Vérification de modèles stochastiques et synthèse de contrôleurs à spécifications probabilistes

EJCIM 2024

Damien Busatto-Gaston

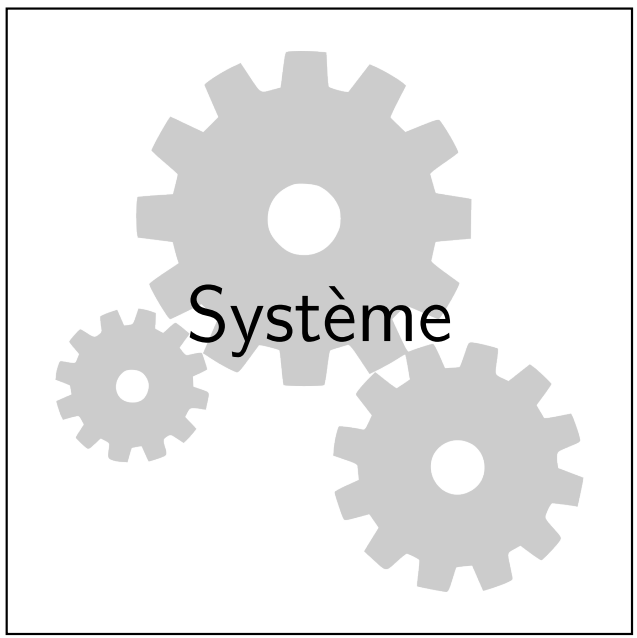
Université Paris-Est Créteil, LACL

21 juin 2024

Vérification de systèmes

Garantir le bon fonctionnement d'un système :

- donner des résultats justes
- dans les délais attendus
- autres propriétés

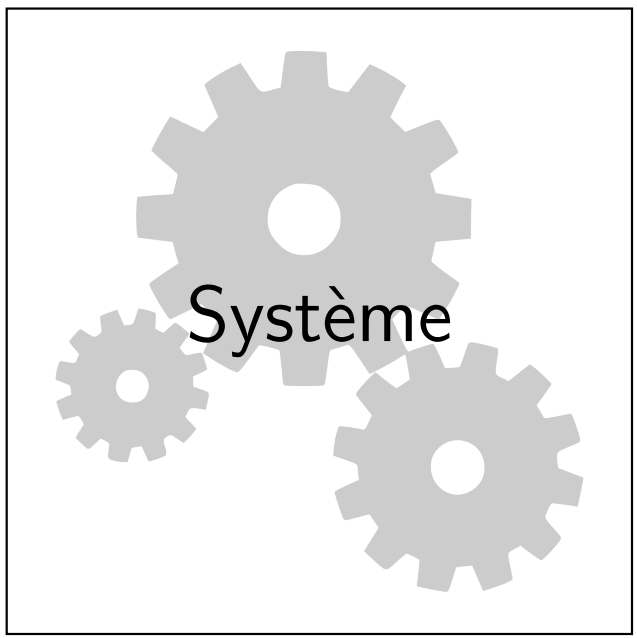


$\models$ Spécification

Vérification de systèmes

Garantir le bon fonctionnement d'un système :

- donner des résultats justes
- dans les délais attendus
- autres propriétés

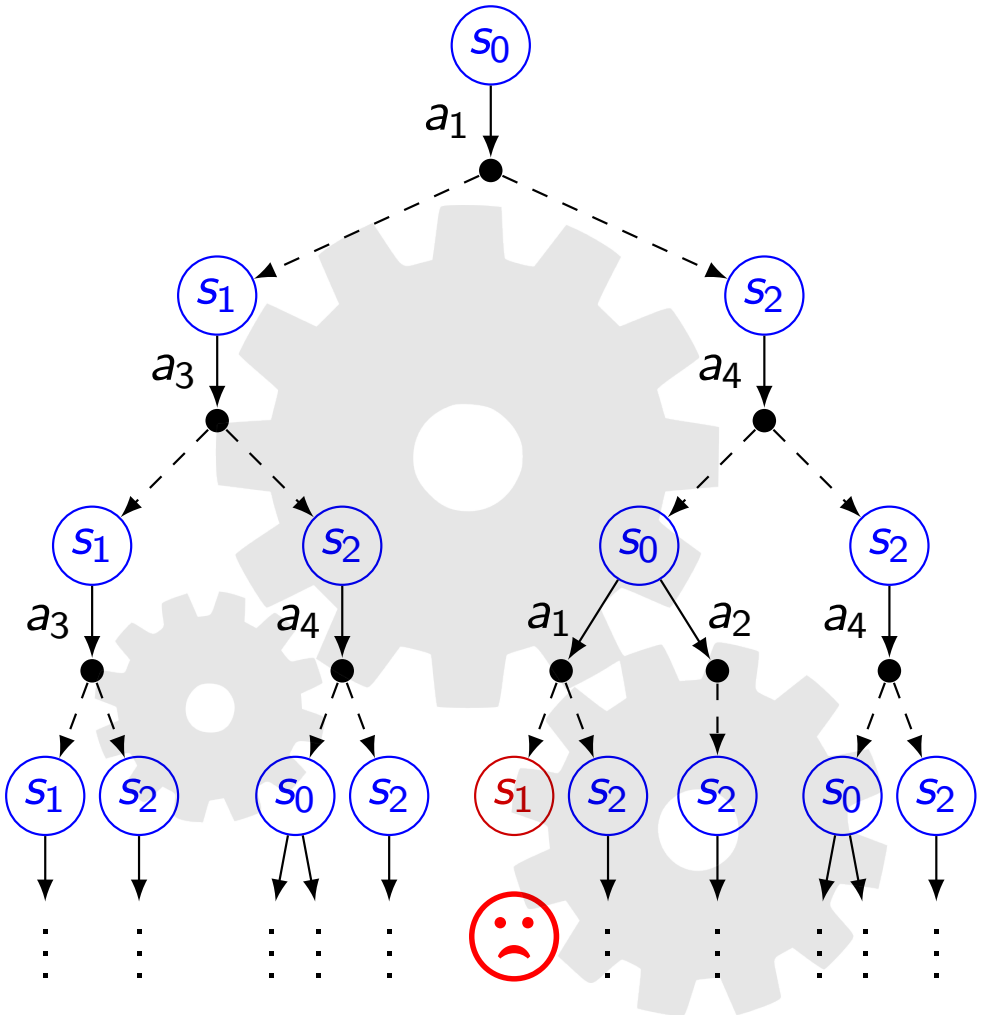


$\models$ Spécification

Approche des *méthodes formelles* :

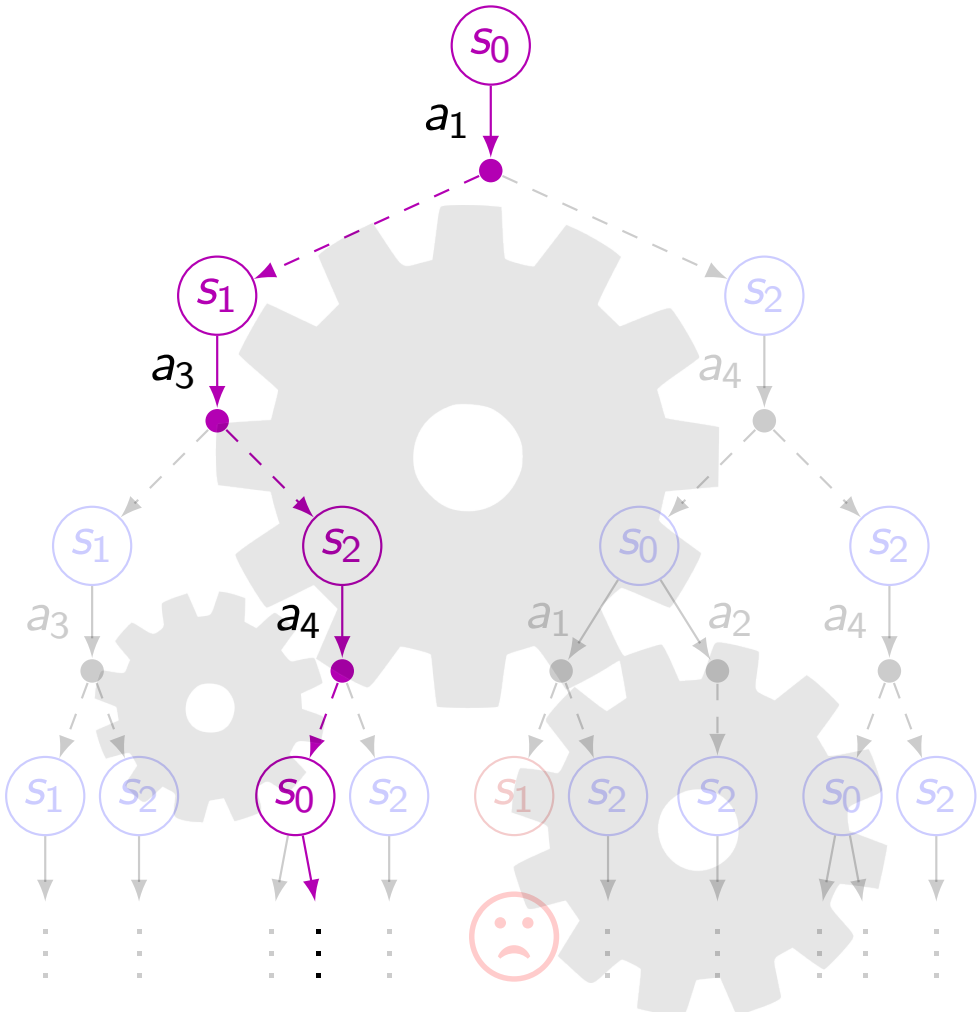
- modèles : machines abstraites
- spécifications : propriétés logiques

Tests vs model-checking



$\models$ Spécification

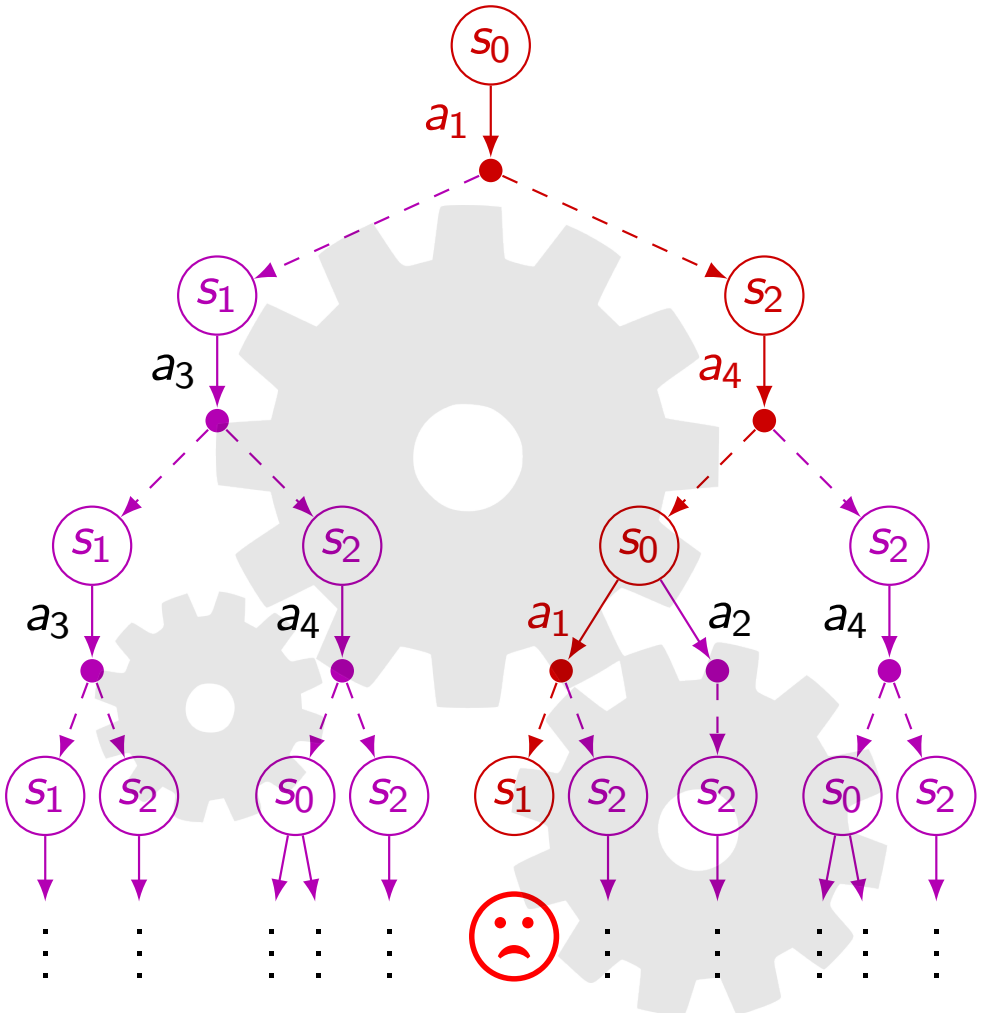
Tests vs model-checking



$\models$ Spécification

- Test

Tests vs model-checking

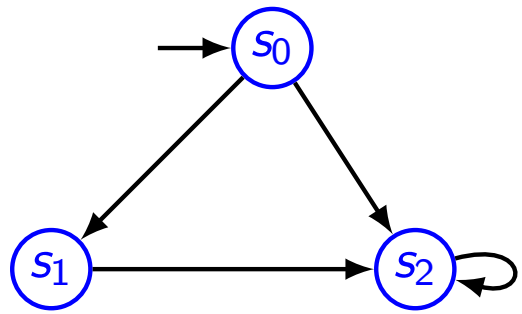


$\models$ Spécification

- Model-checking : Système $\models$ Spécification

Systèmes de transitions

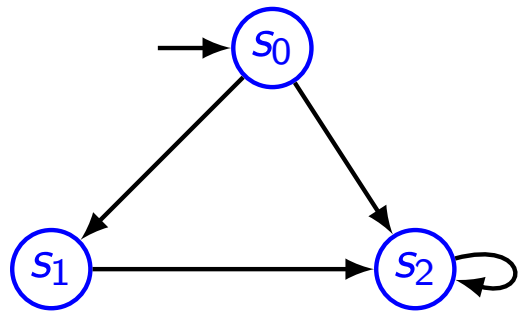
- modèle : système de transitions M



  - représente les différentes exécutions possibles
  - non-déterminisme adversarial

Systèmes de transitions

- modèle : système de transitions M

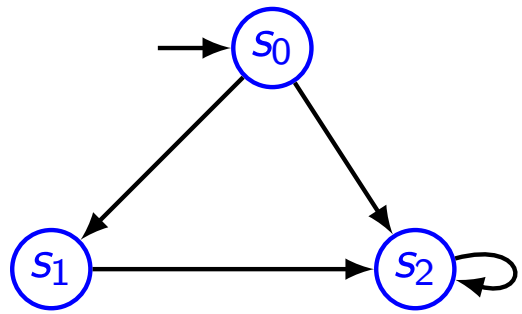


  - représente les différentes exécutions possibles
  - non-déterminisme adversarial

- spécification : formule logique ϕ
  - formule booléenne ? $\rightsquigarrow$ horizon borné

Systèmes de transitions

- modèle : système de transitions M



  - représente les différentes exécutions possibles
  - non-déterminisme adversarial

- spécification : formule logique ϕ
  - formule booléenne ? $\rightsquigarrow$ horizon borné
  - logiques temporelles

Logiques temporelles

Propriétés exprimées sur les exécutions d'un système, par exemple :

- propriétés d'accessibilité $\rightsquigarrow$ terminaison : $\mathsf{F}\, a$
- propriétés de sûreté $\rightsquigarrow$ éviter des erreurs : $\mathsf{G}\, b$

Logique Temporelle Linéaire (LTL) : propriété exprimée sur un chemin

L'état s_2 finit par être atteint sans que s_1 ai été visité

$$\mathsf{F}\, s_2 \wedge \mathsf{G}\, \neg s_1$$

Logiques temporelles

Propriétés exprimées sur les exécutions d'un système, par exemple :

- propriétés d'accessibilité $\rightsquigarrow$ terminaison : $\mathsf{F}\, a$
- propriétés de sûreté $\rightsquigarrow$ éviter des erreurs : $\mathsf{G}\, b$

Logique Temporelle Linéaire (LTL) : propriété exprimée sur un chemin

L'état s_2 finit par être atteint sans que s_1 ai été visité

$$\mathsf{F}\, s_2 \wedge \mathsf{G}\, \neg s_1$$

Logique branchante (CTL) : quantifications sur les chemin

Tous les chemins visitent s_2 et il existe un chemin qui ne visite pas s_1

$$\mathsf{A}\, \mathsf{F}\, s_2 \wedge \mathsf{E}\, \mathsf{G}\, \neg s_1$$

Logiques temporelles

Propriétés exprimées sur les exécutions d'un système, par exemple :

- propriétés d'accessibilité $\rightsquigarrow$ terminaison : $\mathsf{F}\, a$
- propriétés de sûreté $\rightsquigarrow$ éviter des erreurs : $\mathsf{G}\, b$

Logique Temporelle Linéaire (LTL) : propriété exprimée sur un chemin

L'état s_2 finit par être atteint sans que s_1 ai été visité

$$\mathsf{F}\, s_2 \wedge \mathsf{G}\, \neg s_1$$

Logique branchante (CTL) : quantifications sur les chemin

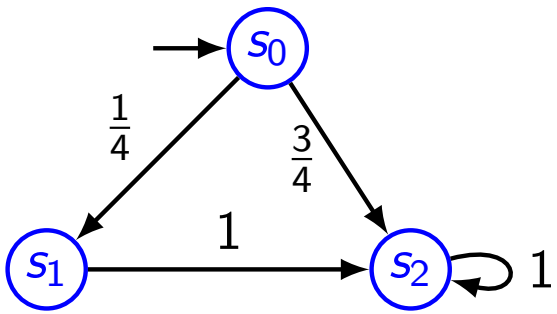
Tous les chemins visitent s_2 et il existe un chemin qui ne visite pas s_1

$$\mathsf{A}\, \mathsf{F}\, s_2 \wedge \mathsf{E}\, \mathsf{G}\, \neg s_1$$

- *model-checking* : étant donné M et ϕ, est-ce que $M \models \phi$?
  [Clarke, Emerson, Sifakis] : prix Turing en 2007

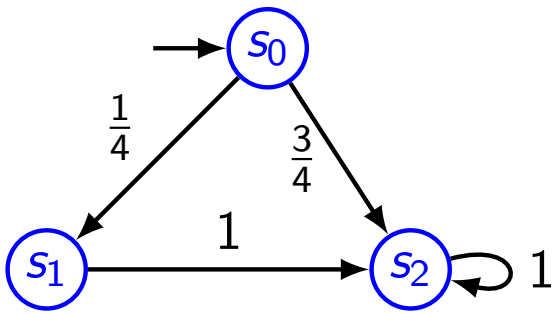
Et les systèmes stochastiques ?

- modèle : Chaîne de Markov M : transitions équipées de probabilités



Et les systèmes stochastiques ?

- modèle : Chaîne de Markov M : transitions équipées de probabilités



- spécification : formule ϕ en logique probabiliste (PCTL)

  Au lieu des quantifications A et E, on exprime la probabilité qu'une formule soit vrai :

  $$\mathbb{P}\left[\mathsf{G}\,\neg s_1\right] \geq \frac{1}{2}$$

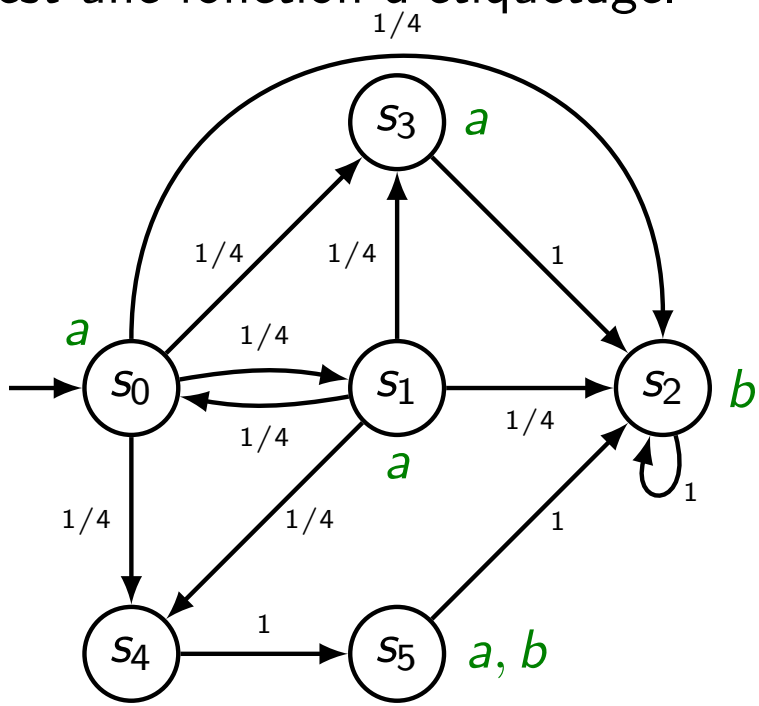
Chaînes de Markov

On définit une chaîne de Markov par un système de transitions d'états :

Definition

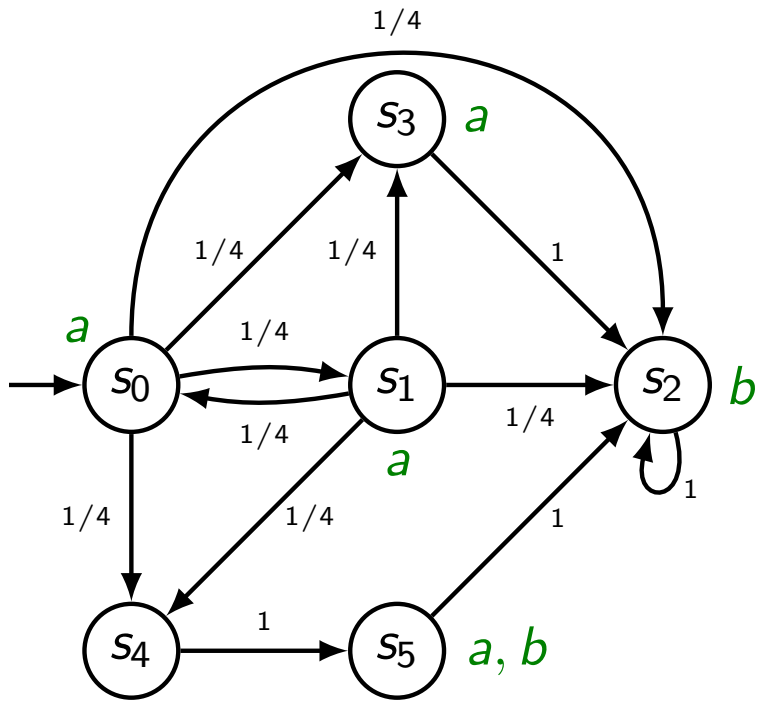
Une *chaîne de Markov* est un tuple $M = \langle S, s_{\text{init}}, \mathbb{P}, \text{PA}, L \rangle$, où

- S est un ensemble fini d'états,
- $s_{\text{init}} \in S$ est un état initial,
- $\mathbb{P} : S \to \text{Dist}(S)$ est une fonction de transition,
- PA est un ensemble fini de propositions atomiques,
- et $L : S \to 2^{\text{PA}}$ est une fonction d'étiquetage.



Chemins et leur probabilités

- chemins finis : $\mathrm{CheminsF}_M(s)$
  - $\rightsquigarrow$ produit des probabilités
- chemins infinis : $\mathrm{Chemins}_M(s)$
  - $\rightsquigarrow$?



Mesure de probabilité

Spécifications : comportements attendus de la part de chemins infinis

Definition

mesure d'un ensemble de chemins infinis $\Pi \subseteq \text{Chemins}_M(s)$:
$\rightsquigarrow$ probabilité qu'un chemin ρ tiré dans M appartiennent à Π

Mesure de probabilité

Spécifications : comportements attendus de la part de chemins infinis

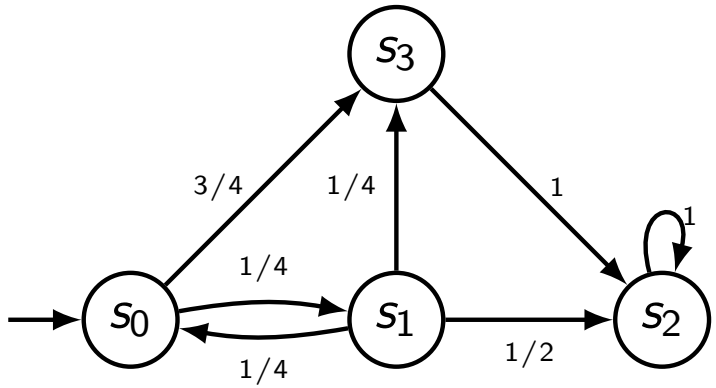
Definition

mesure d'un ensemble de chemins infinis $\Pi \subseteq \text{Chemins}_M(s)$:
$\rightsquigarrow$ probabilité qu'un chemin ρ tiré dans M appartiennent à Π

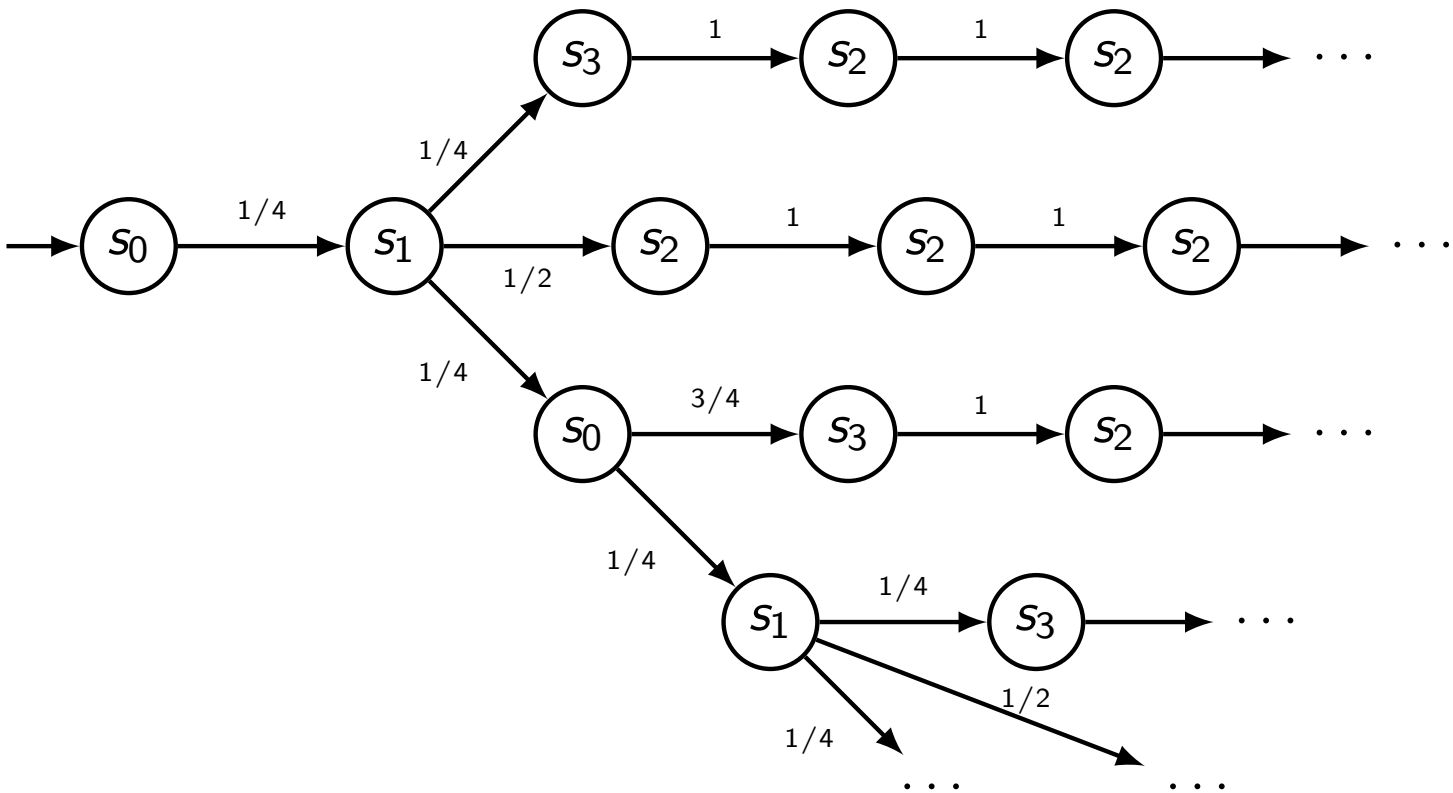
Si ρ est un chemin fini, l'ensemble $\text{Chemins}_M(\rho)$ des chemins infinis qui admettent ρ comme préfixe est appelé le *cylindre* de ρ.

- mesure du cylindre de préfixe ρ : probabilité de ρ

Cylindre



$\mathrm{Chemins}_M(s_0 s_1)$:



Théorème d'extension de Carathéodory

Definition

Une chaîne de Markov M induit naturellement une *mesure de probabilités* μ_M^s sur l'espace mesurable $(\text{Chemins}_M(s), \Omega_M^s)$.

- univers : chemins infinis démarrant en s
- évènements : la tribu cylindrique Ω_M^s, plus petite collection contenant
  - les cylindres de préfixes finis,
  - leurs compléments,
  - et leurs unions dénombrables

Propriété d'accessibilité

- Soit $M = \langle S, s_{\text{init}}, \mathbb{P}, \text{PA}, L \rangle$ une chaîne de Markov.

Definition

On dit que $\rho \in \text{Chemins}_M$ satisfait la propriété *d'accessibilité* $p \in \text{PA}$ si ρ passe par un état s qui satisfait p – c'est-à-dire tel que $p \in L(s)$.

Propriété d'accessibilité

- Soit $M = \langle S, s_{\text{init}}, \mathbb{P}, \text{PA}, L \rangle$ une chaîne de Markov.

Definition

On dit que $\rho \in \text{Chemins}_M$ satisfait la propriété *d'accessibilité* $p \in \text{PA}$ si ρ passe par un état s qui satisfait p – c'est-à-dire tel que $p \in L(s)$.

- Dans ce cas, on écrit $\rho \models \text{F}\, p$.
- $\text{F}\, p$ se lit "un jour p sera atteint", l'opérateur F venant du mot anglais *finally*.

Probabilité d'accessibilité

Soit ρ un chemin tiré aléatoirement dans la chaîne de Markov.

- on s'intéresse au problème suivant :

  Quelle est la probabilité que $\rho \models \mathsf{F}\, p$?

- On note cette probabilité $\mathbb{P}[\mathsf{F}\, p]$

Probabilité d'accessibilité

Soit ρ un chemin tiré aléatoirement dans la chaîne de Markov.

- on s'intéresse au problème suivant :

$$\text{Quelle est la probabilité que } \rho \models \mathsf{F}\, p \,?$$

- On note cette probabilité $\mathbb{P}\left[\mathsf{F}\, p\right]$

- défini formellement comme $\mu_M(\Pi)$, la mesure de l'ensemble des chemins atteignant p, de sorte que

$$\Pi = \{\rho \in \mathsf{Chemins}_M(s_{\mathsf{init}}) \mid \rho \models \mathsf{F}\, p\}\,.$$

- Π mesurable ?

Propriété d'accessibilité à horizon borné

- Soit $M = \langle S, s_{\text{init}}, \mathbb{P}, \text{PA}, L \rangle$ une chaîne de Markov.

Definition

On dit que $\rho \in \text{Chemins}_M$ satisfait la propriété *d'accessibilité* $p \in \text{PA}$ *d'horizon* $\ell \in \mathbb{N}$ si ρ passe par un état s qui satisfait p dans les ℓ premiers états du chemin.

Propriété d'accessibilité à horizon borné

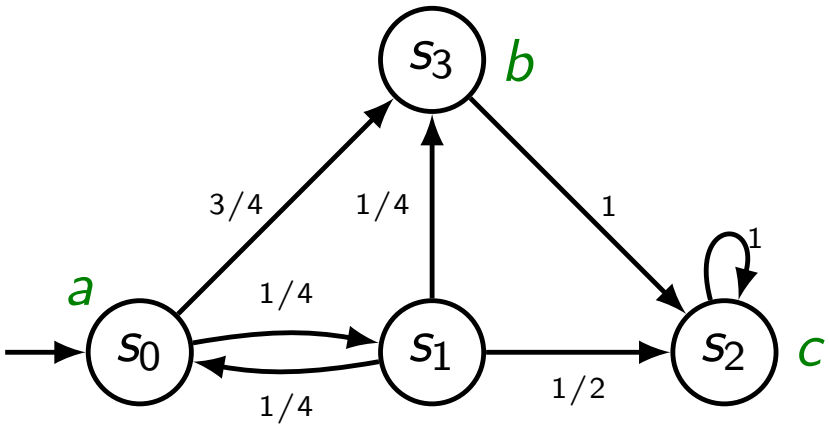
- Soit $M = \langle S, s_{\text{init}}, \mathbb{P}, \text{PA}, L \rangle$ une chaîne de Markov.

Definition

On dit que $\rho \in \text{Chemins}_M$ satisfait la propriété *d'accessibilité* $p \in \text{PA}$ *d'horizon* $\ell \in \mathbb{N}$ si ρ passe par un état s qui satisfait p dans les ℓ premiers états du chemin.

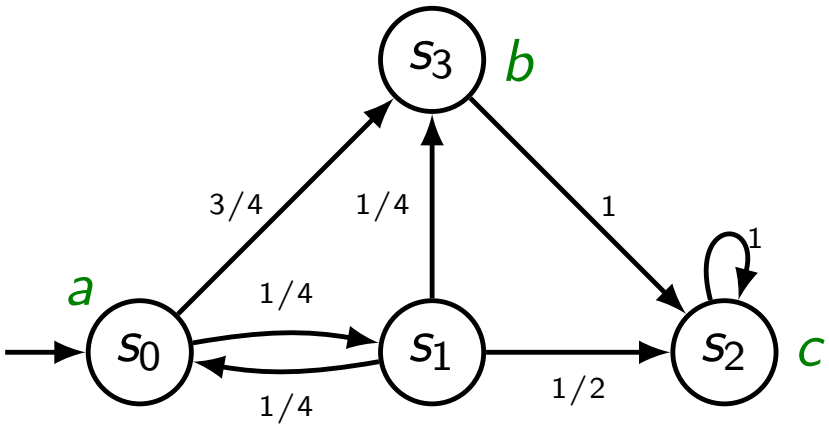
- Dans ce cas, on écrit $\rho \models \text{F}^{\ell}\, p$
- $\text{F}^{\ell}\, p$ se lit "p sera atteint dans les ℓ prochains états"

Exemples



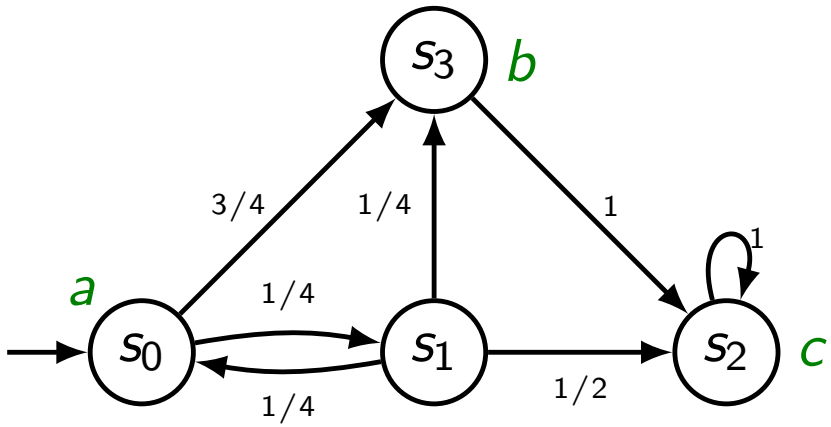
- $\mathbb{P}[\mathsf{F}\, a]$?

Exemples



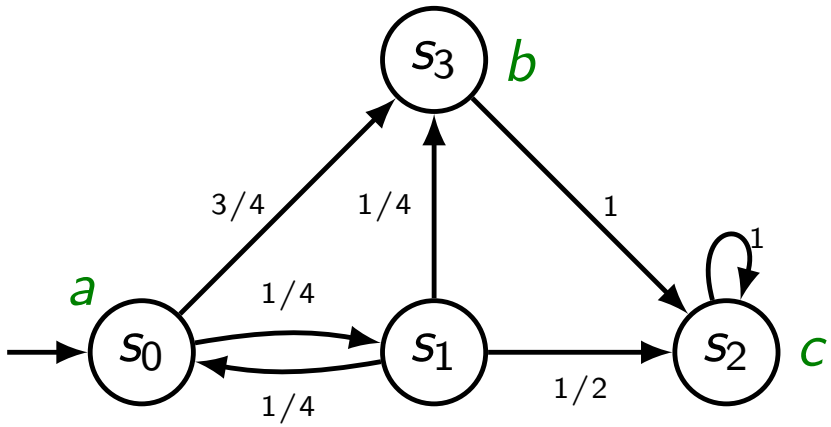
- $\mathbb{P}[\mathsf{F}\, a]$?
  - $\mathbb{P}[\mathsf{F}\, a] = 1$

Exemples



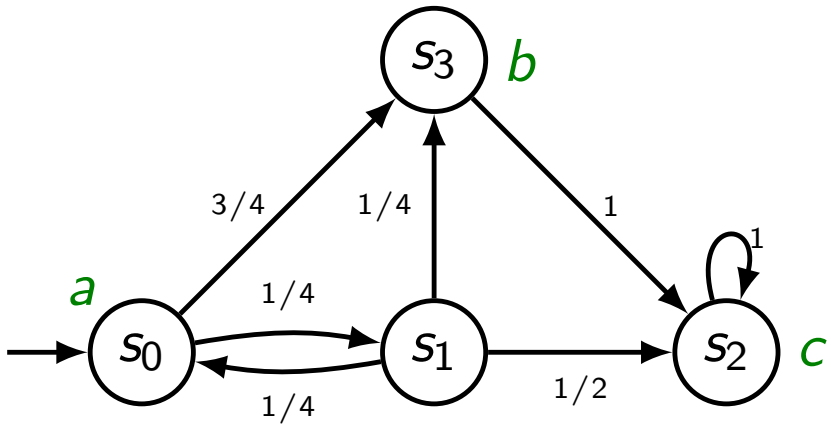
- $\mathbb{P}[\mathsf{F}\, a]$?
  - $\mathbb{P}[\mathsf{F}\, a] = 1$
- $\mathbb{P}\left[\mathsf{F}^3\, b\right]$?

Exemples



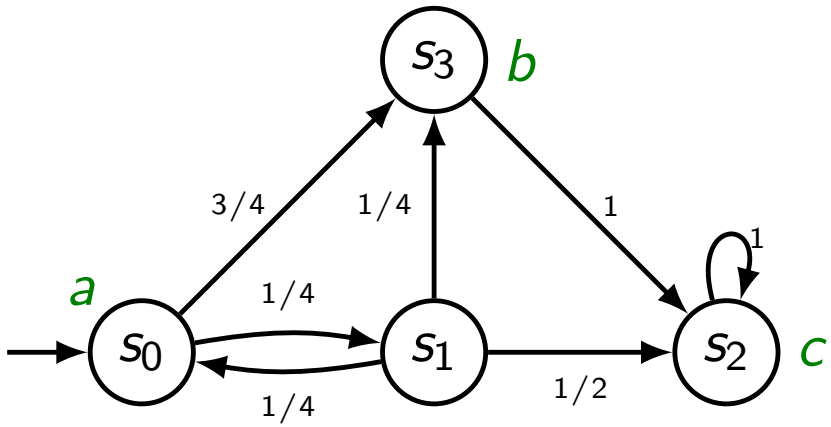
- $\mathbb{P}[\mathsf{F}\, a]$?
  - $\mathbb{P}[\mathsf{F}\, a] = 1$
- $\mathbb{P}\left[\mathsf{F}^3\, b\right]$?
  - $\mathbb{P}\left[\mathsf{F}^3\, b\right] = \frac{3}{4} + \frac{1}{4} \cdot \frac{1}{4} + \frac{1}{4} \cdot \frac{1}{4} \cdot \frac{3}{4} = \frac{55}{64} \approx 0.859$

Exemples



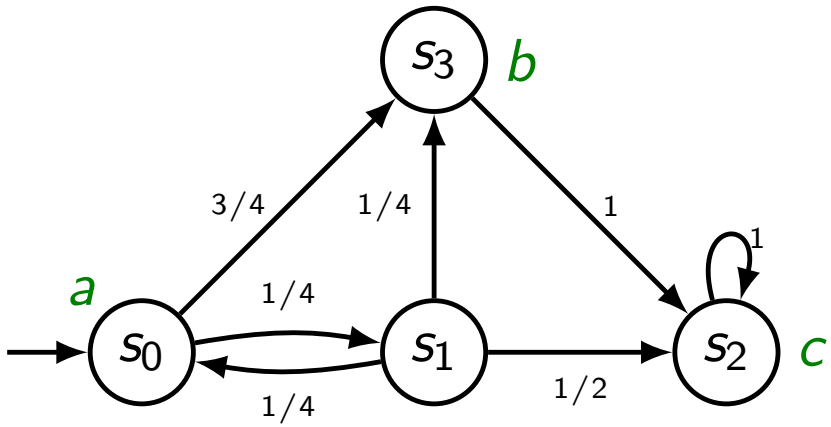
- $\mathbb{P}[\mathsf{F}\, a]$?
  - $\mathbb{P}[\mathsf{F}\, a] = 1$
- $\mathbb{P}\left[\mathsf{F}^3\, b\right]$?
  - $\mathbb{P}\left[\mathsf{F}^3\, b\right] = \frac{3}{4} + \frac{1}{4} \cdot \frac{1}{4} + \frac{1}{4} \cdot \frac{1}{4} \cdot \frac{3}{4} = \frac{55}{64} \approx 0.859$
- $\mathbb{P}[\mathsf{F}\, c]$?

Exemples



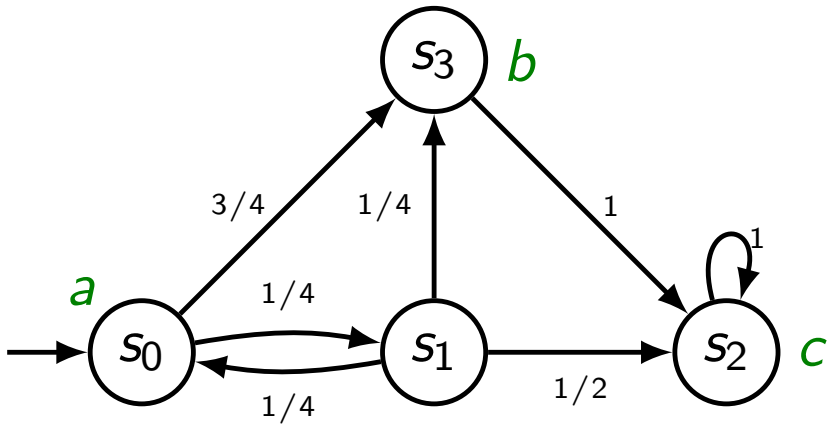
- $\mathbb{P}[\mathsf{F}\, a]$?
  - $\mathbb{P}[\mathsf{F}\, a] = 1$
- $\mathbb{P}\left[\mathsf{F}^3\, b\right]$?
  - $\mathbb{P}\left[\mathsf{F}^3\, b\right] = \frac{3}{4} + \frac{1}{4} \cdot \frac{1}{4} + \frac{1}{4} \cdot \frac{1}{4} \cdot \frac{3}{4} = \frac{55}{64} \approx 0.859$
- $\mathbb{P}[\mathsf{F}\, c]$?
  - $\mathbb{P}[\mathsf{F}\, c] = 1$

Exemples



- $\mathbb{P}[\mathsf{F}\, a]$?
  - $\mathbb{P}[\mathsf{F}\, a] = 1$
- $\mathbb{P}\left[\mathsf{F}^3\, b\right]$?
  - $\mathbb{P}\left[\mathsf{F}^3\, b\right] = \frac{3}{4} + \frac{1}{4} \cdot \frac{1}{4} + \frac{1}{4} \cdot \frac{1}{4} \cdot \frac{3}{4} = \frac{55}{64} \approx 0.859$
- $\mathbb{P}[\mathsf{F}\, c]$?
  - $\mathbb{P}[\mathsf{F}\, c] = 1$
- $\mathbb{P}[\mathsf{F}\, b]$?

Exemples



- $\mathbb{P}[\mathsf{F}\, a]$?
  - $\mathbb{P}[\mathsf{F}\, a] = 1$
- $\mathbb{P}\left[\mathsf{F}^3\, b\right]$?
  - $\mathbb{P}\left[\mathsf{F}^3\, b\right] = \frac{3}{4} + \frac{1}{4} \cdot \frac{1}{4} + \frac{1}{4} \cdot \frac{1}{4} \cdot \frac{3}{4} = \frac{55}{64} \approx 0.859$
- $\mathbb{P}[\mathsf{F}\, c]$?
  - $\mathbb{P}[\mathsf{F}\, c] = 1$
- $\mathbb{P}[\mathsf{F}\, b]$?
  - $\mathbb{P}[\mathsf{F}\, b] = 1 - \frac{1}{8}(1 + \frac{1}{16} + (\frac{1}{16})^2 + \dots) = \frac{13}{15} \approx 0.866$

Probabilité d'accessibilité à horizon borné

Lemma

La probabilité $\mathbb{P}\left[\mathsf{F}^{\ell}\, p\right]$ *pour une chaîne de Markov* M *peut être calculée en temps polynomial en* $|M|$ *et linéaire en* ℓ.

Probabilité d'accessibilité à horizon borné

Lemma

La probabilité $\mathbb{P}\left[\mathsf{F}^{\ell}\, p\right]$ *pour une chaîne de Markov* M *peut être calculée en temps polynomial en* $|M|$ *et linéaire en* ℓ.

- $\mathbb{P}\left[\mathsf{F}^{\ell}\, p\right]$ est la mesure de l'union des cylindres $\mathrm{Chemins}_M(\rho)$ où :
  - ρ est un chemin fini $s_{\mathsf{init}} s_1 \dots s_i$ avec $|\rho| \leq \ell$
  - dont le dernier état s_i satisfait p
  - et tel que pour tout $j < i$, s_j ne satisfait pas p.

Probabilité d'accessibilité à horizon borné

Lemma

La probabilité $\mathbb{P}\left[\mathsf{F}^{\ell}\, p\right]$ *pour une chaîne de Markov* M *peut être calculée en temps polynomial en* $|M|$ *et linéaire en* ℓ.

- $\mathbb{P}\left[\mathsf{F}^{\ell}\, p\right]$ est la mesure de l'union des cylindres $\mathrm{Chemins}_M(\rho)$ où :
  - ρ est un chemin fini $s_{\mathsf{init}} s_1 \dots s_i$ avec $|\rho| \leq \ell$
  - dont le dernier état s_i satisfait p
  - et tel que pour tout $j < i$, s_j ne satisfait pas p.

- Soit $\mathcal{C} \subseteq \mathrm{Chemins}\mathsf{F}_M^{\leq \ell}(s_{\mathsf{init}})$ l'ensemble des chemins ρ de cette forme.
- Énumérer les chemins de $\mathcal{C}$ et sommer les probabilités ?
  $\rightsquigarrow$ exponentiel en ℓ

Meilleure approche : programmation dynamique

calcul récursif de $\mathbb{P}^s\left[\mathsf{F}^\ell\, p\right]$ pour tout état $s \in S$ et tout horizon $\ell \in \mathbb{N}$.

- Si s satisfait p, alors $\mathbb{P}^s\left[\mathsf{F}^\ell\, p\right] = 1$. Sinon,

Meilleure approche : programmation dynamique

calcul récursif de $\mathbb{P}^s\left[\mathsf{F}^\ell\, p\right]$ pour tout état $s \in S$ et tout horizon $\ell \in \mathbb{N}$.

- Si s satisfait p, alors $\mathbb{P}^s\left[\mathsf{F}^\ell\, p\right] = 1$. Sinon,
- Si $\ell = 1$, alors $\mathbb{P}^s\left[\mathsf{F}^1\, p\right] = \sum_{\substack{s \to s' \\ p \in L(s')}} \mathbb{P}(s, s')$.

Meilleure approche : programmation dynamique

calcul récursif de $\mathbb{P}^s\left[\mathsf{F}^\ell\, p\right]$ pour tout état $s \in S$ et tout horizon $\ell \in \mathbb{N}$.

- Si s satisfait p, alors $\mathbb{P}^s\left[\mathsf{F}^\ell\, p\right] = 1$. Sinon,
- Si $\ell = 1$, alors $\mathbb{P}^s\left[\mathsf{F}^1\, p\right] = \sum_{\substack{s \to s' \\ p \in L(s')}} \mathbb{P}(s, s')$.
- Si $\ell > 1$, alors

$$\mathbb{P}^s\left[\mathsf{F}^\ell\, p\right] = \mathbb{P}^s\left[\mathsf{F}^1\, p\right] + \sum_{\substack{s \to s' \\ p \notin L(s')}} \mathbb{P}(s, s')\mathbb{P}^{s'}\left[\mathsf{F}^{\ell-1}\, p\right]$$

En effet, on obtient ce résultat en décomposant $\sum_{\rho \in \mathcal{C}} \mathbb{P}(\rho)$ en deux : les chemins $\rho \in \mathcal{C}$ de taille 1 qui atteint p directement, et ceux qui commencent par une transition $s \to s'$ puis atteignent p depuis s'.

Probabilité d'accessibilité (horizon non borné)

Lemma

La probabilité $\mathbb{P}[\mathsf{F}\, p]$ *pour une chaîne de Markov* M *peut être calculée en temps polynomial en* $|M|$.

Probabilité d'accessibilité (horizon non borné)

Lemma

La probabilité $\mathbb{P}[\mathsf{F}\, p]$ *pour une chaîne de Markov* M *peut être calculée en temps polynomial en* $|M|$.

- Soit $\mathcal{C} \subseteq \mathrm{CheminsF}_M(s_{\mathsf{init}})$ l'ensemble des chemins finis $\rho = s_{\mathsf{init}} s_1 \dots s_i$ dont le dernier état s_i satisfait p et tel que pour tout $j < i$, s_j ne satisfait pas p.
- $\rightsquigarrow \mathbb{P}[\mathsf{F}\, p] = \sum_{\rho \in \mathcal{C}} \mathbb{P}(\rho)$
- Somme indénombrable ?

Système d'équations linéaire

On reprends l'approche précédente :

- Si s satisfait p, alors $\mathbb{P}^s[\mathrm{F}\, p] = 1$. Sinon,

Système d'équations linéaire

On reprends l'approche précédente :

- Si s satisfait p, alors $\mathbb{P}^s[\mathrm{F}\, p] = 1$. Sinon,
- En partitionnant $\mathcal{C}$ entre les chemins de taille 1 qui atteint p directement, et ceux qui commencent par $s \to s'$ puis atteignent p depuis s',

$$\mathbb{P}^s[\mathrm{F}\, p] = \sum_{\substack{s \to s' \\ p \in L(s')}} \mathbb{P}(s, s') + \sum_{\substack{s \to s' \\ p \notin L(s')}} \mathbb{P}(s, s') \mathbb{P}^{s'}[\mathrm{F}\, p]$$

Système d'équations linéaire

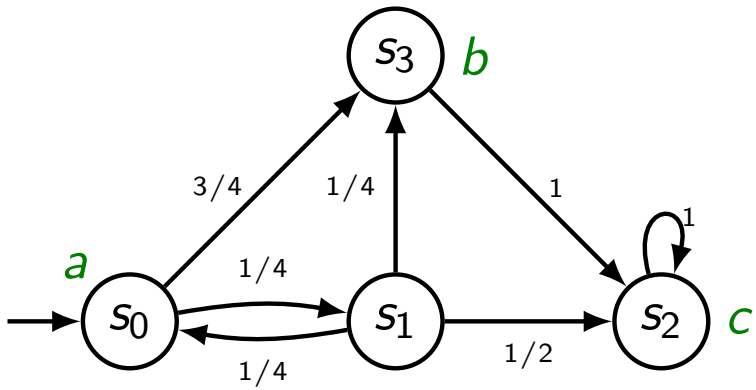
On reprends l'approche précédente :

- Si s satisfait p, alors $\mathbb{P}^s[\mathrm{F}\, p] = 1$. Sinon,
- En partitionnant $\mathcal{C}$ entre les chemins de taille 1 qui atteint p directement, et ceux qui commencent par $s \to s'$ puis atteignent p depuis s',

$$\mathbb{P}^s[\mathrm{F}\, p] = \sum_{\substack{s \to s' \\ p \in L(s')}} \mathbb{P}(s, s') + \sum_{\substack{s \to s' \\ p \notin L(s')}} \mathbb{P}(s, s') \mathbb{P}^{s'}[\mathrm{F}\, p]$$

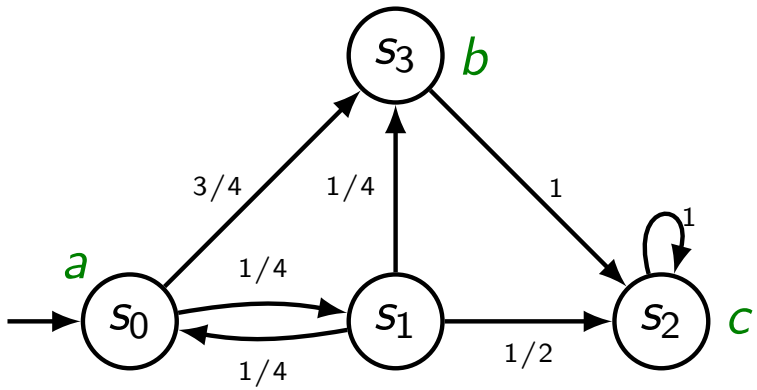
En posant pour chaque $s \in S$ une variable x_s qui représente $\mathbb{P}^s[\mathrm{F}\, p]$, on a donc décrit un système d'équations linéaires sur les variables x_s, de la forme $x_s = \sum_{s'} \mathbb{P}(s, s') x_{s'} + b_s$.
$\rightsquigarrow$ pour la plus petite solution du système d'équation : $x_s = \mathbb{P}^s[\mathrm{F}\, p]$

Exemples



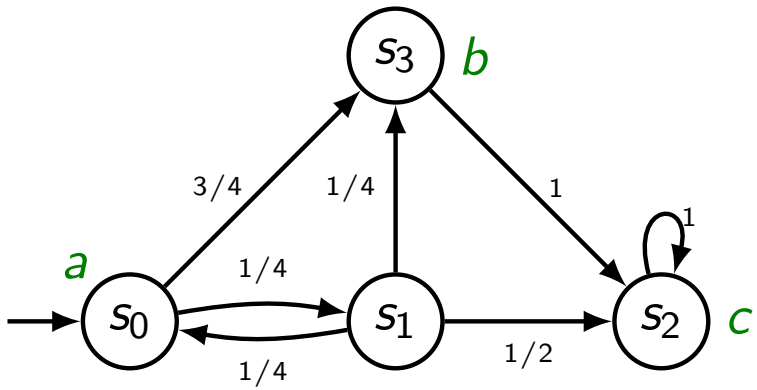
- $\mathbb{P}[\mathrm{F}\, b]$ depuis s_0 ?

Exemples



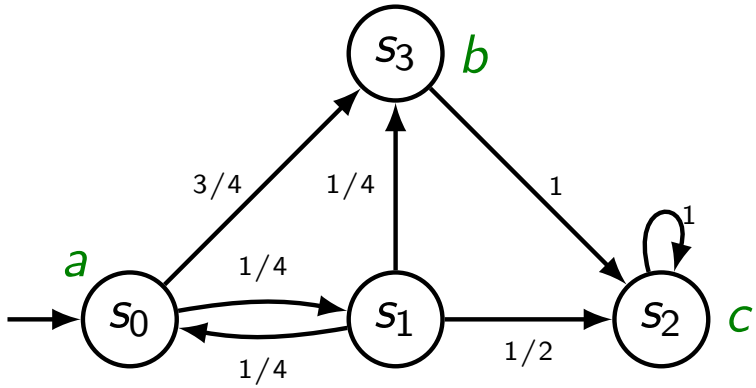
- $\mathbb{P}[\mathrm{F}\, b]$ depuis s_0 ?
  - On pose $x_0 = \mathbb{P}^{s_0}[\mathrm{F}\, b]$, $x_1 = \mathbb{P}^{s_1}[\mathrm{F}\, b]$, x_2, x_3 idem

Exemples



- $\mathbb{P}[\mathrm{F}\, b]$ depuis s_0 ?
  - On pose $x_0 = \mathbb{P}^{s_0}[\mathrm{F}\, b]$, $x_1 = \mathbb{P}^{s_1}[\mathrm{F}\, b]$, x_2, x_3 idem
  - $$\begin{cases} x_0 = \frac{3}{4}x_3 + \frac{1}{4}x_1 \\ x_1 = \frac{1}{4}x_0 + \frac{1}{4}x_3 + \frac{1}{2}x_2 \\ x_2 = x_2 \\ x_3 = 1 \end{cases} \quad \rightsquigarrow x_0 = \frac{3}{4} + \frac{1}{4}\left(\frac{1}{4}x_0 + \frac{1}{4}\right)$$

Exemples



- $\mathbb{P}[\mathrm{F}\, b]$ depuis s_0 ?
  - On pose $x_0 = \mathbb{P}^{s_0}[\mathrm{F}\, b]$, $x_1 = \mathbb{P}^{s_1}[\mathrm{F}\, b]$, x_2, x_3 idem
  - $$\begin{cases} x_0 = \frac{3}{4}x_3 + \frac{1}{4}x_1 \\ x_1 = \frac{1}{4}x_0 + \frac{1}{4}x_3 + \frac{1}{2}x_2 \\ x_2 = x_2 \\ x_3 = 1 \end{cases} \quad \rightsquigarrow x_0 = \frac{3}{4} + \frac{1}{4}\left(\frac{1}{4}x_0 + \frac{1}{4}\right)$$
  - $\rightsquigarrow x_0\left(1 - \frac{1}{16}\right) = \frac{3}{4} + \frac{1}{16} \rightsquigarrow x_0 = \frac{16}{15}\frac{13}{16} = \frac{13}{15}$

Accessibilité sous condition

Definition

On dit que $\rho \in \text{Chemins}_M$ satisfait *la propriété d'accessibilité* $p_2 \in \text{PA}$ sous la *condition* $p_1 \in \text{PA}$ si il existe i tel que $\rho[i]$ satisfait p_2 et que pour tout $j < i$, $\rho[i]$ satisfait p_1.

Accessibilité sous condition

Definition

On dit que $\rho \in \text{Chemins}_M$ satisfait *la propriété d'accessibilité* $p_2 \in \text{PA}$ sous la *condition* $p_1 \in \text{PA}$ si il existe i tel que $\rho[i]$ satisfait p_2 et que pour tout $j < i$, $\rho[i]$ satisfait p_1.

- Dans ce cas, on écrit $\rho \models p_1 \,\mathrm{U}\, p_2$
- $p_1 \,\mathrm{U}\, p_2$ se lit "p_1 est maintenu jusqu'à ce que p_2 soit atteint", l'opérateur U venant du mot anglais *until*.
- Opération issue des logiques temporelles LTL et CTL
- variante U^{ℓ}

Accessibilité sous condition

Definition

On dit que $\rho \in \text{Chemins}_M$ satisfait *la propriété d'accessibilité* $p_2 \in \text{PA}$ sous la *condition* $p_1 \in \text{PA}$ si il existe i tel que $\rho[i]$ satisfait p_2 et que pour tout $j < i$, $\rho[i]$ satisfait p_1.

- Dans ce cas, on écrit $\rho \models p_1 \,\mathsf{U}\, p_2$
- $p_1 \,\mathsf{U}\, p_2$ se lit "p_1 est maintenu jusqu'à ce que p_2 soit atteint", l'opérateur U venant du mot anglais *until*.
- Opération issue des logiques temporelles LTL et CTL
- variante U^ℓ

Lemma

Les probabilités $\mathbb{P}\left[p_1 \,\mathsf{U}\, p_2\right]$ *et* $\mathbb{P}\left[p_1 \,\mathsf{U}^\ell\, p_2\right]$ *pour une chaîne de Markov* M *peuvent être calculées en temps polynomial en* $|M|$*, et linéaire en* ℓ *pour le cas à horizon borné.*

Propriété de sûreté

Autre variante, $\mathsf{G}\, p$:

- Se lit "*Generally* p"
- demande qu'une propriété atomique p soit maintenue tout au long d'une exécution du système, de sorte que $\rho \models \mathsf{G}\, p$ si tous les états s visités par ρ satisfont p.

Propriété de sûreté

Autre variante, $\mathsf{G}\, p$:

- Se lit "*Generally* p"
- demande qu'une propriété atomique p soit maintenue tout au long d'une exécution du système, de sorte que $\rho \models \mathsf{G}\, p$ si tous les états s visités par ρ satisfont p.

- propriété duale des propriétés d'accessibilité, de sorte que $\mathbb{P}\left[\mathsf{G}\, p\right] = 1 - \mathbb{P}\left[\mathsf{F}(\neg p)\right]$

Model-checkers probabiliste

- implémentent ces calculs de manière efficace
- supportent des propriétés plus complexes qu'une simple condition d'accessibilité
- par exemple : combinaisons booléennes d'objectifs

Model-checkers probabiliste

- implémentent ces calculs de manière efficace
- supportent des propriétés plus complexes qu'une simple condition d'accessibilité
- par exemple : combinaisons booléennes d'objectifs

- Les logiciels PRISM, et plus récemment STORM sont des model-checkers probabilistes.
- langage de spécification ?

CTL Probabiliste

Definition (formule PCTL)

Une formule de PCTL est générée par le symbole non-terminal Φ de la grammaire suivante :

$$\Phi := p \mid \neg\Phi \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid \mathbb{P}[\varphi] \bowtie c$$
$$\varphi := \mathsf{X}\,\Phi \mid \Phi_1\,\mathsf{U}^{\ell}\,\Phi_2 \mid \Phi_1\,\mathsf{U}\,\Phi_2$$

où p est une proposition atomique de PA, ℓ est une valeur d'horizon dans $\mathbb{N}$, c est un seuil de probabilité dans $[0, 1]$ et où $\bowtie \in \{<, \leq, =, \neq, \geq, >\}$ est un opérateur de comparaison.

CTL Probabiliste

Definition (formule PCTL)

Une formule de PCTL est générée par le symbole non-terminal Φ de la grammaire suivante :

$$\Phi := p \mid \neg\Phi \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid \mathbb{P}[\varphi] \bowtie c$$
$$\varphi := \mathsf{X}\,\Phi \mid \Phi_1\,\mathsf{U}^{\ell}\,\Phi_2 \mid \Phi_1\,\mathsf{U}\,\Phi_2$$

où p est une proposition atomique de PA, ℓ est une valeur d'horizon dans $\mathbb{N}$, c est un seuil de probabilité dans $[0,1]$ et où $\bowtie \in \{<, \leq, =, \neq, \geq, >\}$ est un opérateur de comparaison.

- Φ formules d'états
- φ formules de chemins

CTL Probabiliste

Definition (formule PCTL)

Une formule de PCTL est générée par le symbole non-terminal Φ de la grammaire suivante :

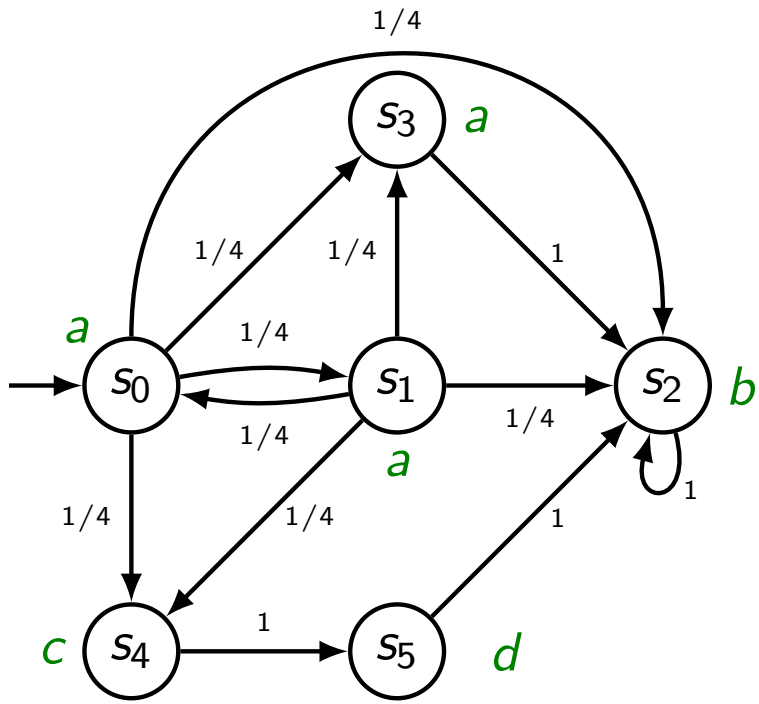
$$\Phi := p \mid \neg\Phi \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid \mathbb{P}[\varphi] \bowtie c$$
$$\varphi := \mathsf{X}\,\Phi \mid \Phi_1\,\mathsf{U}^{\ell}\,\Phi_2 \mid \Phi_1\,\mathsf{U}\,\Phi_2$$

où p est une proposition atomique de PA, ℓ est une valeur d'horizon dans $\mathbb{N}$, c est un seuil de probabilité dans $[0, 1]$ et où $\bowtie \in \{<, \leq, =, \neq, \geq, >\}$ est un opérateur de comparaison.

- Φ formules d'états
- φ formules de chemins

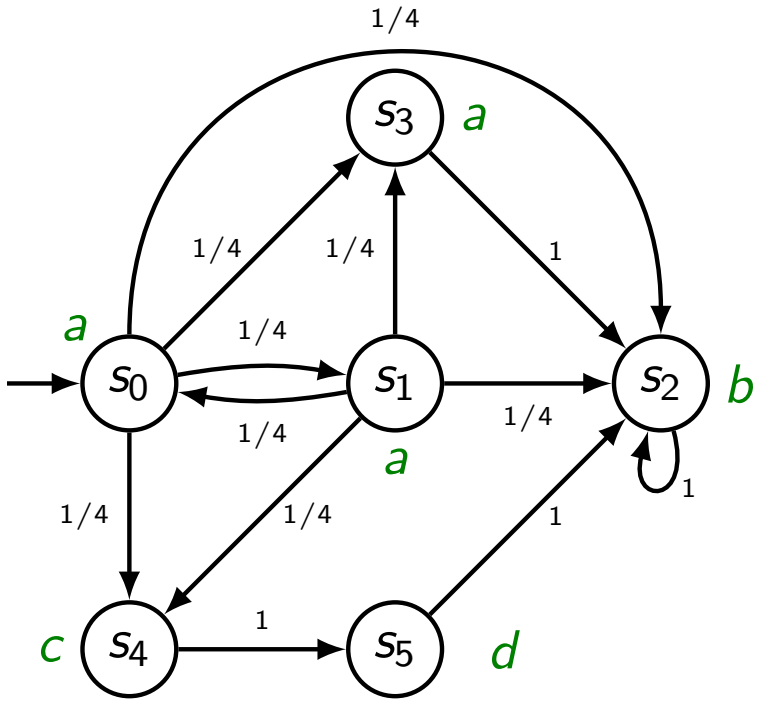
- X est l'opérateur "Next"
- F et G peuvent être définies à partir de U

Exemple



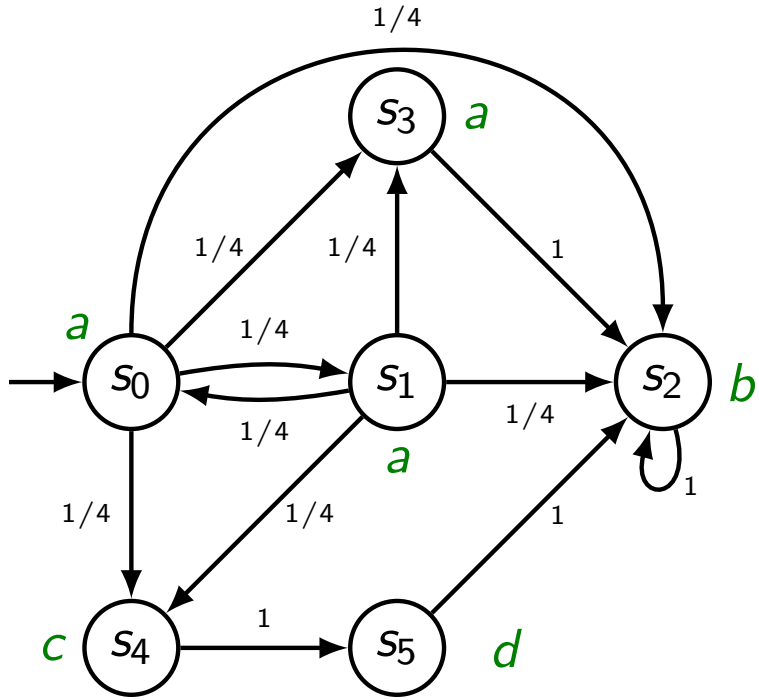
- $\mathbb{P}[\mathrm{X}\, c] \leq \frac{1}{2}$:
  La probabilité que le prochain état ai l'étiquette c est inférieure à $\frac{1}{2}$.

Exemple



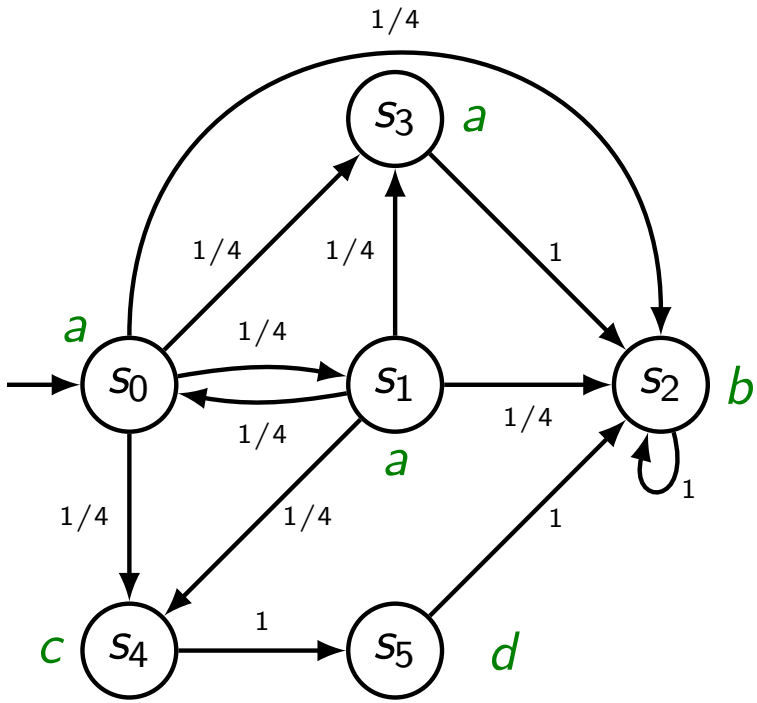
- $(\mathbb{P}[\mathsf{X}\, d] \neq 0) \vee (\mathbb{P}[\mathsf{F}\, b] = 1)$:
  La probabilité que le prochain état ai l'étiquette d est non nulle, ou bien b est visité presque sûrement.

Exemple



- $\neg(\mathbb{P}[a \,\mathsf{U}\, b] = \frac{3}{4}) \wedge (\mathbb{P}[(a \vee c \vee d) \,\mathsf{U}\, b] = 1)$:
  Un chemin tiré dans M ne maintiens pas a jusqu'à atteindre b avec une probabilité de $\frac{3}{4}$, par contre il maintient "a ou c ou d" jusqu'à atteindre b avec probabilité 1.

Exemple



- $\mathbb{P}\left[\mathsf{G}(\mathbb{P}\left[\mathsf{F}^2\, s_2\right] \geq \frac{9}{16})\right] = 1$:
  Pour presque tous les chemins tirés dans M, il est vrai que depuis n'importe quel état s ainsi visité la probabilité d'aller en b en au plus deux étapes depuis s est d'au moins $\frac{9}{16}$.

Sémantique

Definition (sémantique de PCTL)

Étant donné une chaîne de Markov M d'états S, on définit :

- la sémantique d'une formule d'état Φ, notée $[\![\Phi]\!]_M$, comme un sous-ensemble de S (les états satisfaisant la formule Φ).
- la sémantique d'une formule de chemin ϕ depuis un état de départ s, notée $[\![\varphi]\!]^s_M$, comme un ensemble mesurable de chemins infinis de M qui débutent en s

Définition inductive

Definition (sémantique de PCTL)

Ces deux sémantiques sont définies inductivement de la manière suivante :

$$
\begin{aligned}
[\![p]\!]_M &= \{s \in S \mid p \in L(s)\} \\
[\![\neg\Phi]\!]_M &= S \setminus [\![\Phi]\!]_M \\
[\![\Phi_1 \wedge \Phi_2]\!]_M &= [\![\Phi_1]\!]_M \cap [\![\Phi_2]\!]_M \\
[\![\Phi_1 \vee \Phi_2]\!]_M &= [\![\Phi_1]\!]_M \cup [\![\Phi_2]\!]_M \\
[\![\mathbb{P}[\varphi] \bowtie c]\!]_M &= \{s \in S \mid \mu_M([\![\varphi]\!]^s_M) \bowtie c\} \\
[\![\mathsf{X}\,\Phi]\!]^s_M &= \{\rho \in \mathsf{Chemins}(s) \mid \rho[1] \in [\![\Phi]\!]_M\} \\
\left[\!\left[\Phi_1\,\mathsf{U}^{\ell}\,\Phi_2\right]\!\right]^s_M &= \{\rho \in \mathsf{Chemins}(s) \mid \exists j \leq \ell, \rho[j] \in [\![\Phi_2]\!]_M \\
&\qquad\qquad \wedge \forall i < j, \rho[i] \in [\![\Phi_1]\!]_M\} \\
[\![\Phi_1\,\mathsf{U}\,\Phi_2]\!]^s_M &= \{\rho \in \mathsf{Chemins}(s) \mid \exists j \in \mathbb{N}, \rho[j] \in [\![\Phi_2]\!]_M \\
&\qquad\qquad \wedge \forall i < j, \rho[i] \in [\![\Phi_1]\!]_M\}
\end{aligned}
$$

Model-checking de PCTL

Proposition

Le problème du *model-checking* pour une formule Φ de PCTL et une chaîne de Markov M est dans PTIME.

- calculer, pour chaque formule d'état Φ' qui est une sous formule de Φ, l'ensemble des états la satisfaisant, c'est-à-dire $[\![\Phi']\!]_M$

Model-checking de PCTL

Proposition

Le problème du *model-checking* pour une formule Φ de PCTL et une chaîne de Markov M est dans PTIME.

- calculer, pour chaque formule d'état Φ' qui est une sous formule de Φ, l'ensemble des états la satisfaisant, c'est-à-dire $[\![\Phi']\!]_M$

- calcul inductif : en partant des formules atomiques et en remontant l'arbre syntactique de la formule Φ de bas en haut
- unions, intersections et compléments pour les opérations booléennes
- opérations temporelles : calculs détaillé précédemment

Model-checking de PCTL

Proposition

Le problème du *model-checking* pour une formule Φ de PCTL et une chaîne de Markov M est dans PTIME.

- calculer, pour chaque formule d'état Φ' qui est une sous formule de Φ, l'ensemble des états la satisfaisant, c'est-à-dire $[\![\Phi']\!]_M$
- calcul inductif : en partant des formules atomiques et en remontant l'arbre syntactique de la formule Φ de bas en haut
- unions, intersections et compléments pour les opérations booléennes
- opérations temporelles : calculs détaillé précédemment
- la complexité de cette procédure est dans $|M|^{\mathcal{O}(1)}|\Phi|\ell_{\max}$.

Fin partie 1