Méthodes Formelles Approche Probabiliste

Arnaud Sangnier

IRIF - Université de Paris

Cours 6

Vérification de systèmes probabilistes)

Introduction de probabilités dans les modèles

Pourquoi ?

- Algorithme ’randomisé’
- Modélisation de comportements non fiables et partiellement prédictibles
- Évaluation de performances de systèmes

Nouveaux modèles et propriétés

Modèles

1. **Chaînes de Markov à temps discret** (chaînes de Markov)
   - Tous les choix sont **probabilistes**
   - Système de transitions où le choix du sucesseur est une distribution probabiliste
2. **Processus de décision markovien**
   - Choix **probabilistes** et **non déterministes**
   - Choix entre plusieurs distributions probabilistes pour le sucesseur

Propriétés

1. **qualitatives**
   - Permettent de dire que des événément arrivent presque sûrement (avec probabilité 1) ou presque jamais (avec probabilité 0)
2. **quantitatives**
   - Permettent de préciser les probabilités des événéments avec des valeurs autres que 0 ou 1

Chaînes de Markov à temps discret

On les appelera chaînes de Markov (CM)

Définition

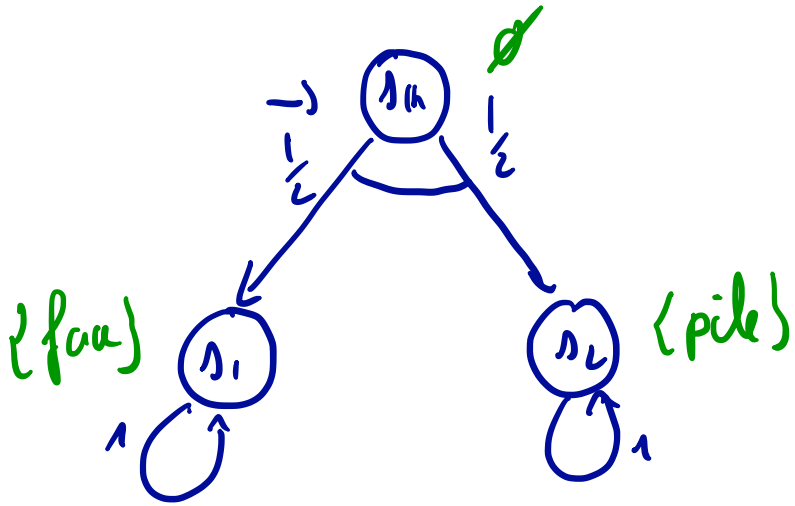
Une chaîne de Markov M est un n-uplet (S, P, s_{in}, PA, L) où :

- S est l'ensemble des états
- $P : S \times S \mapsto [0; 1]$ est la fonction de transitions probabiliste telle que $\Sigma_{s' \in S} P(s, s') = 1$ pour tout $s \in S$
- $s_{in} \in S$ est l'état initial
- PA est l'ensemble des propositions atomiques
- $L : S \mapsto 2^{PA}$ est la fonction d'étiquetage

- $[0; 1]$ correspond aux réels compris entre 0 et 1
- La fonction P définit pour chaque état s la probabilité $P(s, s')$ dans l'état s'
- Dans le cours, nous supposerons que S **est fini** et $P(s, s')$ est rationnel.

Exemple - I

Chaîne de Markov pour lancer de pièce



$S = \{s_{in}, s_1, s_2\}$

$P(s_{in}, s_1) = P(s_{in}, s_2) = \frac{1}{2}$

$P(s_1, s_1) = P(s_2, s_2) = 1$

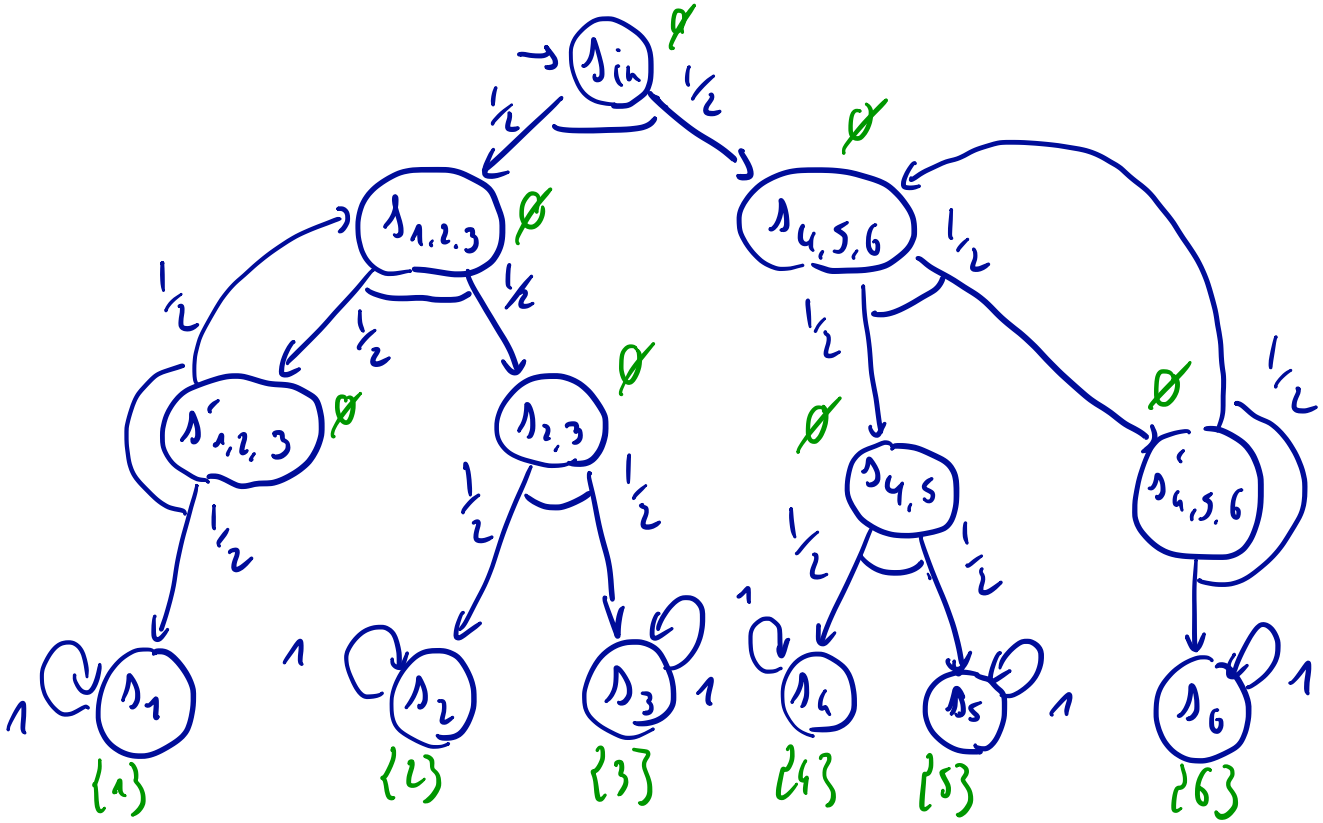
$L(s_{in}) = \emptyset$

$L(s_1) = \{face\}$

$L(s_2) = \{pile\}$.

Exemple - II

Chaine de Markov pour simuler un dé à 6 faces avec une pièce.



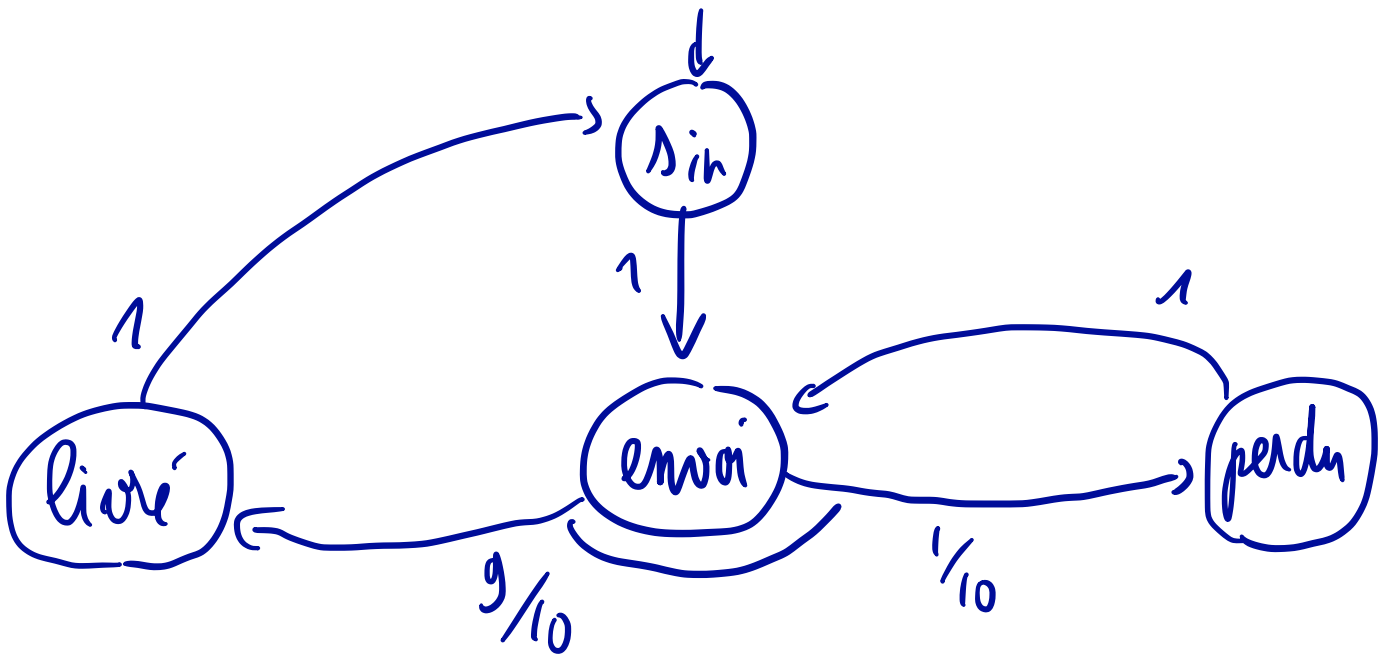
$$\sum_{i=1}^{n} \left(\frac{1}{4}\right)^i = \frac{1-\left(\frac{1}{4}\right)^{n+1}}{1-\frac{1}{4}} - 1$$

Est-ce que $\mathbb{P}(F1) = 1/6$? oui

$$\mathbb{P}(F1) = \frac{1}{2}\cdot\left(\frac{1}{4} + \frac{1}{4^2} + \frac{1}{4^3} + \dots\right) = \lim_{n\to+\infty} \frac{1}{2} \sum_{i=1}^{n} \left(\frac{1}{4}\right)^i = \frac{1}{6}$$

Exemple - III

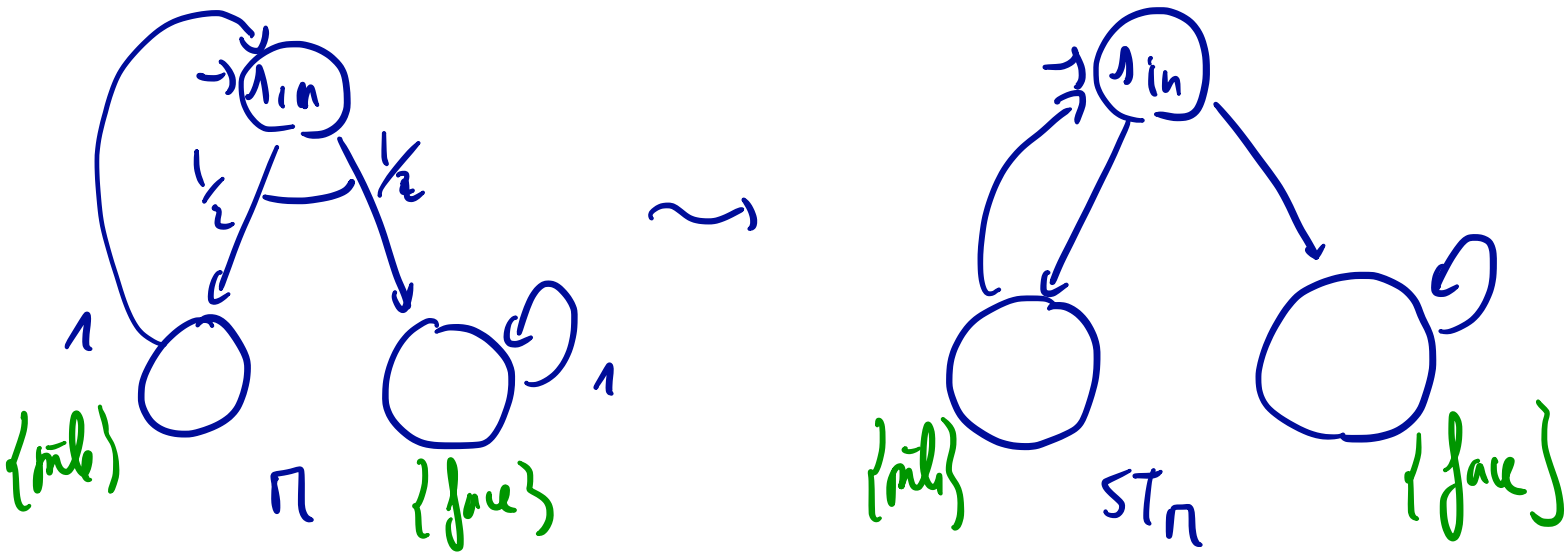
Envoi de messages en boucles. Si un message est perdu, on le réenvoie.
Probabilité qu'un message se perde : 1/10



Chaînes de Markov vs. Systèmes de transitions

BUT : Vérifier des propriétés sur des chaînes de Markov

- **Approche naïve :** On transforme une chaîne de Markov $M = (S, P, s_{in}, PA, L)$ en un système de transitions $ST_M = (S, \to, s_{in}, PA, L)$ avec $s \to s'$ ssi $P(s, s') > 0$



- Dans ST_M la propriété $\mathbb{F}\,face$ n'est pas vérifiée, mais dans M la probabilité d'avoir $\mathbb{F}\,face$ est égale à 1
- Dans M, on verra presque sûrement un jour *face*
- On va donc vouloir raisonner sur un espace de probabilité

Rappels mathématiques - I

Définition

Soit Ω un ensemble appelé l'univers. Une tribu sur Ω est un ensemble $\mathcal{A} \subseteq 2^{\Omega}$ tel que :

1. $\mathcal{A} \neq \emptyset$
2. Pour tout $B \in \mathcal{A}$, on a $\Omega \setminus B \in \mathcal{A}$ (stable par complément)
3. Soit $(B_n)_{n\in\mathbb{N}}$ un famille d'éléments de $\mathcal{A}$, alors $\bigcup_{n\in\mathbb{N}} B_n \in \mathcal{A}$ (stable par union dénombrable)

- Un couple $(\Omega, \mathcal{A})$ où $\mathcal{A}$ est une tribu sur Ω est appelé un **espace mesurable**.

Remarque :

- Par définition $\Omega \in \mathcal{A}$ et $\mathcal{A}$ est stable par intersection dénombrable

Rappels mathématiques - II

Définition

Soit $(\Omega, \mathcal{A})$ un espace mesurable. Une mesure de probabilité sur $(\Omega, \mathcal{A})$ est une fonction $\mathbb{P} : \mathcal{A} \mapsto [0; 1]$ telle que :

1. $\mathbb{P}(\Omega) = 1$
2. SI $(B_n)_{n \in \mathbb{M}}$ est une famille d'éléments de $\mathcal{A}$ telle que pour tout $i, j \in \mathbb{N}$, $i \neq j$ implique $B_i \cap B_j = \emptyset$ alors $\mathbb{P}(\bigcup_{n \in \mathbb{N}} B_n) = \Sigma_{n \in \mathbb{N}} \mathbb{P}(B_n)$.

- Un **espace probabiliste** est un triplet $(\Omega, \mathcal{A}, \mathbb{P})$ où $(\Omega, \mathcal{A})$ est un espace mesurable et $\mathbb{P}$ est une mesure de probabilité sur $(\Omega, \mathcal{A})$
- Dans ce contexte, on dit que les éléments de $\mathcal{A}$ sont mesurables

Quelques règles utiles :

- Pour tout $B \in \mathcal{A}$, on a $\mathbb{P}(\Omega \setminus B) = 1 - \mathbb{P}(B)$
- Pour tout $B, B' \in \mathcal{A}$, si $B \subseteq B'$ alors $\mathbb{P}(B') = \mathbb{P}(B) + \mathbb{P}(B' \setminus B) \geq \mathbb{P}(B)$

Exemple

- Pièce pour faire pile ou face
- L'univers est $\Omega = \{\textit{pile}, \textit{face}\}$
- On prend comme tribu $\mathcal{A} = \{\emptyset, \{\textit{pile}\}, \{\textit{face}\}, \{\textit{pile}, \textit{face}\}, \}$
- Et comme mesure de probabilité :
  - $\mathbb{P}(\emptyset) = 0$
  - $\mathbb{P}(\{\textit{pile}\}) = \frac{1}{2}$
  - $\mathbb{P}(\{\textit{face}\}) = \frac{1}{2}$
  - $\mathbb{P}(\{\textit{pile}, \textit{face}\}) = 1$

Quelques définitions

Soit $M = (S, P, s_{in}, PA, L)$ une chaîne de Markov.

- Un **chemin fini** est une séquence finie d'états $s_0 s_1 \ldots s_n$ telle que pour tout $i \in 0, \ldots, n-1$, on a $P(s_i, s_{i+1}) > 0$
- On note $ChemFin(M, s)$ l'ensemble des chemins finis de M commençant en s
- Un **chemin infini** est une séquence infinie d'états $s_0 s_1 s_2 \ldots$ telle que pour tout $i \in \mathbb{N}$, on a $P(s_i, s_{i+1}) > 0$
- Une **exécution** est un chemin infini $s_0 s_1 s_2 \ldots$ tel que $s_0 = s_{in}$
- On note $Exec(M)$ l'ensemble des exécutions de M

Espace probabiliste associé à une chaîne de Markov

Soit $M = (S, P, s_{in}, PA, L)$ une chaîne de Markov.

- Soit $\hat{\pi} \in ChemFin(M, s_{in})$, le cylindre associé à $\hat{\pi}$ est défini par $Cyl(\hat{\pi}) = \{\pi \in Exec(M) \mid \hat{\pi} \text{ est préfixe de } \pi\}$
- On prend comme univers $Exec(M)$ et comme tribu sur $Exec(M)$, la plus petite tribu qui contient tous les $Cyl(\hat{\pi})$ pour tout $\hat{\pi} \in ChemFin(M, s_{in})$, on note $\mathcal{T}_{Cyl,M}$ cette tribu

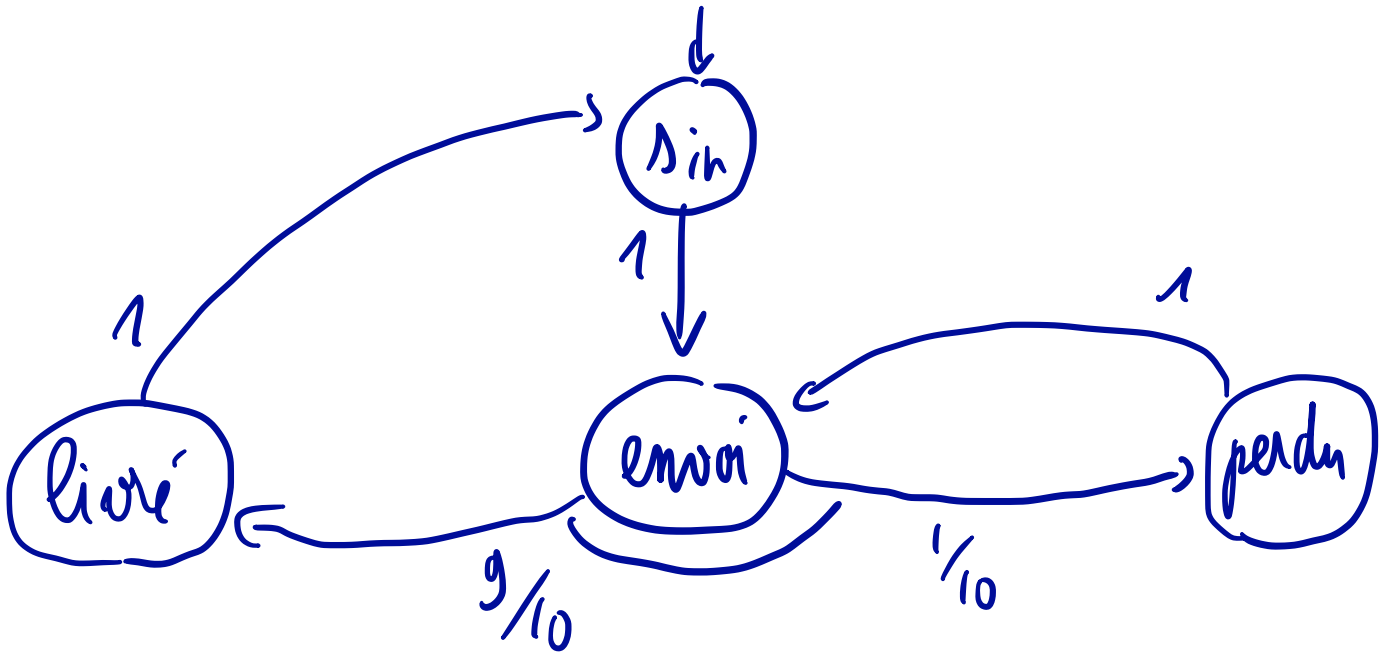
On définit ensuite $\mathbb{P}_M : \mathcal{T}_{Cyl,M} \mapsto [0; 1]$ pour chaque cylindre $Cyl(s_0 s_1 \dots s_n)$ (avec $s_0 s_1 \dots s_n \in ChemFin(M, s_{in})$), on a :

- $\mathbb{P}_M(Cyl(s_0 s_1 \dots s_n)) = \Pi_{i=0}^{n-1} P(s_i, s_{i+1})$, et,
- $\mathbb{P}_M(Cyl(s_{in})) = 1$.

Parfois, on aura besoin de changer l'état initial de M, ainsi pour $s \in S$, on note $M_s = (S, P, s, PA, L)$ et on alors :

- $\mathbb{P}_M(Cyl(s_0 s_1 \dots s_n)) = P(s_0, s_1) \cdot \mathbb{P}_{M_{s_1}}(Cyl(s_1 \dots s_n))$

Exemple



$\hat{\pi} = s_{in}$ envoi . perdu envoi perdu

$P_n(Cyl(\hat{\pi})) = 1 \cdot 1/10 \cdot 1 \cdot 1/10 = 1/100$

Propriétés mesurables - I

- Étant donnée une chaîne de Markov $M = (S, P, s_{in}, PA, L)$, on va supposer que $PA = S$ et pour tout $s \in S$, on a $L(s) = \{s\}$. On confond les états et leurs propositions atomiques.
- On va utiliser des notations à la LTL pour caractériser des événements (ie des sous-ensembles de $Exec(M)$), Soit $A, B \subseteq S$.
  - $\mathtt{F}B = \{s_0 s_1 \ldots \in Exec(M) \mid \exists j.s_j \in B\}$ (i.e. on voit un jour un élément de B)
  - $\mathtt{G}B = \{s_0 s_1 \ldots \in Exec(M) \mid \forall j.s_j \in B\}$ (i.e. on voit toujours un élément de B)
  - $\mathtt{GF}B = \{s_0 s_1 \ldots \in Exec(M) \mid \forall i.\exists j.i \leq j$ and $s_j \in B\}$ (i.e. on voit infiniment souvent un élément de B)
  - $\mathtt{FG}B = \{s_0 s_1 \ldots \in Exec(M) \mid \exists i.\forall j.i < j$ implies $s_j \in B\}$ (i.e. au bout d'un moment on on voit toujours B)
  - $A\mathtt{U}B = \{s_0 s_1 \ldots \in Exec(M) \mid \exists j.s_j \in B$ et $\forall i.i < j$ implies $s_i \in A\}$ (i.e. au bout d'un moment on voit B et avant on voit toujours A)

Propriétés mesurables - III

- Pour une telle formule ϕ et une exécution π, on notera $\pi \models \phi$ ssi $\pi \in \phi$
- Étant donné $s \in S$, on va s'intéresser à la probabilité suivante :

$$\mathbb{P}_M(s \models \phi) = \mathbb{P}_{M_s}(\pi \in \mathit{Exec}(M_s) \mid \pi \models \phi)$$

- Pour que cela soit correct, il faut montrer que $\{\pi \in \mathit{Exec}(M_s) \mid \pi \models \phi\}$ est mesurable !!

Propriétés mesurables - IV

Théorème

$\mathtt{F}B$, $\mathtt{G}B$, $\mathtt{GF}B$, $\mathtt{FG}B$ et $A\mathtt{U}B$ sont des événements mesurables pour la chaîne de Markov M.

Preuve :

- On a $\mathtt{G}B = Exec(M) \setminus (F(S \setminus B))$ et $\mathtt{FG}B = Exec(M) \setminus \mathtt{GF}(S \setminus B)$
- Il nous reste à traiter $\mathtt{F}B$ $\mathtt{GF}B$ et $A\mathtt{U}B$.

$$\mathtt{F}B = \bigcup_{\{s_0 \ldots s_n \in ChemFin(M,s_{in}) | s_0,\ldots,s_{n-1} \notin B \text{ et } s_n \in B\}} Cyl(s_0 \ldots s_n)$$

- Donc $\mathtt{F}B$ est mesurable, le même raisonnement vaut pour $A\mathtt{U}B$ et :

$$\mathbb{P}_M(\mathtt{F}B) = \sum_{\{s_0 \ldots s_n \in ChemFin(M,s_{in}) | s_0,\ldots,s_{n-1} \notin B \text{ et } s_n \in B\}} \mathbb{P}(Cyl(s_0 \ldots s_n))$$

$$\mathtt{GF}B = \bigcap_{n \in \mathbb{N}} \bigcup_{m \geq n} \bigcup_{\{s_0 \ldots s_m \in ChemFin(M,s_{in}) | s_m \in B\}} Cyl(s_0 \ldots s_m)$$

- Donc $\mathtt{GF}B$ est mesurable