux transitions d'événements, tous les arcs qui sont créés correspondent au choix d'une valeur dans un intervalle et donc ont une probabilité non nulle d'être choisis. Les choix éliminés correspondent à une valeur ponctuelle pour une variable aléatoire définie par une densité. Ils ont donc une probabilité nulle d'occurrence.

c.q.f.d. $\Diamond\Diamond\Diamond$

Ce lemme nous permet de décider toutes les propriétés du fragment qualitatif de PCTL qui se vérifient par l'existence d'un préfixe fini particulier de l'exécution comme la formule $Ep\mathcal{U}q$. L'algorithme consiste à rechercher un tel chemin fini dans le graphe des classes.

Par contre la vérification d'une formule telle que $E\mathcal{G}p$ nécessite une correspondance plus forte que celle établie par le lemme précédent.

Lemme 61 *Soit σ une exécution aléatoire démarrant en (s, c).* Presque sûrement *(i.e. avec probabilité 1) le parcours du graphe des classes $\gamma_0(\sigma), \gamma_1(\sigma), \ldots$ termine dans une c.f.c terminale et visite une infinité de fois toutes les classes de cette c.f.c.*

Preuve

Nous établissons d'abord deux résultats intermédiaires.

Résultat 1. On dit qu'une configuration est δ-séparée si les parties fractionnaires non nulles des délais sont distantes d'au moins δ et aussi distantes d'au moins δ des valeurs 0 et 1. Posons $p_{\delta,i} > 0$ la probabilité minimale pour tout intervalle $I \subseteq [0, 1]$ de longueur $\delta/(3^i)$ et toute distribution de délai variable du modèle que la partie fractionnaire d'un nouveau délai appartienne à I. Posons p_c la probabilité minimale non nulle d'un choix d'état du modèle. Soient Z, Z' deux classes reliées par une transition d'événements. Alors (par récurrence sur i) partant de (s, c) une configuration δ-séparée appartenant à Z avec probabilité au moins $p_c p_{\delta,|\mathcal{E}|}$ on atteint une configuration de Z' et $\delta/(3^{|\mathcal{E}|})$ séparée. Le pas de récurrence consiste à diviser l'intervalle où doit atterrir la partie fractionnaire en trois sous-intervalles de même longueur et à imposer que le délai appartienne à l'intervalle médian.

En itérant le raisonnement précédent, pour tout chemin de longueur l et toute configuration δ-séparée du premier sommet du chemin, il existe une valeur $preach_{\delta,l} > 0$ telle que la probabilité de parcourir ce chemin soit au moins égale à $preach_{\delta,l} > 0$.

Résultat 2. Posons $n = 3|\mathcal{E}|$ et divisons l'intervalle $[0, 1]$ en n intervalles consécutifs de longueur n. Etant donnée une configuration, lorsqu'un délai d'un événement à délai variable est choisi, il existe un intervalle I_k $(1 < k < n)$ tel qu'aucune partie fractionnaire des autres délais ne se situe dans les intervalles I_{k-1}, I_k, I_{k+1} et ceci par un argument de comptage élémentaire. Posons $p_m > 0$ la probabilité minimale pour tout I_k et toute distribution de délai du modèle que la partie

fractionnaire du nouveau délai appartienne à I_k. Alors avec probabilité au moins égale à p_m, la partie fractionnaire du nouveau délai est distante de $1/n$ des autres parties fractionnaires.

Posons $t = 1 + \max(u_e \mid e \in \mathcal{E})$. Le délai à l'instant $(k+1)t$ d'un événement u_e franchissable est obtenu par un tirage effectué dans l'intervalle temporel $]kt, (k+1)t]$. Par conséquent, avec une probabilité au moins égale à $(p_m)^{|\mathcal{E}|}$, la configuration visitée à l'instant kt est $1/n$-séparée.

Nous pouvons maintenant conclure. Une exécution visite (au moins) une classe infiniment souvent aux instants kt, disons Z. Puisqu'il existe une probabilité minimale (constante) que la configuration soit $1/n$-séparée au moment de la visite, la séquence visite infiniment souvent Z avec une configuration $1/n$-séparée. Toute classe Z' accessible l'est avec une longueur maximale puisque le graphe des classes est fini. Par conséquent, toute classe accessible Z' a une probabilité minimale (constante) d'être atteinte à chacune de ce type de visite. Donc elle est atteinte avec probabilité 1. Par conséquent, toutes les classes accessibles de Z le sont avec probabilité 1 et de toutes ces classes on revient à Z. Ceci établit le lemme.

c.q.f.d. $\Diamond\Diamond\Diamond$

3.6.1 Vérification du fragment qualitatif de PCTL

Etant donnés un système temps-réel probabiliste et une formule ϕ de PCTL, l'algorithme de vérification procède par évaluation successive des sous-formules de ϕ en « remontant » l'arbre syntaxique de la formule ϕ des feuilles à la racine et en étiquetant chaque classe du graphe des classes avec les sous-formules qu'il vérifie. Ainsi chaque étape de l'algorithme évalue une formule en interprétant les opérandes de l'opérateur le plus externe comme des propositions atomiques.

Le cas des opérations booléennes se traite comme usuellement et ne nécessite pas d'explications. Pour les autres opérateurs, il y a deux cas différents :

- La formule est attestée par l'existence d'un chemin fini lorsque l'opérateur externe est $E\mathcal{U}$. D'après le premier lemme, la vérification se fait comme dans le cas non probabiliste dans un graphe d'états.
- La formule est attestée par l'existence d'un chemin infini lorsque l'opérateur externe est $E\mathcal{G}p$. D'après le deuxième lemme, la vérification se fait en recherchant un chemin qui conduit à une c.f.c. terminale et telle que tous les états du chemin et de la c.f.c. terminale satisfait la sous-formule p.

Un tel algorithme a un temps polynomial par rapport à la taille du graphe des classes qui lui a une taille exponentielle ce qui conduit à un algorithme en EXPTIME. Cependant on peut faire mieux car il n'est pas nécessaire de construire le graphe des classes. Il suffit de chercher et construire un ou plusieurs chemins de manière non déterministe en espace polynomial puis de le déterminiser à l'aide de la procédure de Savitch [SAV 70]. On obtient donc un algorithme en PSPACE.

A titre d'exemple, pour décider si un sommet s appartient à une c.f.c. non terminale, on examine successivement tous les sommets s' et on vérifie si s' est accessible depuis s et s n'est pas accessible depuis s' (les deux en PSPACE).

Plus généralement, dans le cas de la vérification d'une formule on recherche un chemin élémentaire de manière non déterministe en vérifiant pour chaque état rencontré la satisfaction des sous-formules requises, puis on déterminise. On obtient ainsi un algorithme en espace polynomial par rapport à la la taille du système et linéaire par rapport à la taille de la formule.

3.6.2 Vérification du fragment qualitatif de PTCTL

Le model checking de PTCTL combine le model checking de TCTL dans le cas non probabilisé et le model checking de PCTL vu précédemment. Nous en donnons une présentation avec construction d'un graphe des classes étendu sachant que cette construction peut être évitée au moyen d'une recherche non déterministe de chemin (qui nous conduit aussi à une complexité en PSPACE).

En vue de la construction d'un graphe étendu, on ajoute au système un événement *spécial* e^* qui laisse s'écouler un délai fixe $dmax + 1$ (où $dmax$ est le maximum des indices de durée apparaissant dans la formule à vérifier) avant de devenir inactif.

On ajoute aussi au graphe des classes une propriété atomique $p_{\sim d}$ qui est vrai pour les classes telles que :

- e^* est actif et $d + 1 - c(e^*) \sim d$ pour les configurations de la classe.
- e^* est inactif et $d + 1 \sim d$.

Supposons qu'on ait évalué les classes pour les sous-formules d'une formule ϕ. La formule ϕ est évaluée ainsi :

- Une classe Z'_0 est étiquetée par $\Phi \equiv Ep\mathcal{U}_{\sim d}q$ s'il existe un chemin $Z_0, \ldots, Z_n$ telle que :
  1. Z_0 est la classe obtenue à partir Z'_0 en affectant à $c(e^*)$ la valeur $dmax + 1$.
  2. $Z_0, \ldots, Z_{n-1}$ sont étiquetées par p.
  3. Z_n est étiquetée par q et $p_{\sim d}$. Si de plus Z_n n'est pas pas une classe transitoire alors Z_n est étiquetée par p.
- Une classe Z'_0 est étiquetée par $\Phi \equiv E\mathcal{U}^{\circ}_{\sim d}$ s'il existe un chemin $Z_0, \ldots, Z_n$ telle que :
  1. Z_0 est la classe obtenue à partir Z'_0 en affectant à $c(e^*)$ la valeur $dmax + 1$.
  2. $Z_1, \ldots, Z_{n-1}$ sont étiquetées par p.
  3. Z_n est étiquetée par q et $p_{\sim d}$. Si de plus Z_n n'est pas pas une classe transitoire alors Z_n est étiquetée par p.
- Une classe Z'_0 est étiquetée par $\Phi \equiv E\mathcal{G}_{\sim d}p$ s'il existe un chemin $Z_0, \ldots, Z_n$ telle que :
  1. Z_0 est la classe obtenue à partir Z'_0 en affectant à $c(e^*)$ la valeur $dmax + 1$.
  2. $Z_0, \ldots, Z_n$ sont étiquetées par p.
  3. Z_n appartient à une c.f.c. terminale dont tous les sommets sont étiquetés par p ou par $\neg p_{\sim d}$.

La validité de cette procédure résulte immédiatement des lemmes précédents.

Chapitre 4

Model checking de DTMC infinies

4.1 Automates à piles probabilisés [ESP 06]

Dans ce chapitre, nous étendons le model checking de DTMC à des familles de DTMC infinies. Il est évident que ces DTMC doivent être structurées afin d'espérer des résultats de décidabilité. Puisqu'une DTMC « ressemble » à un automate fini probabilisé, une idée d'extension est de probabiliser un automate à pile.

Définition 62 *Un automate à pile probabiliste (*pPDA*) est un tuple* $\mathcal{A} = (Q, \Gamma, \delta, Prob)$ *où :*
- Q *est un ensemble fini d'états ;*
- Γ *est l'alphabet (fini) de la pile ;*
- $\delta \subseteq Q \times \Gamma \times Q \times \Gamma^*$ *est la relation de transition finie.*
  On note $pX \to q\alpha$ *un élement* $(p, X, q, \alpha) \in \delta$
- $Prob : \delta \mapsto]0, 1]$ *affecte à chaque transition une probabilité qui vérifie :*
  $\forall p \in Q \ \forall X \in \Gamma \ \sum_{pX \to q\alpha \in \delta} Prob(pX \to q\alpha) \in \{0, 1\}$
  On note $pX \xrightarrow{x} q\alpha$ *avec* $x = Prob(pX \to q\alpha)$.

Une configuration d'un pPDA est un couple (q, w) où q est un état et w est un mot de Γ^*. Le mot w représente l'état de la pile lue de haut en bas.

Définition 63 *La chaîne de Markov* $\mathcal{M}(\mathcal{A})$ *associée à un* pPDA $\mathcal{A}$ *est définie par :*
- *Les configurations de* $\mathcal{A}$ *sont les états de* $\mathcal{M}(\mathcal{A})$ *;*
- $\mathbf{P}[(p, w), (q, w')] = x$ *s'il existe* $pX \xrightarrow{x} q\alpha$ *et* w'' *t.q.* $w = Xw''$ *et* $w' = \alpha w''$.

Remarquons que certains états sont « absorbants » au sens où les probabilités de transition issues de ces états est nul. Par exemple, tous les états (p, ε) (où ε désigne le mot vide) sont absorbants. Cette extension ne modifie pas les résultats vus sur les DTMC. Si le lecteur est gêné, il peut ajouter une boucle de probabilité 1 autour de ces états.

Exemple 1. Soit le pPDA défini ainsi : il a un unique état que nous omettons dans les transitions. Les symboles de la pile sont Z, D, I. La pile contient initialement Z (pour zéro). Les transitions sont :
- $Z \xrightarrow{x} IZ$, $Z \xrightarrow{1-x} DZ$
- $I \xrightarrow{x} II$, $I \xrightarrow{1-x} \varepsilon$
- $D \xrightarrow{1-x} DD$, $I \xrightarrow{x} \varepsilon$

La figure 4.1 décrit la chaîne de Markov associée au pPDA. Le lecteur aura compris que les états représentent les gains ou les pertes d'un joueur dans un jeu de pile ou face avec une pièce biaisée dont la probabilité de tomber sur pile est x.

A l'aide du théorème 14, nous allons obtenir une caractérisation simple de la récurrence de la chaîne. Supposons d'abord $x > 1/2$ et posons $p = \frac{1-x}{x} < 1$. Le système d'équations de ce théorème

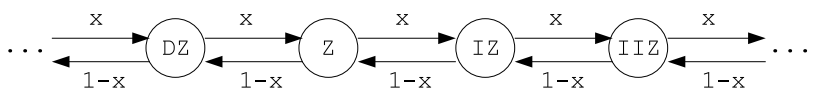

FIGURE 4.1 – Un jeu de pile ou face

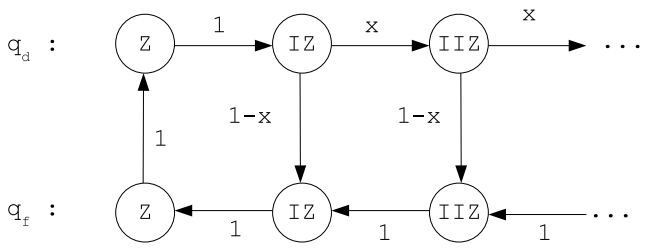

FIGURE 4.2 – Un serveur par lot

pour les états positifs s'écrit $x_1 = xx_2$ et $\forall i \geq 2\ x_i = xx_{i+1} + (1-x)x_{i-1}$.
On vérifie que $x_i = (1-p^i)$ est une solution de ce système. En posant $x_i = 0$ pour i négatif, on obtient une solution non nulle du système. Donc la chaîne est transitoire. Par symétrie si $x < 1/2$, la chaîne est aussi transitoire.

Supposons maintenant $x = 1/2$, Alors
$\forall i \geq 2\ (x_{i+1} - x_i) = x_i - x_{i-1} = \frac{1}{2}x_1$
Si $x_1 > 0$ alors la suite x_i ne peut être bornée par 1, donc $x_1 = 0$ et $\forall i \geq 2\ x_i = 0$. Par symétrie les x_i, pour i négatif, sont aussi nuls. Par conséquent la chaîne est récurrente ssi $x = 1/2$.

Le caractère récurrent d'une chaîne peut facilement s'exprimer à l'aide du fragment qualitatif de PCTL. On voit donc ici que la graphe des transitions n'est pas suffisant pour évaluer ce fragment contrairement au cas des chaînes finies.

Exemple 2. Soit un pPDA comportant deux états q_d et q_f. Ce pPDA modélise un serveur qui traite les requêtes par lots. Lorsqu'il est dans l'état q_d, il constitue son lot puis il traite les requêtes dans l'état q_f. Ses transitions sont :

- $q_dZ \xrightarrow{1} q_dIZ$, $q_fZ \xrightarrow{1} q_dZ$
- $q_dI \xrightarrow{x} q_dII$, $q_dI \xrightarrow{1-x} q_fI$
- $q_fI \xrightarrow{1} q_f\varepsilon$

La figure 4.2 décrit la chaîne de Markov associée au pPDA.

4.2 Une logique temporelle pour les pPDA

La logique que nous proposons est une variante de PCTL. Sa syntaxe est la suivante :

$$\varphi ::= \mathbf{tt} \mid a \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \mathcal{X}^{\bowtie q}\varphi \mid \varphi_1 \mathcal{U}^{\bowtie q}\varphi_2$$

avec $a \in \mathcal{P}$ où $\mathcal{P}$ désigne l'ensemble des propositions atomiques.

La notation adoptée est plus succincte que celle de PCTL car les opérateurs temporels incluent la valeur et l'opérateur de comparaison à appliquer à la probabilité calculée.

Etant donné un pPDA, nous supposons donnée une valuation $\nu : Q \times \Gamma^* \mapsto 2^{\mathcal{P}}$ qui associe aux configurations les propositions atomiques qu'ils satisfont. Remarquons que nous avons là une nouvelle difficulté : comment spécifier cette valuation de manière finie ? Nous répondrons à cette question un peu plus tard.

Pour le moment nous allons montrer comment étendre la valuation. Nous notons dans la suite $S = Q \times \Gamma^*$ l'ensemble infini des configurations. De manière préalable nous rappelons les définitions relatives aux opérateurs de chemin. Soulignons ici une différence (mineure) avec les DTMC standard. Ici lorsque la pile est vide, l'état courant n'a pas de successeur. Afin de raisonner sur la possibilité de blocage, nous considérons les chemins maximaux qui peuvent être soit infinis, soit finis si le chemin se termine sur un état de blocage. On note un tel chemin $\sigma = s_0, s_1, \ldots$ et I_σ désigne l'ensemble (fini ou infini) des indices des états. Soient S', S'' deux sous-ensembles d'états, alors :

- $\sigma \vDash \mathcal{X}S'$ ssi $1 \in I_\sigma \wedge s_1 \in S'$. $\Pr(s, \mathbf{X}S')$ désigne la probabilité qu'un chemin maximal aléatoire issu de s vérifie $\mathbf{X}S'$.
- $\sigma \vDash S'\mathcal{U}S''$ ssi $\exists i \in I_\sigma \; s_i \in S'' \wedge \forall j < i \; s_j \in S'$. $\Pr(s, S'\mathcal{U}S'')$ désigne la probabilité qu'un chemin maximal aléatoire issu de s vérifie $S'\mathcal{U}S''$.

Voici maintenant la sémantique de PCTL.

- $\nu(\mathbf{tt}) = S$
- $\nu(\neg\varphi) = S \setminus \nu(\varphi)$
- $\nu(\varphi_1 \wedge \varphi_2) = \nu(\varphi_1) \cap \nu(\varphi_2)$
- $\nu(\mathbf{X}^{\bowtie\varrho}\varphi) = \{s \mid \Pr(s, \mathbf{X}\nu(\varphi)) \bowtie \varrho)$
- $\nu(\varphi_1\mathcal{U}^{\bowtie\varrho}\varphi_2) = \{s \mid \Pr(s, \nu(\varphi_1)\mathcal{U}\nu(\varphi_2)) \bowtie \varrho)$

Le premier type de propositions atomiques que nous considérons est appelé proposition *simple*. Une proposition simple est une disjonction de propositions de type (q, ε) qui est satisfaite uniquement par la configuration éponyme, et de propositions de type (q, Y) qui est satisfaite par les configurations (q, Yw). Autrement dit ce type de propositions atomiques permet de raisonner sur l'état courant et sur le sommet de pile ou sur le fait que la pile est vide.

4.3 Algorithmes de model checking

4.3.1 Vérification de $a\mathcal{U}^{\bowtie\varrho}b$ avec a, b simples

La possibilité de model checking pour les DTMCinfinies est problématique. Afin de découvrir progressivement les difficultés, nous débutons cette section par la vérification de la formule $a\mathcal{U}^{\bowtie\varrho}b$ lorsque a et b sont des propositions simples.

Comme souvent avec les automates à pile, on pratique une étude de cas selon qu'un chemin qui satisfait la formule passe par un état où la pile a une hauteur moindre que la hauteur initiale ou non. Afin de faciliter cette étude de cas, on introduit de nouvelles notations.

Soit Ω un sous-ensemble de configurations alors :

- $\Omega^\bullet = \{(q, w) \mid (q, w) \in \Omega \wedge w \neq \varepsilon\}$ désigne le sous-ensemble S' privé des configurations avec une pile vide.
- Soit $\alpha \in \Gamma^*$, $U\alpha = \{(q, w\alpha) \mid (q, w) \in \Omega\}$ désigne le sous-ensemble des configurations de Ω complétées au fond de leur pile par le mot α.
- Les deux dernières notations sont relatives à deux sous-ensembles de configurations $S' = \nu(a), S'' = \nu(b)$ avec a, b des propositions simples mais nous ne les faisons pas apparaître dans les expressions dans un souci de clarté. $[pYq] = \Pr((p, Y), S' \setminus S''\mathcal{U}\{(q, \varepsilon)\}\}$ désigne la probabilité qu'un chemin (maximal) issu de la configuration (p, Y) se termine en (q, ε) en ayant toujours appartenu à S' sans jamais appartenir à S'' (sauf éventuellement dans le dernier état).
- $[pY\bullet] = \Pr((p, Y), S'\mathcal{U}S''^\bullet\}$ désigne la probabilité qu'un chemin (maximal) issu de la configuration (p, Y) satisfasse $S'\mathcal{U}S''$ et que le dernier état n'ait pas une pile vide.

A l'aide de ces notations, nous établissons une première équation liée à la décomposition en

cas :

$$\Pr((p, Y_1 \dots Y_n), S'\mathcal{U}S'') = [pY_1\bullet] + \sum_{q\in Q}[pY_1q]\Pr((q, Y_2 \dots Y_n), S'\mathcal{U}S'')$$

Un chemin peut satisfaire la formule soit sans passer par une configuration où la hauteur est moindre que la hauteur initiale, soit en atteignant une telle configuration forcément de la forme $(q, Y_2 \dots Y_n)$. Attention cette égalité n'est vraie que parce que les ensembles S', S'' sont associés à des propositions simples caractérisés par l'état et le sommet de pile courant !

En développant itérativement cette équation (les détails sont laissés au lecteur), on obtient :

$$\Pr((p, Y_1 \dots Y_n), S'\mathcal{U}S'') =$$

$$\sum_{i=1}^{n} \sum_{\substack{(q_1,\dots q_i) \text{ t.q.} \\ p=q_1}} \left(\prod_{j=1}^{i-1}[q_jY_jq_{j+1}]\right)[q_iY_i\bullet] + \sum_{\substack{(q_1,\dots q_{n+1}) \text{ t.q.} \\ p=q_1\wedge(q_{n+1},\varepsilon)\in S''}} \prod_{j=1}^{n}[q_jY_jq_{j+1}]$$

Cette formule traduit aussi une décomposition en cas (i.e. le nombre d'éléments de la pile initiale lus avec le cas de la pile vide).

Ainsi nous avons exprimé $\Pr((p, Y_1 \dots Y_n), S'\mathcal{U}S'')$ comme un polynôme dont les variables sont les $[pY\bullet]$ et les $[pYq]$. Nous allons maintenant étudier les relations qui lient ces valeurs.

Dans la suite, on suppose que les transitions du pPDA produisent des mots de longueur 0, 1 ou 2. Il est facile de transformer un pPDA quelconque en un pPDA dont le comportement est équivalent et qui vérifie cette condition par ajout d'états intermédiaires avec productions consécutives de mots de deux lettres. On peut même s'arranger que pour cette suite de transitions intermédiaires ait une longueur fixe (disons l) moyennant des transitions inutiles et modifier la sémantique de l'opérateur $\mathcal{X}$ pour considérer le $l$ième successeur plutôt que le premier. De toutes façons, il s'agit d'une facilité qui permet uniquement d'alléger les équations.

Nous exhibons maintenant un système d'équations vérifié par les $[pY\bullet]$ et les $[pYq]$.

– Si $(p, Y) \notin S' \setminus S''$ alors pour tout $q \in Q$, $[pYq] = 0$ sinon

$$[pYq] = \sum_{pY\xrightarrow{x}rZT} x\sum_{q'\in Q}[rZq'][q'Tq] + \sum_{pY\xrightarrow{x}rZ} x[rZq] + \sum_{pY\xrightarrow{x}q\varepsilon} x$$

– Si $(p, Y) \in S''$ alors $[pY\bullet] = 1$ sinon si $(p, Y) \notin S'$ alors $[pY\bullet] = 0$ sinon

$$[pY\bullet] = \sum_{pY\xrightarrow{x}rZT} x\left([rZ\bullet] + \sum_{q'\in Q}[rZq'][q'T\bullet]\right) + \sum_{pY\xrightarrow{x}rZ} x[rZ\bullet]$$

Ces équations sont aussi obtenues par des décompositions en cas. Examinons par exemple la deuxième équation. Pour satisfaire la formule en partant de (p, Y) sans vider la pile et sachant que $(p, Y) \in S' \setminus S''$, il faut franchir une transition qui produit un mot de deux lettres ou d'une lettre. Dans le premier cas ($pY \xrightarrow{x} rZT$) on peut satisfaire la formule sans revenir à la hauteur initiale de la pile ($[rZ\bullet]$) ou en y revenant ($[rZq'][q'T\bullet]$). Dans le deuxième cas ($pY \xrightarrow{x} rZ$) on est ramené à la quantité ($[rZ\bullet]$).

La question qui vient naturellement est de savoir si ce système d'équations admet une unique solution. La réponse est négative ... mais par contre les valeurs que nous cherchons constituent la plus petite solution de ce système. Expliquons en la raison. Notons $[pY\bullet]^k$ la probabilité de satisfaire $a\mathcal{U}b$ à partir de (p, Y) sans vider la pile par un chemin de longueur au plus k et $[pYq]^k$ la probabilité de vider la pile en satisfaisant a mais jamais b sur les tous les états sauf éventuellement sur le dernier par un chemin de longueur au plus k. On remarque que $\lim_{k\to\infty}[pY\bullet]^k = [pY\bullet]$ et $\lim_{k\to\infty}[pYq]^k = [pYq]$.

Il nous suffit donc de démontrer par récurrence que les $[pY\bullet]^k$ et $[pYq]^k$ sont inférieurs ou égaux à toute solution du système d'équations vu plus haut que l'on notera $\langle pY\bullet\rangle$ et $\langle pYq\rangle$.

Par construction, les $[pY\bullet]^0 \le \langle pY\bullet\rangle$ et $[pYq]^0 \le \langle pYq\rangle$.

D'autre part,

– Si $(p,Y) \notin S' \setminus S''$ alors pour tout $q \in Q$, $[pYq]^{k+1} = 0$ sinon

$$[pYq]^{k+1} \leq \sum_{pY \xrightarrow{x} rZT} x \sum_{q' \in Q} [rZq']^k [q'Tq]^k + \sum_{pY \xrightarrow{x} rZ} x[rZq]^k + \sum_{pY \xrightarrow{x} q\varepsilon} x$$

– Si $(p,Y) \in S''$ alors $[pY\bullet]^{k+1} = 1$ sinon si $(p,Y) \notin S'$ alors $[pY\bullet]^{k+1} = 0$ sinon

$$[pY\bullet]^{k+1} \leq \sum_{pY \xrightarrow{x} rZT} x \left([rZ\bullet]^k + \sum_{q' \in Q} [rZq']^k [q'T\bullet]^k \right) + \sum_{pY \xrightarrow{x} rZ} x[rZ\bullet]^k$$

On a affaire ici à des inégalités car (par exemple) les chemins qui conduisent à la valeur $[rZq']^k[q'Tq]^k$ sont des chemins de longueur comprises entre 0 et $2k$ mais contiennent tous les chemins de longueur inférieure ou égale à k. En appliquant la récurrence on substitue dans les inégalités $[pY\bullet]^k$ par $\langle pY\bullet\rangle$ et $[pYq]^k$ par $\langle pYq\rangle$. Cette substitution est justifiée car on a affaire à un opérateur croissant.

Nous avons maintenant tous les éléments pour décider si $(q,w) \vDash a\mathcal{U}^{\bowtie\varrho}b$. Notons $\vec{Y}$ un vecteur de variables correspondant aux $[pYq]$ et aux $[pY\bullet]$, $\mathbf{P}(\vec{Y})$ le polynôme définissant $\Pr((q,w), a\mathcal{U}b)$ en fonction des $[pYq]$ et des $[pY\bullet]$, $\vec{\mathbf{Op}}(\vec{Y})$ l'opérateur correspondant au système d'équations que vérifient les $[pYq]$ et aux $[pY\bullet]$. La formule est vérifiée si la formule de logique du premier ordre dans les réels est vraie :

$$\exists \vec{Y}\ \vec{Y} \geq \vec{0} \wedge \vec{Y} = \vec{\mathbf{Op}}(\vec{Y}) \wedge (\forall \vec{Z}\ (\vec{Z} \geq \vec{0} \wedge \vec{Z} = \vec{\mathbf{Op}}(\vec{Z})) \Rightarrow \vec{Z} \geq \vec{Y}) \wedge \mathbf{P}(\vec{Y}) \bowtie \varrho$$

Or la logique du premier ordre sur les réels est décidable [TAR 51] (on pourra aussi consulter mes notes de cours sur la calculabilité et la logique, `http://www.lsv.ens-cachan.fr/~haddad/courslogique.pdf`, section 4.6 pour une preuve en français).

Remarquez la subtilité, on ne sait pas calculer la valeur de la probabilité, mais on sait la comparer avec la valeur ϱ, ce qui est raisonnable puisque cette valeur n'est pas un rationnel mais obtenue à partir d'un zéro d'un polynôme multivariables.

4.3.2 Vérification de $a\mathcal{U}^{\bowtie\varrho}b$ avec a, b régulières

Nous voulons maintenant employer la méthode « bottom-up » afin d'obtenir une évaluation d'une formule de PCTL. Cela signifie que l'on souhaite remplacer la formule $a\mathcal{U}^{\bowtie\varrho}b$ par une propriété simple qui caractérise l'ensemble des configurations qui vérifient $a\mathcal{U}^{\bowtie\varrho}b$.

Nous nous restreignons ici à ce qu'on appelle le fragment qualitatif de PCTL, i.e. lorsque la valeur ϱ à comparer est soit 0 soit 1.

Afin d'illustrer les difficultés que nous rencontrons, prenons un exemple très simple de pPDA : deux états p, q et une unique transition $pY \xrightarrow{1} q\varepsilon$. Supposons que nous voulions déterminer l'ensemble des configurations qui vérifient $\mathbf{X}^{\geq 1}(q,Z)$. Cet ensemble est exactement l'ensemble des configurations de la forme (p, YZw) avec $w \in \Gamma^*$. Autrement dit, même dans le cas du fragment qualitatif de PCTL, les configurations qui vérifient une formule écrite avec des propositions simples ne sont pas caractérisables par une proposition simple.

Nous devons donc généraliser nos types de propositions atomiques. Nous nous tournons vers une généralisation naturelle : les propriétés régulières.

Définition 64 *Soit $\mathcal{A}$ un* pPDA*, un $\mathcal{A}$-automate $\mathcal{B} = (St, \delta', Acc)$ est un automate déterministe complet d'alphabet Γ, de fonction de transition δ', de sous-ensemble d'états d'acceptation Acc et tel que l'ensemble des états St vérifie $Q \subseteq St$.*

Une propriété régulière est une propriété spécifiée par un $\mathcal{A}$-automate. L'ensemble des configurations qui vérifient cette propriété est l'ensemble des configurations (q,w) telles que $\delta'(q, w^R) \in Acc$ où w^R est le mot miroir de w. Autrement dit le contenu de la pile lue de bas en haut conduit à un état d'acceptation en partant de q.

Nous souhaitons réutiliser l'algorithme de vérification de formules à base de propriétés simples pour concevoir un algorithme de vérification de formules à base de propriétés régulières. La solution consiste à construire un pPDA qui permet d'exprimer un ensemble fini de propriétés régulières sur le pPDA original comme un ensemble fini de propriétés simples sur le nouveau pPDA.

Plus précisément, soit $\mathcal{A}$ un pPDA et $b_1, \ldots, b_n$ des propriétés régulières décrites par les $\mathcal{A}$-automates $\mathcal{B}_1, \ldots, \mathcal{B}_n$. Nous construisons le pPDA $\mathcal{A}'$ ainsi :

- L'ensemble des états de $\mathcal{A}'$ est celui de $\mathcal{A}$
- L'alphabet de $\mathcal{A}'$ est $\Gamma' = \Gamma \times St$ où $St = \prod_{i=1}^{n} (St_i)^Q$. Soit $\vec{st} \in St$, on note $\vec{st}(i,p)$ la composante correspondante à i et à p.
- Les transitions de $\mathcal{A}'$ sont définies ainsi :
  1. Si $pY \xrightarrow{x} q\varepsilon \in \delta$ alors $p(Y, \vec{st}) \xrightarrow{x} q\varepsilon$ pour tout $\vec{st}$.
  2. Si $pY \xrightarrow{x} qZ \in \delta$ alors $p(Y, \vec{st}) \xrightarrow{x} q(Z, \vec{st})$ pour tout $\vec{st}$.
  3. Si $pY \xrightarrow{x} qZT \in \delta$ dans $\mathcal{A}$ alors $p(Y, \vec{st}) \xrightarrow{x} q(Z, \vec{st'})(T, \vec{st})$ pour tout $\vec{st}$ et tout $\vec{st'}$ tels que $\vec{st'}(i,r) = \delta'_i(\vec{st}(i,r), T)$ pour tout i et tout r.

Définissons la fonction (injective) $f : S \mapsto S'$ par :

- $f(p, \varepsilon) = (p, \varepsilon)$
- $f(p, Y_1 \ldots Y_k) = (p, (Y_1, \vec{st}_1) \ldots (Y_k, \vec{st}_k))$ où $\vec{st}_k(i,r) = r$ et $\forall j < k\ \vec{st}_j(i,r) = \delta'_i(\vec{st}_{j+1}(i,r), Y_{j+1})$ pour tout i et tout r.

Ainsi étant donnée une configuration $(p, Y_1 \ldots Y_k)$ avec $f(p, Y_1 \ldots Y_k) = (p, (Y_1, \vec{st}_1) \ldots (Y_k, \vec{st}_k))$, $\vec{st}_1(i,r)$ fournit l'état courant du calcul dans $\mathcal{B}_i$ en partant de r et en lisant le contenu de la pile de bas en haut à l'exception du sommet.

De plus par construction :

- Pour tout $s, s' \in S$ si $s \xrightarrow{x} s'$ alors $f(s) \xrightarrow{x} f(s')$
- Pour tout $s \in S, s^* \in S'$ si $f(s) \xrightarrow{x} s^*$ alors $\exists s' \in S'\ s \xrightarrow{x} s'$ et $f(s') = s^*$

On voit donc que f induit un isomorphisme de système probabilisé sur son image. Définissons maintenant b'_i la propriété simple qui correspond à b_i :

$$\nu(b'_i) = \{(p, (Y, \vec{st}))w \mid \delta'_i(\vec{st}(i,p), Y) \in Acc_i\} \cup \{(p, \varepsilon) \mid p \in Acc_i\}$$

Ici encore par construction $s \in \nu(b_i)$ ssi $f(s) \in \nu(b'_i)$.

Nous déduisons de cette construction, un procédé très simple pour vérifier dans $\mathcal{A}$ si $s \vDash a\mathcal{U}^{\bowtie\varrho}b$ avec a et b régulières. On construit l'automate $\mathcal{A}'$ correspondant à l'ensemble $\{a, b\}$ et on vérifie si $f(s) \vDash a'\mathcal{U}^{\bowtie\varrho}b'$.

De plus, supposons maintenant que $S^* \subseteq S'$ soit un ensemble régulier de configurations reconnu par un $\mathcal{A}'$-automate $\mathcal{B}'$, alors $f^{-1}(S^*)$ est régulier et ceci de la manière effective suivante. On construit un $\mathcal{A}'$-automate $\mathcal{B}''$ qui reconnaît $f(S)$: l'automate garantit que deux vecteurs $\vec{st'}, \vec{st}$ consécutifs dans la pile sont tels que $\vec{st'}(i,r) = \delta'_i(\vec{st}(i,r), T)$ avec T le symbole associé à $\vec{st}$. On construit l'automate produit de $\mathcal{B}'$ et $\mathcal{B}''$ qui reconnaît $S^* \cap f(S)$ et en projetant sur le premier composant de l'alphabet on obtient un automate qui reconnaît $f^{-1}(S^*)$. Cette observation sera utilisée au prochain paragraphe.

4.3.3 Vérification du fragment qualitatif de PCTL avec propositions régulières

Le model checking du fragment qualitatif de PCTL avec propositions régulières consiste à évaluer les sous-formules de la formule φ à vérifier de bas en haut de l'arbre syntaxique de φ en remplaçant chaque sous-formule par une proposition régulière (i.e. un automate qui la spécifie). La preuve pour les formules faisant intervenir l'opérateur $\mathbf{X}$ est élémentaire. Aussi nous allons nous consacrer aux formules faisant intervenir l'opérateur $\mathcal{U}$.

En raison de la transformation précédente nous pouvons nous restreindre au cas des propositions simples. En effet si la formule fait intervenir des propositions régulières, on applique la transformation du pPDA et des propositions régulières. On applique ensuite les résultats énoncés

ci-dessous pour obtenir une proposition régulière qui caractérise les états du nouvel automate qui satisfont la formule. Enfin, à l'aide de l'observation qui conclut la section précédente, on calcule la proposition régulière qui caractérise les états de l'automate initial qui satisfont la formule.

Proposition 65 *Soit la formule $\varphi = a\mathcal{U}^{=1}b$ avec a, b des propositions simples. Alors l'ensemble des états $S' = \{s \mid s \vDash \varphi\}$ est régulier et sa représentation est calculable.*

Preuve
Notons $R(p, Y) = \{q \mid [pYq] > 0\}$ l'ensemble des états (q, ε) qu'on peut atteindre de (p, Y) (i.e. avec une probabilité non nulle) en passant par des états qui vérifient a.

Définissons une famille d'ensembles de configurations $\{S_i\}_{i\in\mathbb{N}}$ ainsi :
- $S_0 = \{(q, \varepsilon) \mid (q, \varepsilon) \in \nu(b)\}$
- $S_{i+1} = \{(q, Y\alpha) \mid [qY\bullet] + \sum_{q'\in R(q,Y)}[qYq'] = 1 \wedge \forall q' \in R(q, Y)\ (q', \alpha) \in S_i \wedge \alpha \in \Gamma^*\}$

Nous affirmons que $S' = \bigcup_{i\in\mathbb{N}} S_i$. L'assertion $S_i \subseteq S'$ se démontre par récurrence et elle est laissée en exercice. Soit maintenant $(q, Y_1 \dots Y_n) \in S'$. Démontrons par récurrence sur n que $(q, Y_1 \dots Y_n) \in S_n$. Pour $n = 0$, ceci entraîne que $(q, \varepsilon) \in b$ et par conséquent $(q, \varepsilon) \in S_0$. Supposons maintenant $n > 0$. Les chemins se décomposent en ceux tels que la hauteur de pile sera toujours supérieure ou égale à la hauteur initiale et les autres. La probabilité que les chemins du premier type satisfassent φ est égale à $[qY\bullet]$ et la probabilité pour les chemins du second type est égale à $\sum_{q'\in R(q,Y)}[qYq']\pi(q, Y_2 \dots Y_n)$ où $\pi(q, Y_2 \dots Y_n)$ est la probabilité qu'un chemin issu de $(q, Y_2 \dots Y_n)$ satisfasse φ. Pour que la probabilité cumulée soit égale à 1, il faut nécessairement que $\pi(q, Y_2 \dots Y_n) = 1$ et donc par hypothèse de récurrence que $(q, Y_2 \dots Y_n) \in S_{n-1}$. Alors par définition, $(q, Y_1 \dots Y_n) \in S_n$.

En nous appuyant sur ce résultat, nous décrivons un automate, $\mathcal{A}_p$ qui reconnaît $S' \cap \{(p, \alpha)\}_{\alpha\in\Gamma^*}$. Cette fois les configurations sont décrites avec lecture de la pile de haut en bas mais ce n'est pas un problème car il est très facile (et laissé en exercice) de transformer ensuite l'automate pour qu'il reconnaisse les configurations dont les piles sont lues de bas en haut. L'automate final est simplement l'union des automates transformés. L'automate $\mathcal{A}_p$ déterministe *mais incomplet* est défini par :
- Ses états sont les sous-ensembles de Q, son état initial est $\{p\}$ et ses états terminaux sont les sous-ensembles Q' tels que pour tout $q' \in Q'$, $(q', \varepsilon) \in \nu(b)$ (autrement dit tous les sous-ensembles de $\{q' \mid (q', \varepsilon) \in \nu(b)\}$).
- Il y a une transition $Q' \xrightarrow{Y} Q''$ ssi $\forall q \in Q'\ [qY\bullet] + \sum_{q'\in R(q,Y)}[qYq'] = 1$ et $Q'' = \bigcup_{q\in Q'} R(q, Y)$

D'après la définition des S_i, il est immédiat que le langage de $\mathcal{A}_p$ est $\{\alpha \mid (p, \alpha) \in S'\}$.

c.q.f.d. ◊◊◊

Proposition 66 *Soit la formule $\varphi = a\mathcal{U}^{=0}b$ avec a, b des propositions simples. Alors l'ensemble des états $S' = \{s \mid s \vDash \varphi\}$ est régulier et sa représentation est calculable.*

Preuve
La preuve suit un schéma similaire à la preuve précédente. Définissons une famille d'ensembles de configurations $\{S_i\}_{i\in\mathbb{N}}$ ainsi :
- $S_0 = \{(q, \varepsilon) \mid (q, \varepsilon) \notin \nu(b)\}$
- $S_{i+1} = \{(q, Y\alpha) \mid [qY\bullet] = 0 \wedge \forall q' \in R(q, Y)\ (q', \alpha) \in S_i \wedge \alpha \in \Gamma^*\}$

Nous affirmons que $S' = \bigcup_{i\in\mathbb{N}} S_i$. L'assertion $S_i \subseteq S'$ se démontre par récurrence et elle est laissée en exercice. Soit maintenant $(q, Y_1 \dots Y_n) \in S'$. Démontrons par récurrence sur n que $(q, Y_1 \dots Y_n) \in S_n$. Pour $n = 0$, ceci entraîne que $(q, \varepsilon) \notin b$ et par conséquent $(q, \varepsilon) \in S_0$. Supposons maintenant $n > 0$. Les chemins se décomposent en ceux tels que la hauteur de pile sera toujours supérieure ou égale à la hauteur initiale et les autres. La probabilité que les chemins du premier type satisfassent φ est égale à $[qY\bullet]$ et la probabilité pour les chemins du second type est égale à $\sum_{q'\in R(q,Y)}[qYq']\pi(q, Y_2 \dots Y_n)$ où $\pi(q, Y_2 \dots Y_n)$ est la probabilité qu'un chemin issu de $(q, Y_2 \dots Y_n)$ satisfasse φ. Pour que la probabilité cumulée soit égale à 0, il faut nécessairement

que $\pi(q, Y_2 \dots Y_n) = 0$ et donc par hypothèse de récurrence que $(q, Y_2 \dots Y_n) \in S_{n-1}$. Alors par définition, $(q, Y_1 \dots Y_n) \in S_n$.

En nous appuyant sur ce résultat, nous décrivons un automate, $\mathcal{A}_p$ qui reconnaît $S' \cap \{(p, \alpha)\}_{\alpha \in \Gamma^*}$. Ici aussi les configurations sont décrites avec lecture de la pile de haut en bas. On transforme ensuite l'automate pour qu'il reconnaisse les configurations dont les piles sont lues de bas en haut. L'automate final est simplement l'union des automates transformés. L'automate $\mathcal{A}_p$ déterministe *mais incomplet* est défini par :

- Ses états sont les sous-ensembles de Q, son état initial est $\{p\}$ et ses états terminaux sont les sous-ensembles Q' tels que pour tout $q' \in Q'$, $(q', \varepsilon) \notin \nu(b)$ (autrement dit tous les sous-ensembles de $\{q' \mid (q', \varepsilon) \notin \nu(b)\}$).
- Il y a une transition $Q' \xrightarrow{Y} Q''$ ssi $\forall q \in Q'$ $[qY\bullet] = 0$ et $Q'' = \bigcup_{q \in Q'} R(q, Y)$

D'après la définition des S_i, il est immédiat que le langage de $\mathcal{A}_p$ est $\{\alpha \mid (p, \alpha) \in S'\}$.

c.q.f.d. ◊◊◊

4.4 Survol de la vérification probabiliste des DTMC

Historiquement, la vérification des chaînes à temps discret a précédé celle des chaînes à temps continu. La première approche de vérification de formules LTL sur des DTMC (proposée dans [VAR 85]) est conceptuellement simple : traduire la formule en un automate de Büchi, puis déterminiser cet automate en un automate de Rabin, effectuer le produit synchronisé de cet automate avec la DTMC ce qui conduit à une nouvelle DTMC sur laquelle une variante de l'analyse vue à la section 1.2 fournit la probabilité recherchée. Cependant la complexité de cet algorithme est doublement exponentielle relativement à la taille de la formule. Dans [COU 95], les auteurs construisent aussi une nouvelle DTMC en raffinant itérativement la DTMC initiale par une analyse des opérateurs de la formule. Ceci conduit à une procédure simplement exponentielle. Ils démontrent de plus qu'il s'agit là de la complexité optimale. Un troisième algorithme [COU 03] traduit aussi la formule en un automate de Büchi. Cependant le choix de l'algorithme de traduction permet d'évaluer la probabilité associée à la formule directement à partir du produit synchronisé de l'automate et de la DTMC. Cette méthode a aussi une complexité théorique optimale et se comporte mieux dans les cas pratiques que la précédente.

Une technique classique d'analyse des modèles de performance consiste à associer des «récompenses» aux états et/ou aux transitions d'une chaîne et de calculer des indices de performance relatifs à ces récompenses. Afin d'étendre la portée de la vérification probabiliste à ce type de modèle, une nouvelle logique PRCTL est introduite dans [AND 03] accompagnée d'un algorithme d'évaluation de formules.

Chapitre 5

Model checking de CTMC

5.1 Limites des indices de performance standard

Les indices de performance définis lors de la section précédente apportent des informations précieuses au concepteur du système. Cependant ils ne répondent pas à tous les besoins en terme d'évaluation. Illustrons ce point à l'aide de l'exemple de la disponibilité d'un service. Voici quelques propriétés relatives à ce concept :

- Garantie de disponibilité *instantanée* en régime transitoire. Il s'agit de la probabilité à un instant τ de la disponibilité du service.
- Garantie de disponibilité instantanée en régime stationnaire. Il s'agit de la probabilité à un instant donné de la disponibilité du service en régime stationnaire.
- Garantie de disponibilité *dans la durée* en régime transitoire. Il s'agit de la probabilité que le service soit constamment disponible entre deux instants τ et τ'.
- Garantie de disponibilité dans la durée en régime stationnaire. Il s'agit de la probabilité que le service soit constamment disponible entre deux instants en régime stationnaire. Puisque le processus est en régime stationnaire. Cette mesure ne dépend que la durée de l'intervalle constitué des deux instants.
- Garantie de disponibilité et de temps de réponse en régime stationnaire. Il s'agit la probabilité qu'après une requête, le service soit fonctionnel jusqu'à la réponse et que le temps de réponse n'excède pas une borne donnée.

Si les deux premières propriétés se déduisent facilement des distributions stationnaires et transitoires, il n'en est pas de même des autres. On pourrait imaginer un algorithme ad hoc pour chacune de celles-ci. Mais, il est plus judicieux d'introduire une logique afin d'exprimer des indices de performance complexes et de concevoir un algorithme général d'évaluation de formules de cette logique.

5.2 Une logique temporelle pour les chaînes de Markov

La logique temporelle CSL («Continuous Stochastic Logic») que nous allons détailler est une adaptation de la logique CTL («Computation Tree Logic» [EME 80]) aux chaînes de Markov à temps continu. Elle exprime des formules *qui s'évaluent sur les états* et dont la syntaxe est la suivante. Ici, nous suivrons principalement l'approche de [BAI 03a].

Définition 67 *Une formule de CSL est définie inductivement par :*

- *Si $\phi \in \mathcal{P}$ alors ϕ est une formule de CSL ;*
- *Si ϕ et ψ sont des formules de CSL alors $\neg\phi$ et $\phi \wedge \psi$ sont des formules de CSL ;*
- *Si ϕ est une formule de CSL, $a \in [0,1]$ est un réel, $\bowtie \in \{<, \leq, >, \geq\}$ alors $S_{\bowtie a}\phi$ est une formule de CSL ;*

– *Si ϕ et ψ sont des formules de CSL, $a \in [0,1]$ est un réel, $\bowtie \in \{<, \leq, >, \geq\}$ et I est un intervalle de $\mathbb{R}_{\geq 0}$ alors $P_{\bowtie a}\mathcal{X}^I\phi$ et $P_{\bowtie a}\phi\mathcal{U}^I\psi$ sont des formules de CSL.*

Seule l'interprétation des deux derniers points nécessite quelques explications. La formule $S_{\bowtie a}\phi$ est satisfaites par s un état de la chaîne si, pour le processus démarré en s, la probabilité stationnaire cumulée (disons p) des états qui satisfont ϕ vérifie $p \bowtie a$. L'évaluation de cette formule est bien définie car pour une CTMC finie, une distribution stationnaire existe toujours. Notons que l'évaluation de cette formule est indépendante de l'état considéré si la chaîne est ergodique.

Une réalisation du processus stochastique satisfait $\mathcal{X}^I\phi$ si le premier changement d'état a lieu dans l'intervalle I et l'état atteint vérifie ϕ. Un état s satisfait $P_{\bowtie a}\mathcal{X}^I\phi$ si la probabilité (disons p) qu'une réalisation du processus démarré en s satisfasse la contrainte énoncée vérifie $p \bowtie a$.

Une réalisation du processus stochastique satisfait $\phi\mathcal{U}^I\psi$ s'il existe un instant $\tau \in I$ tel que ψ soit satisfait et qu'à tous les instants précédents ϕ soit satisfait. Un état s satisfait $P_{\bowtie a}\phi\mathcal{U}^I\psi$ si la probabilité (disons p) qu'une réalisation du processus démarré en s satisfasse la contrainte énoncée vérifie $p \bowtie a$.

A titre d'exemple, nous formalisons maintenant les propriétés de disponibilité énoncées plus haut.

– Garantie de disponibilité instantanée en régime transitoire de 99% :

$$P_{\geq 0.99} true \mathcal{U}^{[\tau,\tau]} disp$$

où *disp* est une proposition atomique indiquant si le service est disponible.

– Garantie de disponibilité instantanée en régime stationnaire de 99% :

$$S_{\geq 0.99} disp$$

– Garantie de disponibilité dans la durée en régime transitoire de 99% :

$$P_{<0.01} true \mathcal{U}^{[\tau,\tau']} \neg disp$$

– Garantie de disponibilité dans la durée en régime stationnaire de 99% :

$$S_{<0.01} true \mathcal{U}^{[\tau,\tau']} \neg disp$$

– Garantie de disponibilité et de temps de réponse (3 unités de temps) en régime stationnaire de 99% :

$$S_{\geq 0.99}(req \Rightarrow P_{\geq 0.99}(disp \mathcal{U}^{[0,3]} acq))$$

où *req* est une proposition atomique indiquant une réception de requête et *acq* est une proposition atomique indiquant une réponse à une requête. On notera qu'en réalité les deux occurrences de 99% n'ont pas la même signification. Celle correspondant à l'opérateur interne est une exigence sur le comportement du processus démarré en un état particulier tandis que la deuxième occurrence est une exigence globale sur les états pondérée par une distribution stationnaire. *A priori*, des valeurs différentes d'exigence auraient pu être spécifiées.

5.3 Algorithme de vérification

Etant données une CTMC et une formule ϕ de CSL, l'algorithme de vérification procède par évaluation successive des sous-formules de ϕ en «remontant» l'arbre syntaxique de la formule ϕ des feuilles à la racine et en étiquetant chaque état avec les sous-formules qu'il vérifie. Ainsi chaque étape de l'algorithme évalue une formule en interprétant les opérandes de l'opérateur le plus externe comme des propositions atomiques.

Nous sommes donc conduits à étudier chaque opérateur.

$\boxed{\phi = \neg\psi}$ L'algorithme étiquette avec ϕ chaque état non étiqueté avec ψ.

$\boxed{\phi = \psi \wedge \chi}$ L'algorithme étiquette avec ϕ chaque état étiqueté avec ψ et χ.

$\boxed{\phi = S_{\bowtie a}\psi}$ L'algorithme calcule la distribution stationnaire du processus démarré en s (ainsi qu'indiqué à la section 1.3). Puis il cumule les probabilités des états étiquetés par ψ et étiquette s avec ϕ si la quantité obtenue (disons p) vérifie $p \bowtie a$. Notons que pour les états d'une c.f.c. puits, un seul calcul est nécessaire pour tous les états de la c.f.c. De même, si la CTMC admet une unique distribution stationnaire alors la formule a une valeur de vérité indépendante de l'état.

$\boxed{\phi = P_{\bowtie a}\mathcal{X}^I\psi}$ Soit un état s, l'occurrence de la prochaine transition dans l'intervalle I et la satisfaction de ψ par l'état atteint sont deux événements indépendants. La probabilité recherchée est donc le produit de la probabilité de chacun de ces événements. Notons $I = [\tau, \tau']$; nous supposons ici sans perte de généralité que les intervalles sont fermés. En effet, en raison de la continuité des distributions, le fait que les bornes supérieures et inférieures de l'intervalle en fassent partie n'a pas d'incidence sur l'évaluation de la formule. Soit $\mathbf{Q}$ le générateur infinitésimal de la chaîne et $\mathbf{P}$ la matrice de transition de la chaîne incluse, alors la probabilité du premier événement est donnée par $e^{\tau\mathbf{Q}[s,s]} - e^{\tau'\mathbf{Q}[s,s]}$ tandis que celle du second événement est donnée par $\sum_{s' \vDash \psi} \mathbf{P}[s, s']$.

$\boxed{\phi = P_{\bowtie a}\psi\mathcal{U}^I\chi}$ L'évaluation de cette formule consiste essentiellement à effectuer une analyse transitoire de chaînes obtenues par des transformations élémentaires à partir de la chaîne originelle. Ainsi soit X une chaîne, alors X^ϕ est la chaîne obtenue en rendant absorbants les états qui vérifient ϕ. Afin de simplifier la présentation, nous étudions les différents types d'intervalle.

- $\phi = P_{\bowtie a}\psi\mathcal{U}^{[0,\infty[}\chi$. Dans ce cas, la réalisation du processus doit rester dans des états qui vérifient ψ jusqu'à ce qu'un état vérifiant χ soit atteint et ceci sans contrainte de temps. Autrement dit, on suit le comportement de la chaîne jusqu'à ce qu'on rencontre un état qui vérifie $\neg\psi \vee \chi$. Etudions la chaîne $X^{\neg\psi\vee\chi}$. Si une c.f.c. puits de cette chaîne contient un état qui vérifie χ alors la probabilité recherchée est 1 pour tous les états de cette c.f.c. (car tous les états d'une c.f.c. puits sont récurrents) sinon cette probabilité est nulle. Appelons une c.f.c. associée à une probabilité 1, une "bonne" c.f.c. Par conséquent, la probabilité recherchée pour les états restants est égale à la probabilité d'atteindre un état d'une bonne c.f.c. Cette probabilité ne dépend que de la chaîne incluse de $X^{\neg\psi\vee\chi}$ et son calcul a déjà été décrit à la section 1.2.
- $\phi = P_{\bowtie a}\psi\mathcal{U}^{[0,\tau]}\chi$. Dans ce cas, la réalisation du processus doit rester dans des états qui vérifient ψ jusqu'à ce qu'un état vérifiant χ soit atteint et ceci au plus tard à l'instant τ. Autrement dit on suit le comportement de la chaîne jusqu'à ce qu'on rencontre un état qui vérifie $\neg\psi \vee \chi$. La probabilité à calculer est donc égale à $\Pr(X^{\neg\psi\vee\chi}(\tau) \vDash \chi \mid X^{\neg\psi\vee\chi}(0) = s)$.
- $\phi = P_{\bowtie a}\psi\mathcal{U}^{[\tau,\tau]}\chi$. Dans ce cas, la réalisation du processus doit rester dans des états qui vérifient ψ durant l'intervalle $[0, \tau]$ et de plus vérifier χ à l'instant τ. On néglige la possibilité d'un changement d'état à l'instant τ car sa probabilité est nulle. Par conséquent, la probabilité à calculer est égale à $\Pr(X^{\neg\psi}(\tau) \vDash \psi \wedge \chi \mid X^{\neg\psi}(0) = s)$.
- $\phi = P_{\bowtie a}\psi\mathcal{U}^{[\tau,\infty[}\chi$. Dans ce cas, la réalisation du processus doit rester dans des états qui vérifient ψ durant l'intervalle $[0, \tau]$ puis à partir de l'état atteint s à l'instant τ verifier la formule $\psi\mathcal{U}^{[0,\infty[}\chi$. La probabilité recherchée est donc $\sum_{s' \vDash \psi} \Pr(X^{\neg\psi}(\tau) = s' \mid X^{\neg\psi}(0) = s) \cdot \boldsymbol{\pi}(s')$ où $\boldsymbol{\pi}(s')$ est calculée suivant la procédure du premier cas.
- $\phi = P_{\bowtie a}\psi\mathcal{U}^{[\tau,\tau']}\chi$. Un raisonnement similaire au cas précédent conduit la formule suivante pour la probabilité recherchée : $\sum_{s' \vDash \psi} \Pr(X^{\neg\psi}(\tau) = s' \mid X^{\neg\psi}(0) = s) \cdot \Pr(X^{\neg\psi\vee\chi}(\tau' - \tau) \vDash \chi \mid X^{\neg\psi\vee\chi}(0) = s')$.

5.4 Panorama de la vérification probabiliste de chaînes de Markov

Historiquement, la vérification des chaînes à temps discret a précédé celle des chaînes à temps continu. La première approche de vérification de formules LTL sur des DTMC (proposée dans [VAR 85]) est conceptuellement simple : traduire la formule en un automate de Büchi, puis déterminiser cet automate en un automate de Rabin, effectuer le produit synchronisé de cet automate

avec la DTMC ce qui conduit à une nouvelle DTMC sur laquelle une variante de l'analyse vue à la section 1.2 fournit la probabilité recherchée. Cependant la complexité de cet algorithme est doublement exponentielle relativement à la taille de la formule. Dans [COU 95], les auteurs construisent aussi une nouvelle DTMC en raffinant itérativement la DTMC initiale par une analyse des opérateurs de la formule. Ceci conduit à une procédure simplement exponentielle. Ils démontrent de plus qu'il s'agit là de la complexité optimale. Un troisième algorithme [COU 03] traduit aussi la formule en un automate de Büchi. Cependant le choix de l'algorithme de traduction permet d'évaluer la probabilité associée à la formule directement à partir du produit synchronisé de l'automate et de la DTMC. Cette méthode a aussi une complexité théorique optimale et se comporte mieux dans les cas pratiques que la précédente.

Une technique classique d'analyse des modèles de performance consiste à associer des «récompenses» aux états et/ou aux transitions d'une chaîne et de calculer des indices de performance relatifs à ces récompenses. Afin d'étendre la portée de la vérification probabiliste à ce type de modèle, une nouvelle logique PRCTL est introduite dans [AND 03] accompagnée d'un algorithme d'évaluation de formules.

Les premiers travaux significatifs relatifs aux CTMC ont été établis dans [AZI 00]. Il y est démontré que la vérification de formules CSL sur les CTMC est décidable. Cependant l'algorithme correspondant est extrêmement complexe car il «s'interdit» les approximations que nous avons implicitement faites lors des calculs du paragraphe précédent.

De fait, même avec la méthode décrite plus haut, le calcul peut s'avérer impraticable pour des CTMC de grande taille. Une approche efficace pour faire face à ce problème consiste à tirer profit de la modularité de la spécification. On cherche alors à remplacer un module par un module plus petit mais équivalent vis à vis de la formule à vérifier. On procède ensuite à la vérifcation du modèle composé des modules réduits. Cette démarche initiée par [BAI 03a] a été généralisée dans [BAI 03b] où de nombreuses formes d'équivalence sont étudiées.

Une approche radicalement différente pour réduire la complexité de la vérification est proposée dans [YOU 05]. Supposons que nous devions vérifier la formule $P_{\leq a}\phi$, nous pouvons générer des exécutions aléatoires et calculer le ratio des exécutions qui vérifient ϕ ; en vertu de résultats classiques de probabilité, cette valeur tend vers la probabilité recherchée. Lorsque l'évaluation de la formule ϕ ne requiert qu'une exécution temporellement bornée, cette méthode est particulièrement efficace.

Chapitre 6

Processus de décision markoviens : rappels

6.1 Présentation des processus de décision markoviens

Supposons que nous devions analyser l'exécution d'un ensemble de transactions telles que chacune d'entre elles puisse être modélisée par une DTMC. Dans la recherche d'une représentation du système complet, nous sommes alors confrontés au fait que l'ordonnanceur du système transactionnel nous est inconnu. Nous pourrions représenter les choix de l'ordonnanceur par des actions probabilistes et se ramener ainsi à une DTMC globale. Mais cette solution limite considérablement la portée des mesures ainsi obtenues. En effet, les résultats s'interpréteraient comme des indices de performance valables pour un ordonnanceur « moyen ». Or dans la pratique, les indices que l'on recherche sont des indices extrêmes tels que la probabilité maximale d'un abandon de transaction en considérant l'ensemble (infini) des ordonnanceurs possibles.

Il convient donc d'adopter un formalisme plus expressif que celui des DTMC. Plus précisement, ce formalisme doit permettre d'exprimer à la fois des choix probabilistes et des choix non déterministes. Ceci nous conduit naturellement aux *processus de décision markoviens* (« Markov Decision Process » MDP).

Définition 68 *Un processus de décision markovien $\Sigma = (S, \mathcal{P}, V, next)$ est défini par :*
- *S, l'ensemble (fini) des états ;*
- *$\mathcal{P}$, l'ensemble (fini) des propositions atomiques ;*
- *V, la fonction caractéristique des états qui associe à chaque état s, le sous-ensemble $V(s)$ de $\mathcal{P}$ des propositions qui sont vraies en s ;*
- *next la fonction qui associe à chaque état s, l'ensemble $next(s) = \{\boldsymbol{\pi}^s_1, \ldots, \boldsymbol{\pi}^s_{k_s}\}$ de distributions dont le support est S.*

L'ingrédient fondamental de cette définition est la fonction *next* qui contrôle l'évolution du processus. Dans un état s, le processus choisit de manière non déterministe une distribution $\boldsymbol{\pi}^s_i \in next(s)$, puis effectue un tirage probabiliste selon cette distribution ce qui détermine l'état suivant. En accord avec cette interprétation, nous introduisons une relation de succession (immédiate) ρ définie par $\rho(s, s') \Leftrightarrow \exists \boldsymbol{\pi}^s_i \ \boldsymbol{\pi}^s_i(s') > 0$. Un chemin d'exécution est alors une suite d'états tels que tout couple de deux états consécutifs satisfasse cette relation.

Nous désirons placer ce système dans un cadre probabiliste « pur». A cette fin, nous définissons la notion de stratégie. Une stratégie St est une fonction qui associe à un chemin d'exécution $s_0, s_1, \ldots, s_n$, $St(s_0, s_1, \ldots, s_n)$ une distribution appartenant à $next(s_n)$. Pour une stratégie fixée et un état initial donné, le processus de décision markovien se comporte comme un processus stochastique à temps discret et par conséquent, la probabilité d'un événement Ev de ce processus est bien définie et sera notée $\Pr^{St}(Ev)$.

Chapitre 7

Model checking de MDP

7.1 Une logique temporelle pour les processus de décision markoviens

La logique temporelle pCTL («probabilistic Computation Tree Logic») que nous allons détailler est une adaptation de CTLaux processus de décision markoviens. Ici, nous suivons principalement l'approche de [BIA 95]. Les formules de cette logique s'évaluent sur les états et leur syntaxe est la suivante.

Définition 69 *Une formule de pCTL est définie inductivement par :*
- *Si $\phi \in \mathcal{P}$ alors ϕ est une formule de pCTL ;*
- *Si ϕ et ψ sont des formules de pCTL alors $\neg\phi$ et $\phi \wedge \psi$ sont des formules de pCTL ;*
- *Si ϕ et ψ sont des formules de pCTL, $a \in [0,1]$ est un réel et $\bowtie \in \{<, \leq, >, \geq\}$ alors $A\phi\mathcal{U}\psi$, $E\phi\mathcal{U}\psi$ et $P_{\bowtie a}\phi\mathcal{U}\psi$ sont des formules de pCTL.*

Seule l'interprétation du dernier point nécessite quelques explications. Les deux premiers opérateurs ne font pas intervenir les valeurs numériques des distributions. $A\phi\mathcal{U}\psi$ (resp. $E\phi\mathcal{U}\psi$) est vrai en un état s ssi tout (resp. au moins un) chemin d'exécution à partir de s comprend un préfixe constitué d'états qui satisfont ϕ suivi d'un état qui satisfait ψ. Le dernier opérateur fait intervenir les stratégies de la manière suivante : $P_{\bowtie a}\phi\mathcal{U}\psi$ est vrai en s si *pour toute stratégie*, la probabilité (disons p) pour le processus stochastique associé qu'un chemin d'exécution issu de s comprenne un préfixe constitué d'états qui satisfont ϕ suivi d'un état qui satisfait ψ vérifie $p \bowtie a$.

7.2 Algorithme de vérification

Etant donné un processus de décision markovien et une formule ϕ de pCTL, l'algorithme de vérification procède par évaluation successive des sous-formules de ϕ en «remontant» l'arbre syntaxique de la formule ϕ des feuilles à la racine et en étiquetant chaque état avec les sous-formules qu'il vérifie. Ainsi chaque étape de l'algorithme évalue une formule en interprétant les opérandes de l'opérateur le plus externe comme des propositions atomiques.

Nous sommes donc conduits à étudier chaque opérateur.

$\boxed{\phi = \neg\psi}$ L'algorithme étiquette avec ϕ chaque état non étiqueté avec ψ.

$\boxed{\phi = \psi \wedge \chi}$ L'algorithme étiquette avec ϕ chaque état étiqueté avec ψ et χ.

$\boxed{\phi = E\psi\mathcal{U}\chi}$ Dans un premier temps, l'algorithme étiquette les états étiquetés avec χ. Puis en remontant à partir de ces états à l'aide de la relation de prédécesseur (ρ^{-1}) il étiquette les états étiquetés avec ψ. Il itère cette étape à partir des états nouvellement étiquetés jusqu'à saturation.

$\boxed{\phi = A\psi\mathcal{U}\chi}$ L'algorithme emploie une fonction récursive *en marquant* les états visités. Lorsqu'il évalue un état étiqueté par χ, il l'étiquette avec ϕ et renvoie vrai. Lorsqu'il évalue un état non

étiqueté par χ et par ψ, il renvoie faux. Lorsqu'il évalue un état non étiqueté par χ mais étiqueté par ψ et *non encore visité*, il appelle la fonction pour chacun des successeurs de l'état et l'étiquette par ϕ si tous les appels renvoient vrai. Lorsqu'il évalue un état *déjà visité* et non étiqueté, il renvoie faux. Le lecteur vérifiera que cette procédure renvoie faux s'il existe un chemin issu de l'état qui comprend un état non étiqueté par ϕ ou χ avant tout état étiqueté par χ ou un chemin (infini) constitué d'états étiquetés par ϕ mais pas par χ. Ce dernier cas est détecté par l'existence d'un circuit à l'aide du marquage des états.

$\boxed{\phi = P_{\geq a}\psi\mathcal{U}\chi}$ Nous traiterons uniquement ce cas d'opérateur probabiliste, les autres cas étant similaires. L'algorithme calcule simultanément pour tous les états la probabilité minimale (disons $\boldsymbol{\pi}_{min}(s) = Inf(\{\Pr^{St}(s \vDash \psi\mathcal{U}\chi)\})$) des «bons» chemins puis la compare avec a afin de déterminer les états à étiqueter.

Si un état vérifie χ, alors quelque soit la stratégie St, $\Pr^{St}(s \vDash \psi\mathcal{U}\chi) = 1$ et par conséquent $\boldsymbol{\pi}_{min}(s) = 1$. Appelons ce sous-ensemble d'états S_{good}. A partir de S_{good}, on obtient l'ensemble des états pour lesquels $\boldsymbol{\pi}_{min}(s) > 0$. Cet ensemble, noté $S_{>0}$, est obtenu en l'initialisant à S_{good} puis en l'élargissant (itérativement) avec les états qui, quelque soit la stratégie adoptée, ont une probabilité non nulle de l'atteindre en un pas : $S_{>0} \leftarrow S_{>0} \cup \{s \mid \forall \boldsymbol{\pi}^i_s, \exists s' \in S_{>0}, \boldsymbol{\pi}^i_s(s') > 0\}$. Cette procédure se termine nécessairement. Appelons $S_{bad} = S \setminus S_{>0}$. On vérifie aisément que $\forall s \in S_{bad}, \boldsymbol{\pi}_{min}(s) = 0$. Il nous reste à évaluer $S_{int} = S_{>0} \setminus S_{good}$. Cette évaluation est au coeur de la méthode et de ses extensions, aussi nous allons maintenant la détailler en démontrant sa correction.

Première observation Le vecteur $\boldsymbol{\pi}_{min}$ est solution de l'équation 7.1 où le vecteur $\mathbf{x}$ est l'inconnue.

$$\forall s \in S_{int}, \mathbf{x}(s) = Inf(\{\sum_{s' \in S_{int}} \boldsymbol{\pi}^i_s(s')\mathbf{x}(s') + \sum_{s' \in S_{good}} \boldsymbol{\pi}^i_s(s')\}_{1 \leq i \leq k_s}) \tag{7.1}$$

Preuve

Nous établissons l'égalité en démontrant l'inégalité dans les deux sens.

($\geq$) Soit St une stratégie pour le processus démarrant en s, alors

$\Pr^{St}(s \vDash \psi\mathcal{U}\chi) = \sum_{s' \in S_{int}} \boldsymbol{\pi}^{St(s)}_s(s')\Pr^{St_{s'}}(s' \vDash \psi\mathcal{U}\chi) + \sum_{s' \in S_{good}} \boldsymbol{\pi}^{St(s)}_s(s')$

avec $St_{s'}$ la stratégie définie par $St_{s'}(s', \ldots, s_n) = St(s, s', \ldots, s_n)$.

Par conséquent,

$\Pr^{St}(s \vDash \psi\mathcal{U}\chi) \geq \sum_{s' \in S_{int}} \boldsymbol{\pi}^{St(s)}_s(s')\boldsymbol{\pi}_{min}(s') + \sum_{s' \in S_{good}} \boldsymbol{\pi}^{St(s)}_s(s')$

$\geq Inf(\{\sum_{s' \in S_{int}} \boldsymbol{\pi}^{St(s)}_s(s')\boldsymbol{\pi}_{min}(s') + \sum_{s' \in S_{good}} \boldsymbol{\pi}^{St(s)}_s(s')\}_{1 \leq i \leq k_s})$

Cette dernière inégalité étant vraie pour tout St, on obtient :

$\forall s \in S_{int}, \boldsymbol{\pi}_{min}(s) \geq Inf(\{\sum_{s' \in S_{int}} \boldsymbol{\pi}^i_s(s')\boldsymbol{\pi}_{min}(s') + \sum_{s' \in S_{good}} \boldsymbol{\pi}^i_s(s')\}_{1 \leq i \leq k_s})$

($\leq$) Soit maintenant $\epsilon > 0$ alors, par définition de $\boldsymbol{\pi}_{min}$, pour tout s' il existe une stratégie $St_{s'}$ telle que $\Pr^{St_{s'}}(s' \vDash \psi\mathcal{U}\chi) \leq \boldsymbol{\pi}_{min}(s') + \epsilon$. Etant donné un état s, nous construisons une stratégie St pour le processus démarrant en s de la façon suivante. St choisit la distribution $\boldsymbol{\pi}^i_s$ qui minimise la quantité $\sum_{s' \in S_{int}} \boldsymbol{\pi}^i_s(s')\Pr^{St_{s'}}(s \vDash \psi\mathcal{U}\chi) + \sum_{s' \in S_{good}} \boldsymbol{\pi}^i_s(s')$ puis applique au prochain état s' atteint la stratégie $St_{s'}$. Par construction,

$\forall i, \Pr^{St}(s \vDash \psi\mathcal{U}\chi) \leq \sum_{s' \in S_{int}} \boldsymbol{\pi}^i_s(s')\Pr^{St_{s'}}(s' \vDash \psi\mathcal{U}\chi) + \sum_{s' \in S_{good}} \boldsymbol{\pi}^i_s(s')$

$\leq \sum_{s' \in S_{int}} \boldsymbol{\pi}^i_s(s')(\boldsymbol{\pi}_{min}(s') + \epsilon) + \sum_{s' \in S_{good}} \boldsymbol{\pi}^i_s(s')$

$\leq \epsilon + \sum_{s' \in S_{int}} \boldsymbol{\pi}^i_s(s')\boldsymbol{\pi}_{min}(s') + \sum_{s' \in S_{good}} \boldsymbol{\pi}^i_s(s')$

Par conséquent, $\boldsymbol{\pi}_{min}(s) \leq \Pr^{St}(s \vDash \psi\mathcal{U}\chi)$

$\leq \epsilon + Inf(\{\sum_{s' \in S_{int}} \boldsymbol{\pi}^i_s(s')\boldsymbol{\pi}_{min}(s') + \sum_{s' \in S_{good}} \boldsymbol{\pi}^i_s(s')\}_{1 \leq i \leq k_s})$

Cette dernière inégalité étant vraie pour ϵ arbitrairement petit établit la deuxième inégalité et conclut la preuve.

c.q.f.d. $\Diamond\Diamond\Diamond$

Deuxième observation Le vecteur $\boldsymbol{\pi}_{min}$ est *l'unique* solution de l'équation 7.1.

Preuve

Afin d'établir l'unicité, nous étudions les stratégies *markoviennes*, c'est à dire les stratégies pour

lesquelles la distribution choisie ne dépend que du dernier état du chemin d'exécution. Notons $St(s)$ la distribution choisie lorsque cet état est s. Remarquons que le comportement du processus est alors celui d'une DTMC. L'équation vérifiée par une stratégie markovienne est :

$$\forall s \in S_{int}, \Pr^{St}(s \vDash \psi \mathcal{U} \chi) = \sum_{s' \in S_{int}} \boldsymbol{\pi}_s^{St(s)}(s') \Pr^{St}(s' \vDash \psi \mathcal{U} \chi) + \sum_{s' \in S_{good}} \boldsymbol{\pi}_s^{St(s)}(s') \tag{7.2}$$

Afin de simplifier les notations, $\mathbf{x}(s)$ désignera $\Pr^{St}(s \vDash \psi \mathcal{U} \chi)$, $\mathbf{A}[s, s']$ désignera $\boldsymbol{\pi}_s^{St(s)}(s')$ et $\mathbf{b}(s)$ désignera $\sum_{s' \in S_{good}} \boldsymbol{\pi}_s^{St(s)}(s')$. L'équation 7.2 se réécrit alors sous la forme vectorielle $\mathbf{x} = \mathbf{A} \cdot \mathbf{x} + \mathbf{b}$. La quantité $\mathbf{A}^n[s, s']$ est la probabilité d'être en s' partant de s après n pas sans quitter S_{int}. D'après la définition de S_{int}, pour toute stratégie la probabilité de rester indéfiniment dans S_{int} est nulle ce qui se traduit en termes de DTMC par la convergence de la série $\sum_{n \geq 0} \mathbf{A}^n$ (voir la section 1.2). En remplaçant (n fois) dans le terme droit de l'égalité, $\mathbf{x}$ par son expression on obtient $\mathbf{x} = \sum_{i \leq n} \mathbf{A}^i \mathbf{b} + \mathbf{A}^{n+1} \mathbf{x}$. Par passage à limite, $\mathbf{x} = \sum_{n \geq 0} \mathbf{A}^n \mathbf{b}$, ce qui signifie que l'équation 7.2 admet une solution unique.

Soit maintenant $\mathbf{x}$ une solution de l'équation 7.1. Notons St la stratégie markovienne qui consiste à choisir pour un état s, la distribution $\boldsymbol{\pi}_s^i$ pour laquelle le minimum est atteint avec la solution $\mathbf{x}$. Alors $\mathbf{x}$ vérifie l'équation 7.2 correspondant à cette stratégie. Par conséquent, $\mathbf{x}(s) = \Pr^{St}(s \vDash \psi \mathcal{U} \chi)$. Nous en déduisons que $\forall s, \mathbf{x}(s) \geq \boldsymbol{\pi}_{min}(s)$. Soit maintenant St' la stratégie markovienne conduisant à $\boldsymbol{\pi}_{min}$. Nous remarquons que :
$\forall s \in S_{int}$,
$\sum_{s' \in S_{int}} \boldsymbol{\pi}_s^{St'(s)}(s')(\mathbf{x}(s') - \boldsymbol{\pi}_{min}(s')) =$
$(\sum_{s' \in S_{int}} \boldsymbol{\pi}_s^{St'(s)}(s')\mathbf{x}(s') + \sum_{s' \in S_{good}} \boldsymbol{\pi}_s^{St'(s)}(s'))$
$-(\sum_{s' \in S_{int}} \boldsymbol{\pi}_s^{St'(s)}(s')\boldsymbol{\pi}_{min}(s') + \sum_{s' \in S_{good}} \boldsymbol{\pi}_s^{St'(s)}(s'))$
$\geq \mathbf{x}(s) - \boldsymbol{\pi}_{min}(s)$

Réécrit avec les notations vectorielles précédentes, ceci s'exprime par $\mathbf{A}(\mathbf{x} - \boldsymbol{\pi}_{min}) \geq \mathbf{x} - \boldsymbol{\pi}_{min} \geq \mathbf{0}$. En itérant, on obtient $\mathbf{A}^n(\mathbf{x} - \boldsymbol{\pi}_{min}) \geq \mathbf{x} - \boldsymbol{\pi}_{min} \geq \mathbf{0}$. Et finalement par passage à la limite, $\mathbf{x} - \boldsymbol{\pi}_{min} = \mathbf{0}$ ce qui établit cette observation.

c.q.f.d. ◊◊◊

Troisième observation Le vecteur $\boldsymbol{\pi}_{min}$ est l'unique solution du programme linéaire :

Maximiser $\sum_{s \in S_{int}} \mathbf{x}(s)$ soumis aux contraintes

$$\forall s \in S_{int}, \forall 1 \leq i \leq k_s, \mathbf{x}(s) \leq \sum_{s' \in S_{int}} \boldsymbol{\pi}_s^i(s')\mathbf{x}(s') + \sum_{s' \in S_{good}} \boldsymbol{\pi}_s^i(s')$$

Preuve
Soit $\mathbf{x}$ satisfaisant les contraintes de ce programme, alors $\mathbf{x}$ satisfait la version de l'équation 7.1 où les égalités sont remplacées par des inégalités larges. Supposons de plus que $\mathbf{x}$ soit une solution optimale et que l'une des inégalités de l'équation 7.1 soit stricte (disons pour $\mathbf{x}(s)$). Alors on peut remplacer $\mathbf{x}(s)$ par le terme droit de l'inégalité en question et obtenir une meilleure solution. Par conséquent, une solution optimale vérifie l'équation 7.1 et en vertu de la deuxième observation $\boldsymbol{\pi}_{min}$ est l'unique solution de ce programme linéaire.

c.q.f.d. ◊◊◊

L'évaluation consiste donc à résoudre ce programme linéaire.
Complexité Par construction, l'algorithme a une complexité linéaire en fonction de la taille de la formule. La complexité, fonction de la taille du processus, dépend des opérateurs. Pour les opérateurs non probabilistes, la description faite ci-dessus devrait convaincre le lecteur qu'elle est à nouveau linéaire. Pour les opérateurs probabilistes, l'étape la plus coûteuse est la résolution d'un programme linéaire qui se fait en temps polynomial à l'aide des méthodes intérieures [ROO 97].

Bibliographie

[ALF 97] de Alfaro L. Model Checking of Probabilistic and Nondeterministic Systems. *STACS'97*, LNCS vol. 1200, pages 165-176, Springer-Verlag, 1997.

[ACD 91] Alur R., Courcoubetis C., Dill D. L. Model-Checking for Probabilistic Real-Time Systems. *ICALP 1991*, pages 115-126, LNCS vol. 510, Springer 1991

[ACD 93] Alur R., Courcoubetis C., Dill D. L. Model-checking in dense real-time. *Information and Computation*, 104(1) :2-34, 1993.

[AND 03] Andova S., Hermanns H., Katoen J.-P. Discrete-time rewards model-checked. *Formal Modelling and Analysis of Timed Systems(FORMATS 2003)*, LNCS vol. 2791, pages 88-103, Springer-Verlag, 2003.

[AZI 00] Aziz A., Sanwal K., V.Singhal, Brayton R. Model Checking continuous-time Markov chains. *ACM Transactions on Computational Logic*, vol. 1, n° 1, pages 162-170, 2000.

[BAI 03a] Baier C., Haverkort B., Hermanns H., Katoen J.-P. Model-Checking Algorithms for Continuous Time Markov Chains. *IEEE Transactions on Software Engineering*, vol. 29, n° 7, pages 524-541, Juillet 2003.

[BAI 03b] Baier C., Hermanns H., Katoen J.-P., Wolf V., Comparative branching-time semantics for Markov chains. *Concurrency Theory (CONCUR 2003)*, LNCS vol. 2761, pages 492-507, Springer Verlag, 2003.

[BIA 95] Bianco A., de Alfaro L. Model Checking of Probabilistic and Nondeterministic Systems. *FSTTCS 95 : Foundations of Software Technology and Theoretical Computer Science*, LNCS vol. 1026, pages 499-513, Springer-Verlag, 1995.

[COU 95] Courcoubetis C., Yannakakis M. The complexity of probabilistic verification. *Journal of the ACM*, vol. 42(4), pages 857-907, Juillet 1995.

[COU 99] Couvreur J-M. On-the-fly verification of linear temporal logic. *In Proc. of the Formal Methods'99*, LNCS vol. 1708, pages 253-271, Springer-Verlag, 1999.

[COU 03] Couvreur J.-M., Saheb N., Sutre G. An optimal automata approach to LTL model checking of probabilistic systems. *In Proc. 10th Int. Conf. Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'2003)*, LNAI vol. 2850, pages 361-375, Springer Verlag, 2003.

[EME 80] Emerson E. A., Clarke E. M. Characterizing Correctness Properties of Parallel Programs Using Fixpoints. *7^{th} International Colloquium on Automata, Languages and Programming, (ICALP)*, pages 169-181, 1980.

[EME 86] Emerson E. A., Halpern J. Y. "Sometimes" and "Not Never" revisited : on branching versus linear time temporal logic. *JACM* 33(1) : 151-178, 1986.

[ESP 06] Esparza J., Kucera A., Mayr R. Model checking probabilistic pushdown automata. *Logical Methods in Computer Science* vol. 2 (1), 2006.

[FEL 68] Feller W. An introduction to probability theory and its applications. Volume I. John Wiley & Sons, 1968, (third edition).

[FEL 71] Feller W. An introduction to probability theory and its applications. Volume II. John Wiley & Sons, 1971, (second edition).

[FOA 98] Foata D., Fuchs A. Calcul des probabilités. Dunod, 1998, Seconde édition.

[FOA 02] Foata D., Fuchs A. Processus stochastiques. Processus de Poisson, chaînes de Markov et martingales. Dunod, 2002.

[JEN 53] Jensen A. Markov chains as an aid in the study of Markov processes. *Skand. Aktuarietidskrift*, vol. 3, pages 87-91, 1953.

[KS 60] Kemeny J.G., Snell J.L. Finite Markov Chains. D. Van Nostrand-Reinhold, New York, NY, 1960.

[LMS 06] Laroussinie F., Markey N., Schnoebelen P. Efficient Timed Model Checking for Discrete-Time Systems. *Theoretical Computer Science* 353(1-3), pages 249-271, 2006.

[LS 05] Laroussinie F., Sproston J. Model Checking Durational Probabilistic Systems. *FoSSaCS 2005* pages 140-154, LNCS vol. 3441, Springer 2005

[Ledoux 96] Ledoux J. Weak lumpability of finite Markov chains and positive invariance of cones. *rapport de recherche INRIA-IRISA*, n° 2801, 1996

[PJSCH 84] Schweitzer P. J. Aggregation Methods for Large Markov Chains. *Proceedings of the International Workshop on Computer Performance and Reliability*, pages 275-286, North-Holland, 1984

[PUT 94] Puterman M. Markov decision processes : Discrete Stochastic Dynamic Programming. John Wiley & Sons inc., 1994.

[ROO 97] Roos C., Terlaky T., Vial J.-P. Theory and Algorithms for Linear Optimization. An Interior Point Approach. Wiley-Interscience, John Wiley & Sons Ltd, West Sussex, England, 1997.

[SAV 70] Savitch W. J., Relationship between nondeterministic and deterministic tape classes. *Journal of Computer and System Sciences*, 4, pages 177-192, 1970

[STE 94] Stewart W. J., Introduction to the numerical solution of Markov chains. Princeton University Press, USA, 1994.

[TAR 51] Tarski A. A Decision Method for Elementary Algebra and Geometry. Univ. of California Press, Berkeley, 1951.

[VAR 85] Vardi M. Automatic Verification of Probabilistic Concurrent Finite-State Programs. *FOCS 1985*, pages 327-338, 1985.

[YOU 05] Younes H., Kwiatkowska M., Norman G., Parker D. Numerical vs. Statistical Probabilistic Model Checking. *Int. Journal on Software Tools for Technology Transfer (STTT)*, vol. 8(3) pages 216-228, 2006.