Stage de première année

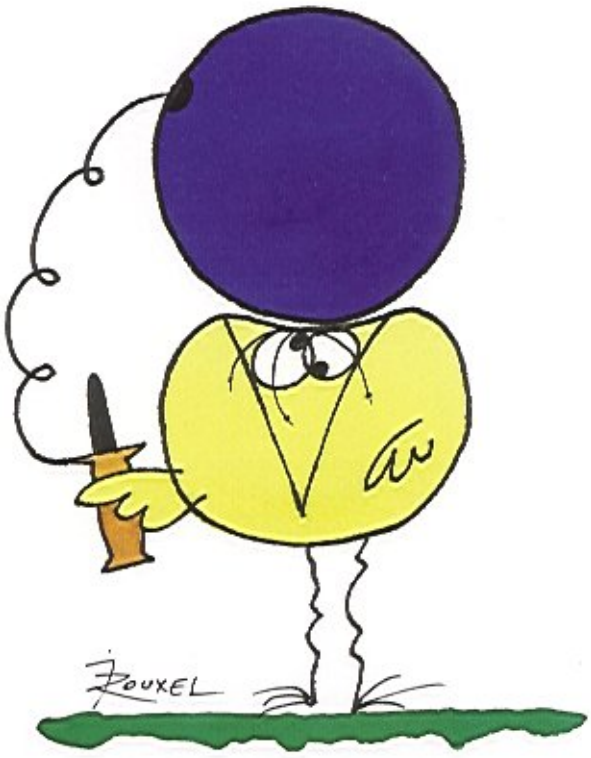
Problèmes décidables et indécidables pour les automates probabilistes

Auteur :
Engel Lefaucheux

Responsables :
M. Hugo Gimbert

Juin/Juillet 2012

Les devises Shadok



EN ESSAYANT CONTINUELLEMENT
ON FINIT PAR RÉUSSIR. DONC:
PLUS ÇA RATE, PLUS ON A
DE CHANCES QUE ÇA MARCHE.

Table des matières

Introduction

Le stage de fin de première année que l'ENS nous demande a vocation a nous faire découvrir la recherche par l'immersion dans l'équipe de notre choix. Le choix du thème est par conséquent très important. En entendant que j'étais intéressé par la théorie des jeux, mon tuteur, Dietmar Berwanger, m'a tout de suite parlé des travaux d'Hugo Gimbert. Je suis rapidement entré en contact avec ce dernier qui m'a proposé de développer l'algorithmique des automates probabilistes au cours d'un stage de 6 semaines.

Les automates probabilistes ont été introduits par M. Rabin en 1963 dans [1]. Il s'agit d'une généralisation des automates finis non déterministes. Par conséquent les langages reconnus par les automates probabilistes (les langages stochastiques) contiennent les langages rationnels. L'inclusion est stricte, en effet on peut noter que le nombre de langages stochastiques est indénombrable alors que celui des langages rationnels est dénombrable. L'algorithmique des automates probabilistes possède deux problèmes indécidables centraux : le problème du vide et le problème de la valeur isolée.
Le problème du vide est : existe-t-il un mot de probabilité supérieure à λ avec $0 \leq \lambda \leq 1$? Le problème de l'isolation est : existe-t-il des mots de probabilité arbitrairement proche de λ ?

Le problème du vide pour les automates probabilistes a été montré indécidable par A. Paz dans [2] (A. Paz réduit un problème sur les langages hors contexte). Le problème de l'isolation a été traité pour λ différent de 0 ou 1 par A. Bertoni dans [3]. Le cas $\lambda = 1$ et par symétrie $\lambda = 0$ a ensuite été montré indécidable par Y. Oualhadj et H. Gimbert dans [5].
Les recherches menées durant mon stage ont eu pour but de trouver des classes d'automates probabilistes pour lesquelles le problème du vide ou de l'isolation est décidable.

1 Les automates probabilistes

1.1 Définitions

Définition 1 : Soit $\mathcal{Q}$ un ensemble fini. Une matrice de transition sur $\mathcal{Q}$ est une matrice carrée $M \in [0,1]^{\mathcal{Q}\times\mathcal{Q}}$ telle que pour tout $q \in \mathcal{Q}$, $\sum_{r\in\mathcal{Q}} M_{q,r} = 1$.

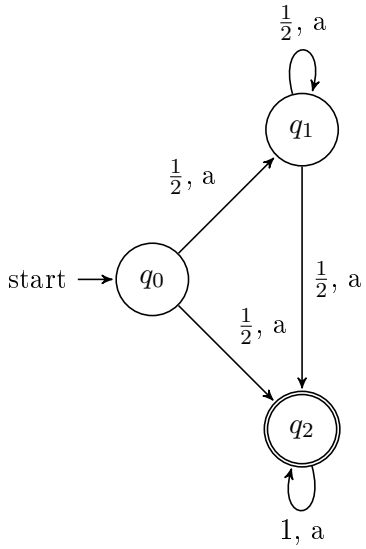
Définition 2 : Un automate probabiliste sur des mots finis $\mathcal{A}$ est défini par un quintuplet $\{\mathcal{Q}, \Sigma, \mathcal{M}, q_0, \mathcal{F}\}$, avec
- $\mathcal{Q}$ un ensemble fini d'états
- Σ l'alphabet de travail.
- $\mathcal{M} = (M_a)_{a\in\Sigma}$ où M_a est une matrice de transition.
- q_0 l'état initial
- $\mathcal{F}$ l'ensemble des états finaux.

Définition 3 : Soit $\mathcal{Q}$ un ensemble fini. On note 1_q pour $q \in \mathcal{Q}$ le vecteur ligne dont toutes les composantes valent 0 sauf q qui vaut 1.

Définition 4 : Soit $w = a_0a_1...a_n \in \Sigma^*$ un mot. Pour $R \subseteq Q$, on définit $\mathbb{P}_{\mathcal{A}}(q_0, w, R) = \sum_{r\in R} 1_q M_{a_0} M_{a_1} ... M_{a_n} (1_r)^t$.
La probabilité d'acceptation d'un mot w est $\mathbb{P}_{\mathcal{A}}(w) = \mathbb{P}_{\mathcal{A}}(q_0, w, \mathcal{F})$.

1.2 Langage reconnu par un automate probabiliste

Définition 5 : Un point de coupure est une valeur $\lambda \in [0;1]$.
Le langage reconnu par l'automate $\mathcal{A}$ et le point de coupure λ est l'ensemble $L_{\mathcal{A},\lambda} = \{w \in \Sigma^* | \mathbb{P}_{\mathcal{A}}(w) \geq \lambda\}$.



Exemple 1 :

Pour cet automate, la matrice de transition de a est

$$M_a = \begin{pmatrix} 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 1 \end{pmatrix}$$

le mot a^n a une probabilité $1 - (\frac{1}{2})^n$. Par conséquent le langage reconnu par cet automate et un point de coupure λ tel que $1 - (\frac{1}{2})^m \leq \lambda \leq 1 - (\frac{1}{2})^{m+1}$ est $\{a^n | n > m\}$.

Définition 6 : Un point de coupure λ est dit isolé s'il existe ϵ tel que

$$\forall w \in \Sigma^*, |\mathbb{P}_{\mathcal{A}}(w) - \lambda| \geq \epsilon.$$

Cette notion de point de coupure isolé a été introduite par M. Rabin dans son article [1]. L'intérêt des points de coupure isolé vient du théorème suivant :

Théorème 1 (M. Rabin, 1963) : Soient $\mathcal{A}$ un automate probabiliste et λ un point de coupure isolé. Alors il existe un automate déterministe $\mathcal{B}$ tel que $L_{\mathcal{A},\lambda} = L_{\mathcal{B}}$. Par ailleurs si $\mathcal{A}$ a n états et λ est ϵ-isolé alors on peut choisir $\mathcal{B}$ tel que $\mathcal{B}$ ait e états où e vérifie :

$$e \leq (1 + \frac{1}{\epsilon})^{n-1}.$$

2 Le problème du vide

2.1 État de l'art

Il existe à ce jour plusieurs démonstrations de l'indécidabilité du vide pour les automates, l'original étant par A. Paz dans [2] (pour d'autres démonstrations voir [4] et [5]).
Des travaux ont aussi été réalisés pour savoir à partir de combien d'états probabilistes le problème du vide était indécidable. On trouve dans [6] les théorèmes :

Théorème 2 : Le problème du vide pour les automates ayant au plus un état probabiliste est décidable.

Théorème 3 : Le problème du vide pour les automates ayant deux états probabilistes est indécidables.

2.2 Les automates DAG

Définition 7 : Un automate DAG est un automate probabiliste sans cycle.

Le théorème suivant a été établi au cours de mes recherches mais il était déjà connu (voir [6]).

Théorème 4 : Le problème du vide est décidable pour les automates DAG.

Démonstration : L'automate n'ayant pas de cycle, on peut se le représenter avec une relation de parenté comme dans un arbre (à ceci près qu'un nœud peut avoir plusieurs parents). Par conséquent, il existe un nombre fini de mot étiquetant les chemins allant de l'état initial (racine) aux état finaux (feuilles).
Il suffit alors de tester ce nombre fini de mot pour savoir si le langage reconnu est non vide.

2.3 Une classe indécidable : les automates quasi acyclique

Les automates DAG étant décidables, j'ai voulu trouver une classe légèrement supérieure aux automates DAG pour l'étudier, j'ai ainsi approfondi le cas des automates quasi acycliques.

Définition 8 : Un automate quasi acyclique est un automate probabiliste sans cycle hormis les boucles.

Mais le seul ajout des boucles rend le problème indécidable. Le théorème suivant a pu être formulé en s'inspirant de la démonstration de l'indécidabilité du problème de l'égalité pour les automates simples (automates dont les transitions sont 0, $\frac{1}{2}$ ou 1) par A. Bertoni.

Théorème 5 : Le problème du vide pour les automates quasi acycliques est indécidable.

Démonstration :

On procède en deux étapes : on réduit d'abord le problème de correspondance de Post au problème de l'égalité pour les automates quasi acyclique, puis on réduit ce problème de l'égalité au problème du vide des automates quasi acycliques.

Première étape :

Une instance du problème de correspondance de Post (PCP en abrégé) est la donnée d'un entier m ≥ 1 et de deux suites $u_1, \ldots, u_m$ et $v_1, \ldots, v_m$ de chacune m mots sur un alphabet A. On dit qu'une instance du problème de Post a une solution s'il existe une suite finie $i_1, \ldots, i_n$ d'entiers dans l'intervalle [1,m] telle que

$$u_{i_1} u_{i_2} \ldots u_{i_n} = v_{i_1} v_{i_2} \ldots v_{i_n}$$

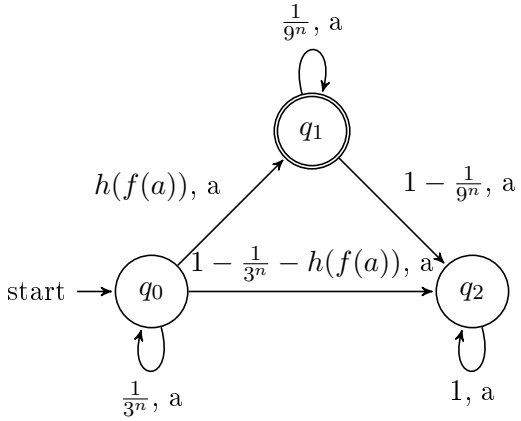
où $u_{i_1} u_{i_2} \ldots u_{i_n}$ et $v_{i_1} v_{i_2} \ldots v_{i_n}$ désignent respectivement la concaténation des n mots $u_{i_1}, u_{i_2} \ldots, u_{i_n}$ et la concaténation des n mots $v_{i_1}, v_{i_2}, \ldots, v_{i_n}$.
Ce problème est connu comme étant indécidable.

Comme il n'y a pas de cycle de plus d'un état, on peut ordonner les états $q_0, ..., q_n$ de façon à ce que $q_i \to q_k \Rightarrow k \geq i$.
Ainsi les matrices M_a (pour toute lettre a) sont triangulaires supérieures.
Montrons que le problème de l'égalité est indécidable en réduisant le problème de correspondance de Post.
Soient f, g deux fonctions de Σ vers $\{1;2\}^*$ représentant une instance de PCP.
Soit h : $\{0;1\}^* \to [0; \frac{2}{3}]$ définie par $h(a_1 \ldots a_n) = \frac{a_1}{3^{2n-1}} + \ldots + \frac{a_n}{3^n}$
La fonction h est injective.

On construit l'automate H à trois états où $q = 0$ est initial, q_1 est acceptant et q_2 est un état puits.
Pour tout a $\in \Sigma$, on choisit la matrice $M_a =$

$$\begin{pmatrix} \frac{1}{3^n} & h(f(a)) & 1 - \frac{1}{3^n} - h(f(a)) \\ 0 & \frac{1}{9^n} & 1 - \frac{1}{9^n} \\ 0 & 0 & 1 \end{pmatrix}$$

où n = |f(a)|.
Graphiquement on a :



Par récurrence, on obtient $M(a_1 \dots a_n) =$

$$\begin{pmatrix} \frac{1}{3^m} & h(f(a_1 \dots a_n)) \\ 0 & \frac{1}{9^m} \end{pmatrix}$$

où m = |f($a_1 \dots a_n$)|.
On a : $M_{ab} = M_a M_b \neq M_{ba}$ par injectivité de h.

L'automate H accepte w avec une probabilité h(f(w)).
On construit l'automate H' en remplaçant f par g et en échangeant les états acceptants et rejetants. L'automate H' accepte w avec une probabilité 1-h(g(w)).
On construit ensuite l'automate H" en ajoutant un état supplémentaire initial amenant à H et H' avec une probabilité $\frac{1}{2}$ en lisant #. L'automate H" accepte #w avec la probabilité $\frac{(1-h(f(w))+h(g(w)))}{2}$.
Donc H" accepte #w avec la probabilité $\frac{1}{2}$ si et seulement si h(f(w)) = h(g(w)) ce qui est équivalent à f(w) = g(w) car h est injective.
Le problème de l'égalité est donc indécidable sur les automates quasi acycliques.

Deuxième étape :
Soit $\mathcal{H}_1 = \{\mathcal{Q}_1, \Sigma, \mathcal{M}_1, q_1, F_1\}$ et $\mathcal{H}_2 = \{\mathcal{Q}_2, \Sigma, \mathcal{M}_2, q_2, F_2\}$ deux automates probabilistes. On construit l'automate $\mathcal{H}_3 = \{\mathcal{Q}_3, \Sigma, \mathcal{M}_3, q_3, F_3\}$ tel que :

- $\mathcal{Q}_3 = \mathcal{Q}_1 \times \mathcal{Q}_2$.
- $q_3 = (q_1, q_2)$.
- $F_3 = F_1 \times F_2$
- $\mathcal{M}_3$ est de sorte que si on peut passer de q_1 à q_1' dans $\mathcal{H}_1$ avec une probabilité p en lisant a et de q_2 à q_2' dans $\mathcal{H}_2$ avec une probabilité p', alors on passe de (q_1,q_2) à (q_1', q_2') avec une probabilité pp'.

On a alors $\forall w \in \Sigma^*, \mathbb{P}_{\mathcal{H}_3}(w) = \mathbb{P}_{\mathcal{H}_1}(w)\mathbb{P}_{\mathcal{H}_2}(w)$.
En effet, soit $w = a_1...a_n \in \Sigma^*, q \in \mathcal{Q}_1, q' \in \mathcal{Q}_2$.

$$\begin{aligned}\mathbb{P}_{\mathcal{H}_3}(q_3, w, (q, q')) &= 1_{(q_1,q_2)}.M^{a_1}_{\mathcal{H}_1\times\mathcal{H}_2}...M^{a_n}_{\mathcal{H}_1\times\mathcal{H}_2}.(1_{(q,q')})^t \\ &= (1_{(q_1)}.M^{a_1}_{\mathcal{H}_1}...M^{a_n}_{\mathcal{H}_1}.(1_q)^t).(1_{(q_2)}.M^{a_1}_{\mathcal{H}_2}...M^{a_n}_{\mathcal{H}_2}.(1_{q'})^t) \\ &= \mathbb{P}_{\mathcal{H}_1}(q_1, w, q).\mathbb{P}_{\mathcal{H}_2}(q_2, w, q')\end{aligned}$$

On appelle $\mathcal{Q}_3$ le produit cartésien de $\mathcal{Q}_1$ et de $\mathcal{Q}_2$.
Donc en construisant le produit cartésien $\mathcal{G}$ de l'automate $\mathcal{H}$ et de son conjugué, conjugué qui a les mêmes transitions mais échange les états acceptants et non acceptants, on a pour tout mot $w \in \Sigma^*$, $\mathbb{P}_{\mathcal{G}}(w) = (\mathbb{P}_{\mathcal{H}}(w))(1-\mathbb{P}_{\mathcal{H}}(w))$.
Or la fonction f(x) = x(1-x) atteint son maximum $\frac{1}{4}$ en $\frac{1}{2}$. Donc
$\mathbb{P}_{\mathcal{H}}(w) = \frac{1}{2} \Leftrightarrow \mathbb{P}_{\mathcal{G}}(w) \geq \frac{1}{4}$.
Ainsi le problème du vide est indécidable.

Remarque : Une construction (mise en annexe 1) permet de passer du problème du vide au sens large au problème du vide au sens strict.

2.4 Les automates à point de coupure isolé

Le cas des automates à point de coupure isolé est intéressant du fait qu'il existe un automate déterministe reconnaissant le même langage. Or le problème du vide est décidable pour les automates déterministes. Une question intéressante à résoudre est donc : Pour un automate déterministe $\mathcal{B}$, un automate probabiliste $\mathcal{A}$ et un point de coupure isolé λ donné peut-on décider de l'égalité $\mathcal{L}_{\mathcal{B}} = \mathcal{L}_{\mathcal{A},\lambda}$?
J'ai obtenu le théorème plus faible suivant :

Théorème 6 : Connaissant un automate déterministe $\mathcal{B}$, $\varepsilon \in [0; 1]$, un automate probabiliste $\mathcal{A}$ et un point de coupure ε-isolé λ, on peut décider de l'égalité $\mathcal{L}_{\mathcal{B}} = \mathcal{L}_{\mathcal{A},\lambda}$.

Démonstration : Comme nous connaissons le nombre d'états de $\mathcal{A}$ ainsi que ε, le théorème 1 nous donne une borne h telle qu'il existe un automate déterministe $\mathcal{C}$ reconnaissant le même langage que ($\mathcal{A}$, λ) et ayant moins de h états.
Par ailleurs, le plus petit mot distinguant deux automates déterministes est de taille au plus le produit des états de chaque automate (Annexe 2). Soit m le nombre d'états de $\mathcal{B}$, le mot le plus petit différenciant $\mathcal{B}$ et $\mathcal{C}$ est donc de taille au plus p = mh. Il existe un nombre fini de mots de taille inférieure à p, on peut donc calculer :
E= $\{w \in \Sigma^* | \ |w| \leq p$ et w est accepté par $\mathcal{B}$ ou par ($\mathcal{A}$, λ) mais pas par les deux$\}$.
On a alors l'équivalence :
$\mathcal{L}_{\mathcal{B}} = \mathcal{L}_{\mathcal{A},\lambda} \Leftrightarrow$ E est vide.

Remarque : La supposition dans ce théorème que l'on connait ε est loin d'être négligeable comme nous le verrons dans la partie suivante.

Corollaire : Soit $\varepsilon \in [0;1]$, le problème du vide est décidable pour les automates probabilistes avec point de coupure ε-isolé.

Démonstration : On applique le théorème précédent à l'automate probabiliste et au point de coupure ε-isolé donné en le comparant à un automate déterministe reconnaissant le langage $\emptyset$. Il y a égalité des langages si et seulement si l'automate probabiliste ne reconnait aucun mot.

3 Le problème de l'isolation

3.1 État de l'art

Les travaux de A. Bertoni, Y. Oualhadj et H. Gimbert dans [3] et [5] ont établi le théorème suivant :

Théorème 7 : Pour tout $0 \leq \lambda \leq 1$, le problème de l'isolation de λ est indécidable.

Des approfondissements de cette question ont été réalisés. L'article [7] montre que l'indécidabilité a lieu dès qu'il y a un état probabiliste. Il expose également une sous-classe des automates probabilistes décidables pour le problème de la valeur 1 (C'est à dire l'isolation pour le cas $\lambda = 1$).

3.2 Indécidabilité de l'ε-isolation

Le théorème 6 suppose que nous disposons d'un oracle nous donnant la valeur ε telle que le point de coupure soit ε-isolé. Le problème est plus faible que le problème de l'isolation, en effet on sait d'avance que le point de coupure est isolé, il ne reste qu'à trouver un ε approprié. Malheuresement ce problème reste indécidable.

Théorème 8 : Soient λ autre que 0 ou 1 et ε tels que $\lambda - \varepsilon > 0$ ou $\lambda + \varepsilon < 1$. Alors le problème de l'ε-isolation pour un automate A donné de λ est indécidable.

Démonstration : Réduisons le problème du vide au sens large pour le point de coupure λ (problème indécidable si λ est autre que 0 et 1).
Nous supposons par la suite que $\lambda - \varepsilon > 0$. Dans le cas contraire, l'automate complémentaire B a son point de coupure $1 - \lambda$ ε-isolé si et seulement si λ est ε-isolé dans A. Par ailleurs $1 - \lambda - \varepsilon > 0$ car $\lambda + \varepsilon < 1$. On réduit alors le problème du vide à l'ε-isolation de $1 - \lambda$.

Par la transformation suivante on déplace les termes de probabilités supérieures à λ dans l'intervalle $[\lambda - \varepsilon; \lambda + \varepsilon]$ et les mots de probabilités strictement inférieures à λ deviennent strictement inférieures à $\lambda - \varepsilon$:
Comme $\lambda - \varepsilon > 0$, il existe $\alpha > 0$ tel que $\lambda - \varepsilon - \alpha\varepsilon\lambda > 0$. On construit un automate B qui doit d'abord lire une lettre #. Cette lettre envoie avec probabilité $\alpha\varepsilon$ sur l'état initial de A et avec une probabilité $\lambda - \varepsilon - \alpha\varepsilon\lambda$ sur un état acceptant.
L'automate A accepte w avec probabilité p si et seulement si l'automate B accepte #w avec probabilité $p' = \lambda - \varepsilon - \alpha\varepsilon\lambda + \alpha\varepsilon p$.
Ainsi $p \in [\lambda; 1] \Leftrightarrow p' \in [\lambda - \varepsilon; \lambda - \varepsilon + \alpha\varepsilon(1 - \lambda)]$.
Par conséquent, A reconnait un mot w avec le point de coupure λ si

et seulement si λ n'est pas ε-isolé dans B.
Le problème de l'ε-isolation est donc indécidable.

Remarque : Si le ε donné ne vérifie aucune des deux inégalités demandés alors le problème est trivialement décidable car l'espace $[\lambda - \varepsilon; \lambda + \varepsilon]$ contient le segment $[0; 1]$.

Cette démonstration ne peut s'étendre aux cas $\lambda = 0$ et $\lambda = 1$. Le problème reste néanmoins indécidable.

Théorème 9 : Soit $\varepsilon < 1$ alors le problème de l'ε-isolation de 1 est indécidable.

Démonstration : Soit $\varepsilon < 1$.
Pour tout point de coupure λ autre que 0 et 1, le problème du vide pour le point de coupure λ est indécidable. Par conséquent, le problème du vide est indécidable pour le point de coupure $\lambda = 1 - \varepsilon$.
Par ailleurs, 1 est ε-isolé dans l'automate $\mathcal{A}$ si et seulement si l'automate $\mathcal{A}$ reconnait un mot avec une probabilité supérieure à $1-\varepsilon$. Donc l'ε-isolation de 1 est indécidable.

Remarque : On obtient le cas $\lambda = 0$ en appliquant le théorème précédent à l'automate conjugué.

3.3 Monoïde de Markov : définitions et conjectures

Définition 9 : Un mot limite est une fonction $\mathbf{u} : \mathcal{Q}^2 \to \{0; 1\}$ telle que $\forall s \in \mathcal{Q}, \exists t \in \mathcal{Q}, \mathbf{u}(s, t) = 1$.

Définition 10 : Soit $\mathbf{u}$ un mot limite, un état s est $\mathbf{u}$-récurrent si pour tout état t on a $\mathbf{u}(s, t) = 1 \Rightarrow \mathbf{u}(t, s) = 1$.

On supposera par la suite que l'automate d'entrée $\mathcal{A}$ est complet. On peut ainsi former les mots limites $\mathbf{a}$ induits par les lettres $a \in \Sigma$ définis par :

$$\forall s, t \in \mathcal{Q}, (\mathbf{a}(s, t) = 1 \Leftrightarrow \mathbb{P}_{\mathcal{A}}(s, a, t) > 0).$$

Nous construirons des mots limites à partir des deux méthodes suivantes :
- *Concaténation de deux mots limites :* La concaténation de deux mots limites $\mathbf{u}$ et $\mathbf{v}$ est le mot limite $\mathbf{uv}$ tel que pour tout $s, t \in \mathcal{Q}$,

$$\mathbf{uv}(s, t) = 1 \Leftrightarrow \exists q \in \mathcal{Q}, \mathbf{u}(s, q) = 1 \text{ et } \mathbf{v}(q, t) = 1.$$

– *itération d'un mot limite idempotent :* L'itération d'un mot limite $\mathbf{u}$ n'est définie que si ce mot est idempotent (i.e $\mathbf{uu} = \mathbf{u}$). On note l'itération $\mathbf{u}^{\#}$ et on a :

$$\mathbf{u}^{\#}(s,t) = 1 \Leftrightarrow \mathbf{u}(s,t) = 1 \text{ et } t \text{ est } \mathbf{u}\text{-récurrent.}$$

Définition 11 : Le monoïde de Markov associé à un automate $\mathcal{A}$ est le plus petit ensemble de mots limites contenant $\{\mathbf{a} \mid a \in \Sigma\}$, le mot limite identité ε et fermé par la concaténation et l'itération.

Définition 12 : Soit $\mathcal{A}$ un automate probabiliste, le monoïde de Markov M associé possède une preuve de valeur 1 s'il contient un mot limite $\mathbf{u}$ tel que pour tout $s \in \mathcal{Q}$,

$$\mathbf{u}(i,s) = 1 \Rightarrow s \in \mathcal{F}.$$

Définition 13 : On dit que deux automates $\mathcal{A}$ et $\mathcal{B}$ sont équivalents en support et on note $\mathcal{A} \equiv_S \mathcal{B}$ si

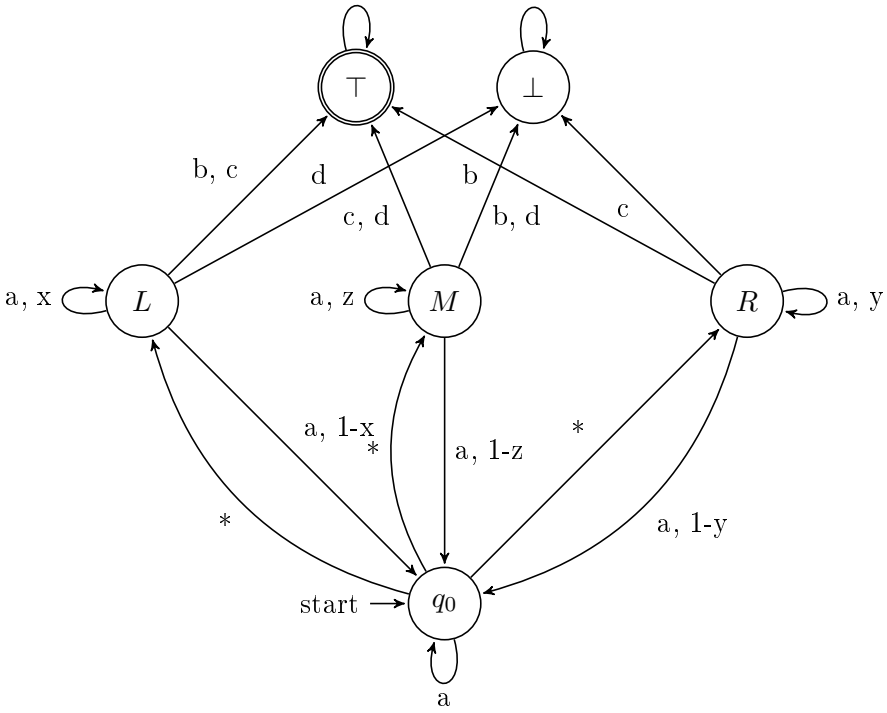
$$\forall s,t \in \mathcal{Q}, a \in \Sigma, (\mathbb{P}_{\mathcal{A}}(s,a,t) > 0 \Leftrightarrow \mathbb{P}_{\mathcal{B}}(s,a,t) > 0).$$

Quel lien existe-t-il entre la preuve de valeur 1 du monoïde de Markov et la propriété de valeur 1 de l'automate (i.e il existe des mots de probabilité arbitrairement proche de 1 dans l'automate) ?
La conjecture de départ était :

$$\forall \mathcal{A}' \equiv_S \mathcal{A}, \exists (u_n)_{n\in\mathbb{N}} \in (\Sigma^*)^{\mathbb{N}}, \mathbb{P}_{\mathcal{A}'}(u_n) \to_{n\to\infty} 1$$

$$\Longleftrightarrow \text{Le monoïde associé à } \mathcal{A} \text{ a une preuve de valeur 1.}$$

Nathanaël Fijalkow a montré que cette conjecture était fausse grâce au contre-exemple suivant :



En effet, pour cet automate, le monoïde associé ne possède pas de preuve de valeur 1.
En revanche, quelles que soient les probabilités x, y et z, on a une suite de mots dont la probabilité tend vers 1. En effet, on a dans tous les cas une des trois inégalités suivantes :
x + y > z, x + z > y ou y + z > x.
Dans le premier cas, pour tout $\varepsilon > 0$ il existe une suite $(n_i)_{i\in\{0...k\}}$ telle que le mot $w = *a^{n_0}b*a^{n_1}b...*a^{n_k}b$ ait une probabilité d'être accepté supérieure à ε. Les deux autres cas sont similaires. L'automate a donc valeur 1.
On réalise des suites similaires dans les autres cas.

La conjecture est ainsi devenue :

Conjecture : $\exists(u_n)_{n\in\mathbb{N}} \in (\Sigma^*)^{\mathbb{N}}, \forall \mathcal{A}' \equiv_S \mathcal{A}, \mathbb{P}_{\mathcal{A}'}(u_n) \to_{n\to\infty} 1 \iff$
Le monoïde associé à $\mathcal{A}$ a une preuve de valeur 1.

La démonstration n'a pas encore abouti, la réciproque ainsi qu'une piste pour la preuve du sens direct sont mis en annexe 3.

Conclusion

La découverte d'une classe très restrictive d'automates probabilistes indécidables pour le problème du vide s'avère être un blocage important pour perpétuer dans cette voie.
À l'inverse, le problème de la valeur 1 peut se développer : certaines classes importantes d'automates sont décidables pour la valeur 1 et celles-ci présentent une preuve de valeur 1 dans leur monoïde de Markov. Il est donc naturel de savoir précisément les informations apportées par le monoïde.

Ce stage a été une expérience fortement enrichissante. Bien qu'en un mois il soit difficile de réaliser un travail important, ce stage permet d'avoir un aperçu sur le métier de chercheur. Le plus grand choc est d'affronter un problème nouveau : scolairement, on nous présente des problèmes pour lesquels nous sommes plus ou moins guidés pas à pas vers la réponse. Ici, toutes les méthodes sont envisageables pour résoudre la question et par conséquent, il faut une motivation d'autant plus forte pour y arriver.

Références

[1] Michael O. Rabin. *Probabilistic Automata.* Information and Control, 6(3) : 230-245, 1963

[2] Azaria Paz. *Introduction to probabilistic automata (Computer science and applied mathematics).* Academic Press, Inc., Orlando, FL, USA, 1971.

[3] Alberto Bertoni, Giancarlo Mauri et Mauro Torelli. *Some recursive unsolvable problems relating to isolated cutpoints in probabilistic automata.* Proceedings of the Fourth Colloquium on Automata, Languages and Programming, pages 87-94, London, UK, 1977. Springer-Verlag.

[4] Omid Madani, Steve Hanks et Anne Condon. *On the undecidability of probabilistic planning and related stochastic optimization problems*, Artificial Intelligence, 147 :5-34, 2003.

[5] Hugo Gimbert, Youssouf Oualhadj. *Probabilistic Automata on Finite Words : Decidable and Undecidable Problems*, ICALP (2), 527-538, 2010

[6] Youssouf Oualhadj. *Automates probabilistes : problèmes décidables et indécidables*, mémoire de stage, 2009.

[7] Hugo Gimbert, Youssouf Oualhadj, Nathanaël Fijalkow. *Deciding the value 1 problem of probabilistic leaktight automata*, LICS, 2012.

Annexe 1 :

Énoncé : Le problème du vide strice est indécidable pour les automates quasi-acycliques.

Démonstration : Nous reprenons ici les mêmes notations que dans la démonstration du théorème 5.

Toutes les transitions de l'automate $\mathcal{G}$ sauf celle quittant l'état initial sont des sommes de multiples de $\frac{1}{9}$ (la première étant $\frac{1}{4}$). Par conséquent, on peut construire un automate $\mathcal{A}$ reconnaissant un mot avec la probabilité x si et seulement si $\mathcal{G}$ reconnait un mot avec la probabilité x et dont les transitions sont des multiples de $\frac{1}{9}$ (sauf la première qui reste $\frac{1}{4}$). Par conséquent, dans $\mathcal{A}$, on a pour tout mot w tel que $|w| = n + 1$,

$$\mathbb{P}_{\mathcal{A}}(w) \geq \frac{1}{4} \Leftrightarrow \mathbb{P}_{\mathcal{A}}(w) > \frac{1}{4} - \frac{1}{4.9^n}.$$

Et donc, en ajoutant quatre états q_0, q_1, q_2 et q_3, on forme l'automate $\mathcal{B}$ tel que :

- L'état q_0 est l'état initial, il mène en lisant $\#$ avec une probabilité $\frac{1}{2}$ à l'état initial de $\mathcal{A}$ ou à q_1.
- L'état q_1 mène avec une probabilité $\frac{1}{4}$ à l'état q_2 et $\frac{3}{4}$ à q_3 en lisant $\#$.
- L'état q_2 est acceptant, il mène à l'état q_2 avec une probabilité $\frac{1}{9}$ et à q_3 avec une probabilité $\frac{8}{9}$.
- L'état q_3 est un état puit.

Ainsi l'automate $\mathcal{B}$ accepte le mot $\#\#w$ où $|w| = n$ avec une probabilité $\frac{1}{2}(\mathbb{P}_{\mathcal{A}}(\#w) + \frac{1}{4.9^n})$.
Donc $\mathbb{P}_{\mathcal{A}}(\#w) \geq \frac{1}{4} \Leftrightarrow \mathbb{P}_{\mathcal{B}}(\#\#w) > \frac{1}{8}$.

Annexe 2 :

Énoncé : Soient $\mathcal{A}$, $\mathcal{B}$ deux automates déterministes ayant respectivement n et m états. Le plus petit mot distinguant $\mathcal{A}$ et $\mathcal{B}$, s'il existe, est de taille au plus nm.

Démonstration : Soit $\mathcal{B}'$ (respectivement de $\mathcal{A}'$) l'automate conjugué de $\mathcal{B}$ (resp. de $\mathcal{A}$). On pose m le nombre d'états de $\mathcal{B}'$.

On construit $\mathcal{C}$ (resp. de $\mathcal{C}'$) l'automate intersection de $\mathcal{A}$ et de $\mathcal{B}'$ (resp. de $\mathcal{A}'$ et de $\mathcal{B}$). Alors $\mathcal{C}$ possède nm états.

Soit $\mathcal{D}$ l'automate union de $\mathcal{C}$ et de $\mathcal{C}'$. Alors $\mathcal{D}$ a 2nm états.

Le plus petit mot distinguant $\mathcal{A}$ et $\mathcal{B}$ est le plus petit mot reconnu par $\mathcal{D}$. Par ailleurs, le plus petit mot accepté par un automate déterministe est de taille inférieure au nombre d'états de l'automate car ce mot n'emprunte pas de cycle. Donc $\mathcal{L}_{\mathcal{D}} = \emptyset$ ou $\mathcal{D}$ reconnait un mot w de

taille inférieure à 2nm.
Ainsi on a $\mathcal{L}_\mathcal{A} \neq \mathcal{L}_\mathcal{B}$ si et seulement si le plus petit mot les distinguant est de taille inférieure à 2nm.

Annexe 3 :

Énoncé : Piste pour l'étude du monoïde de Markov

Réciproque Soit $\mathcal{A}$ un automate. Soit $\mathbf{u}$ un mot limite du monoïde associé à $\mathcal{A}$, alors il existe une suite $(u_n)_{n\in\mathbb{N}}$ telle que pour tous états s et t, la suite $(\mathbb{P}_\mathcal{A}(s,u_n,t))_{n\in\mathbb{N}}$ converge et $\mathbf{u}(s,t)=1 \Leftrightarrow lim_{n\to\infty}\mathbb{P}_\mathcal{A}(s,u_n,t) > 0$. On dit que $(u_n)_{n\in\mathbb{N}}$ réifie $\mathbf{u}$.

Démonstration : On opère par induction structurelle.

- Si $\mathbf{u}$ est construit à partir de $u \in \Sigma$, alors par définition u réifie $\mathbf{u}$.
- Si $\mathbf{u} = \mathbf{vw}$ où $\mathbf{v}$ et $\mathbf{w}$ sont deux mots limites, alors il existe $(v_n)_{n\in\mathbb{N}}$ et $(w_n)_{n\in\mathbb{N}}$ réifiant $\mathbf{v}$ et $\mathbf{w}$. On note $(u_n)_{n\in\mathbb{N}}$ la suite telle que $\forall n \in \mathbb{N}, u_n = v_n w_n$.
  Ainsi $(u_n)_{n\in\mathbb{N}}$ réifie $\mathbf{u}$ car pour tous états s et t on a :
  $$\mathbb{P}_\mathcal{A}(s,u_n,t) = \sum_{r\in\mathcal{Q}} \mathbb{P}_\mathcal{A}(s,v_n,r)\mathbb{P}_\mathcal{A}(r,w_n,t)$$
  et par définition de la concaténation de deux mots limites.
- Si $\mathbf{u} = \mathbf{v}^\#$ où $\mathbf{v}$ est un mot limite idempotent, alors par induction il existe $(v_n)_{n\in\mathbb{N}}$ réifiant $\mathbf{v}$. On notera $\mathrm{V} \in [0;1]^{\mathcal{Q}^2}$ la matrice telle que pour tous états s et t, $\mathrm{V}(s,t) = \lim_{n\to\infty}\mathbb{P}_\mathcal{A}(s,v_n,t)$.
  L'espace $[0;1]^{\mathcal{Q}^2}$ étant compact, il existe une fonction ϕ telle que la suite de matrices $(\mathrm{V}^{\phi(n)})_{n\in\mathbb{N}}$ converge vers une matrice Z. Cette matrice possède une propriété de pseudo Z-récurrence :
  $$\forall s,t \in \mathcal{Q}, (\mathrm{Z}(s,t) > 0 \Rightarrow (\forall r \in \mathcal{Q}, \mathrm{Z}(t,r) > 0 \Rightarrow \mathrm{Z}(r,t) > 0)). \qquad (*)$$
  Comme $(v_n)_{n\in\mathbb{N}}$ converge en tant que matrice associée vers V et par continuité du produit matriciel, pour tout k $\in \mathbb{N}$, la suite de matrices $(v_n^k)_{n\in\mathbb{N}}$ converge vers V^k. Par conséquent il existe une fonction Ψ telle que $\forall k \in \mathbb{N}, ||\mathrm{V}^k - v^k_{\Psi(n)}||_\infty < \frac{1}{k}$. Donc la suite
  $(z_n)_{n\in\mathbb{N}} = (v^{\phi(n)}_{\Psi(\phi(n))})_{n\in\mathbb{N}}$ converge vers Z.
  La suite $(z_n)_{n\in\mathbb{N}}$ réifie u. En effet :
  $$\begin{aligned}
  \mathbf{v}^\#(s,t) = 1 &\Leftrightarrow t \text{ est } \mathbf{v}\text{-récurrent et } \mathbf{v}(s,t) = 1 && (1)\\
  &\Leftrightarrow t \text{ est pseudo V-récurrent et } \mathrm{V}(s,t) > 0 && (2)\\
  &\Leftrightarrow t \text{ est pseudo Z-récurrent et } \mathrm{Z}(s,t) > 0 && (3)\\
  &\Leftrightarrow \mathrm{Z}(s,t) > 0 && (4)\\
  &\Leftrightarrow \lim_{n\to\infty} z_n(s,t) > 0 && (5)
  \end{aligned}$$

où (1) est dû à la définition de l'itération, (2) est vrai car $(u_n)_{n\in\mathbb{N}}$ réifie **u**, (3) vient du fait que Z, étant l'itérée de V, elle a les mêmes états récurrents, (4) vient de (*) et (5) découle de la construction de $(z_n)_{n\in\mathbb{N}}$.

Par induction, on en déduit le résultat voulu. Une conséquence immédiate étant que si **u** est une preuve de valeur 1 du monoïde, alors il existe une suite $(u_n)_{n\in\mathbb{N}}$ réifiant **u**, donc telle que la suite $(\mathbb{P}_{\mathcal{A}}(u_n))_{n\in\mathbb{N}}$ tend vers 1.

Sens direct : Cette démonstration est encore incomplète.

Soit $(u_n)_{n\in\mathbb{N}}$ tel que $p(u_n) \to_{n\to\infty} 1$.
On construit le langage L à partir de $L' = \Sigma^*$ ainsi :
Si $L' = a \in \Sigma$, alors L $= a$.
Si $L' = L'_1 L'_2$ alors on applique la construction sur L'_1 et L'_2 et
L $= L_1 L_2$.
Si $L' = L'_1 + L'_2$ alors L'_1 ou L'_2 (ou les deux) contient une infinité de termes de la suite. L $= L_i$ où L_i contient une infinité de termes.
Si $L' = (L_1)^*$ et $L_1 = a \in \Sigma$, alors s'il existe n tel que la suite contienne une infinité de a^n, on prend L $= a^n$. Sinon on assure l'idempotence en prenant k tel q'il y ait une infinité de u_n dans
L $= a^k(a^N)^*$ où N est le nombre d'états de A.
Si $L' = (L_1)^*$ et $L_1 = L_2 + L_3$ alors soit il existe une infinité de termes utilisant un nombre fini d'échanges entre L_j et L_i (disons k), on peut alors prendre L' de la forme $(L_i)^*(L_j)^*...(L_i)^*(L_j)^*$ en ayant k itérations et on étudie ce nouveau L' ; Soit il y a une infinité d'interversions et on prend $L' = (L_2^* L_3^*)^*$.
Si $L' = (L'_1)^*$ et $L'_1 = L'_2 L'_3$, alors par induction sur L'_2 et L'_3 on forme L_2 et L_3 et $L_1 = L_2 L_3$. S'il existe n tel que la suite contienne une infinité de L_1^n, on prend L $= L_1^n$. Sinon on assure l'idempotence en prenant k tel qu'il y ait une infinité de u_n dans L $= L_1^k(L_1^N)^*$ où N est le nombre d'états de A.

Cette construction donne un langage L contenant une infinité de $(u_n)_{n\in\mathbb{N}}$ de la forme **w** $= a_1(b_1)^*... \, a_m(b_m)^*$ où les a_i sont des lettres et les b_i sont de la même forme et où par ailleurs si on a r^* dans l'écriture de w, alors $(u_n)_{n\in\mathbb{N}}$ contient des termes r^n pour des valeurs arbitrairement grande de n.
Il s'agit maintenant de montrer que **w** est une écriture d'une preuve de valeur 1 du monoïde.

Soit t tel que $\mathbf{w}$(i,t) = 1.

- Si $\mathbf{w} = \epsilon$ ou $\mathbf{w} = a \in \Sigma$, par définition, $\mathbf{w}$(i,t) = 1 si et seulement s'il y a une transition de probabilité non nulle de i à t en lisant w, or comme la probabilité de $(u_n)_{n\in\mathbb{N}}$ tend vers 1 et L contient une infinité de $(u_n)_{n\in\mathbb{N}}$, il y a une probabilité non nulle.
- Si $\mathbf{w} = L_1L_2$, il existe deux suites $(b_n)_{n\in\mathbb{N}}$ et $(c_n)_{n\in\mathbb{N}}$ ayant une infinité de termes dans L_1 et L_2 tels que $u_n = b_nc_n$.
  On note I = {s $\in Q \mid L_1(i,s) = 1$} et J = {s $\in Q \mid L_2(s,t) = 1$}.
  Comme $\mathbf{w}$(i,t) = 1, il existe s tel que $s \in I \cap J$. Par induction, $lim_{n\to+\infty} b_n(i,s) > 0$ et $lim_{n\to+\infty} u_n(s,t) > 0$, donc $lim_{n\to+\infty} u_n(i,t) > 0$.
- Le cas $\mathbf{w} = (L_1)^*$ n'a été traité que dans un cas particulier pour le moment.