Vérification de modèles stochastiques et synthèse de contrôleurs à spécifications probabilistes

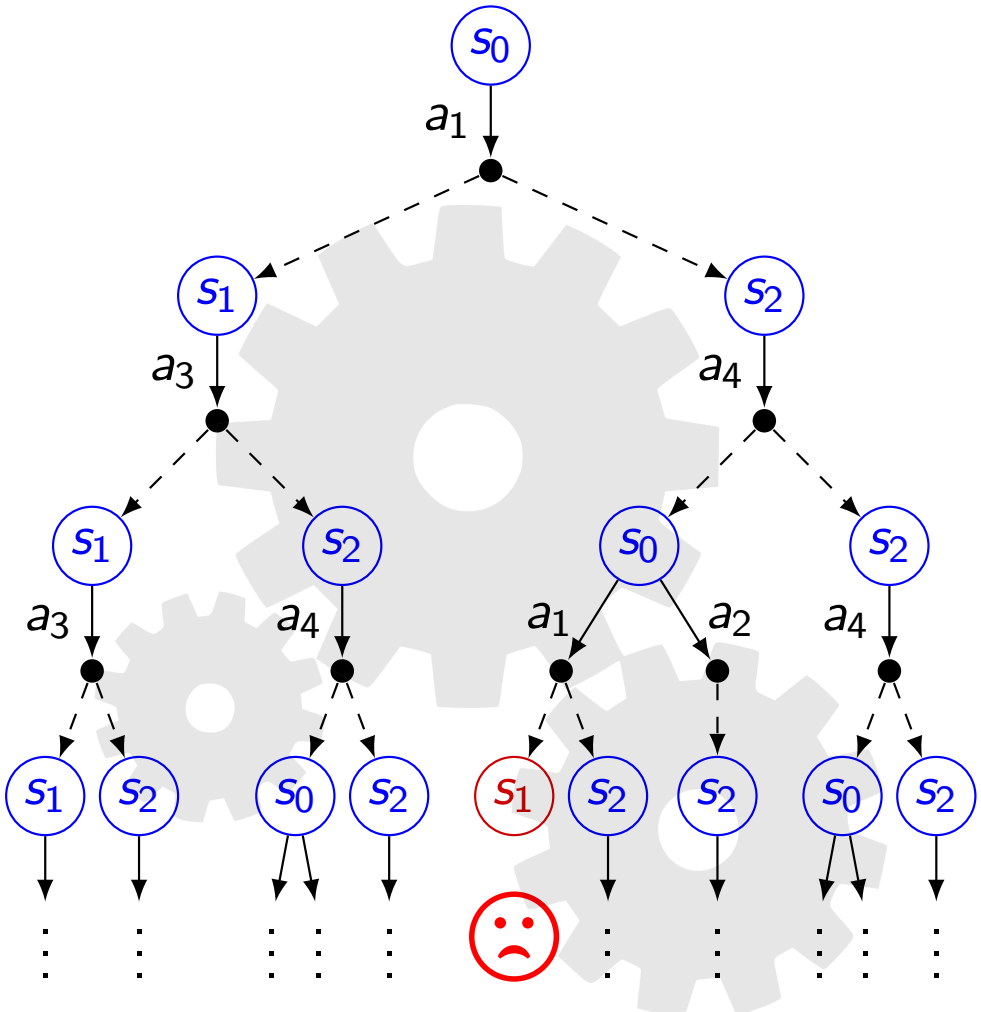
EJCIM 2024

Damien Busatto-Gaston

Université Paris-Est Créteil, LACL

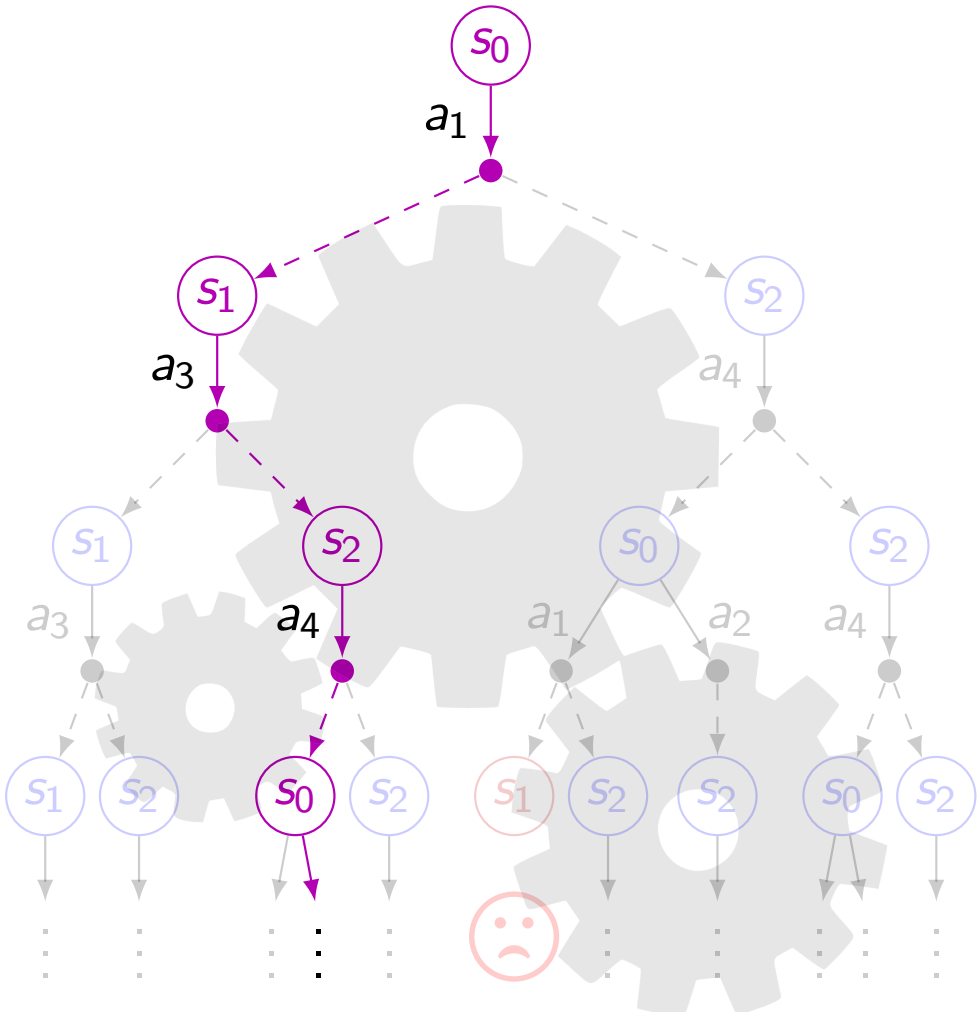
21 juin 2024

Tests vs model-checking vs synthèse



$\models$ Spécification

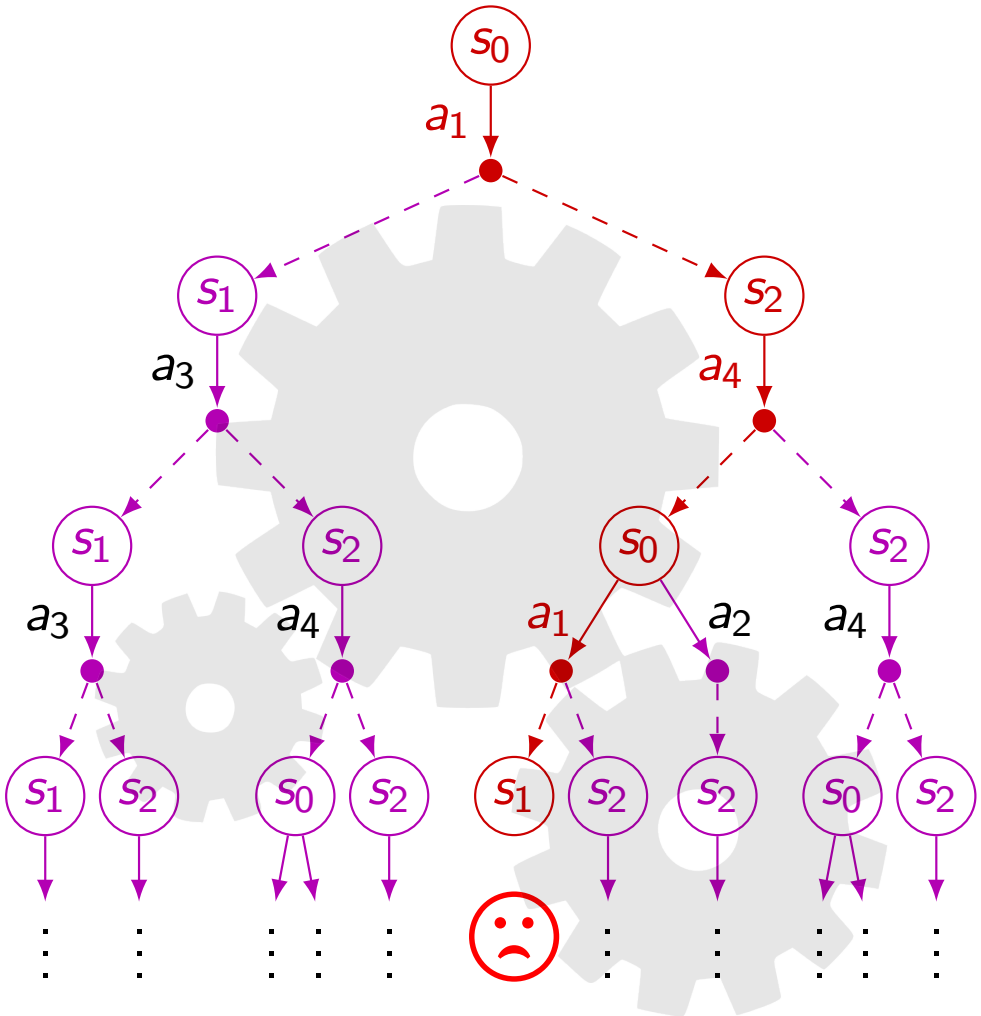
Tests vs model-checking vs synthèse



$\models$ Spécification

- Test

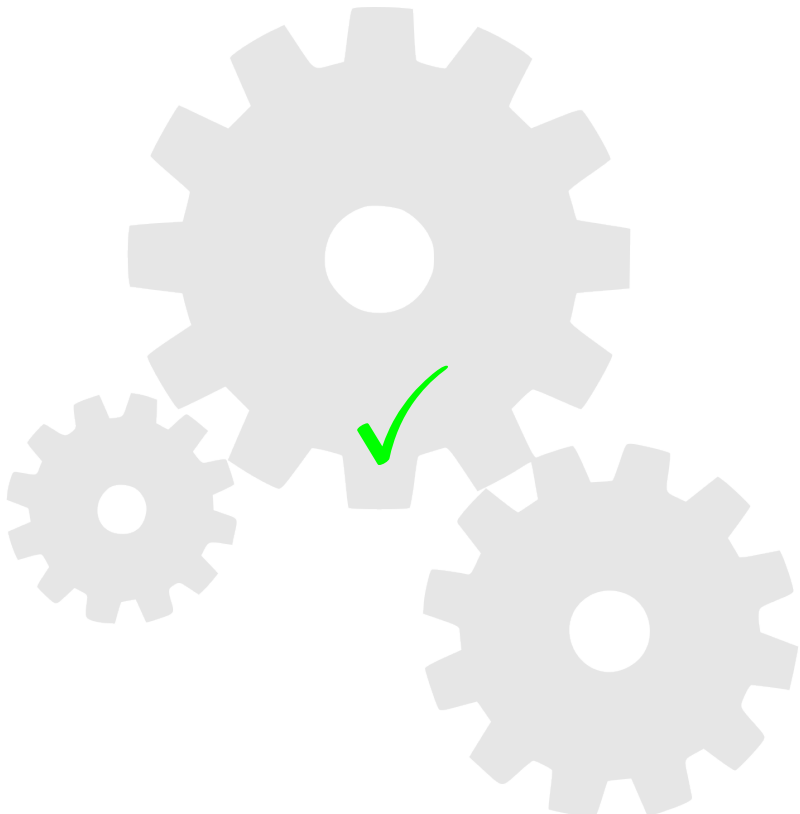
Tests vs model-checking vs synthèse



$\models$ Spécification

- Model-checking : Système $\models$ Spécification

Tests vs model-checking vs synthèse

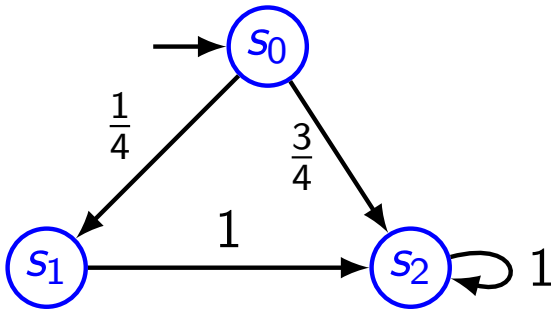


$\Leftarrow$ Spécification

- Model-checking : $\boxed{\text{Système}} \models \text{Spécification}$
- Synthèse : Spécification $\rightarrow \boxed{\text{Système}}$

Résultats pour chaînes de Markov

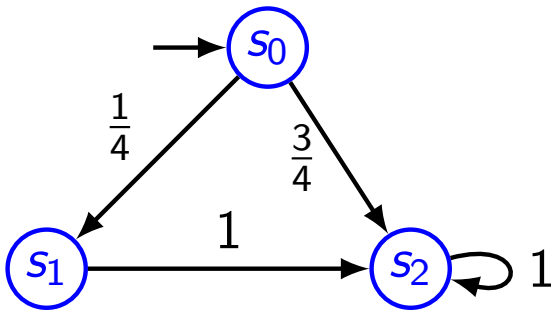
- model : Chaîne de Markov M



- spécification : formule ϕ en logique probabiliste PCTL

Résultats pour chaînes de Markov

- model : Chaîne de Markov M

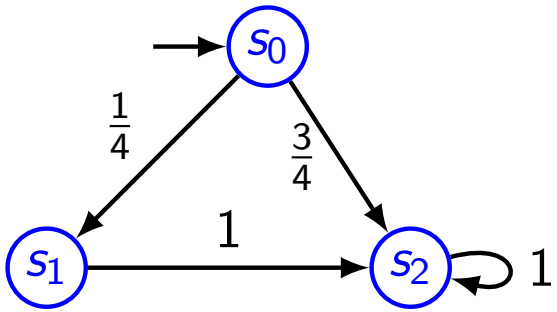


- spécification : formule ϕ en logique probabiliste PCTL

- *model-checking* : étant donné M et ϕ, est-ce que $M \models \phi$?
  - $\leadsto$ PTIME

Résultats pour chaînes de Markov

- model : Chaîne de Markov M



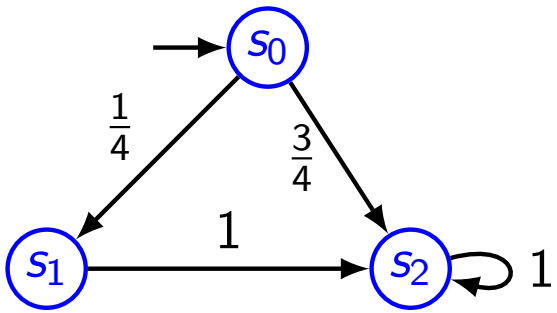
- spécification : formule ϕ en logique probabiliste PCTL

- *model-checking* : étant donné M et ϕ, est-ce que $M \models \phi$?
  - $\leadsto$ PTIME

- *satisfaisabilité* : étant donné ϕ, est-ce qu'il existe M tel que $M \models \phi$?

Résultats pour chaînes de Markov

- model : Chaîne de Markov M



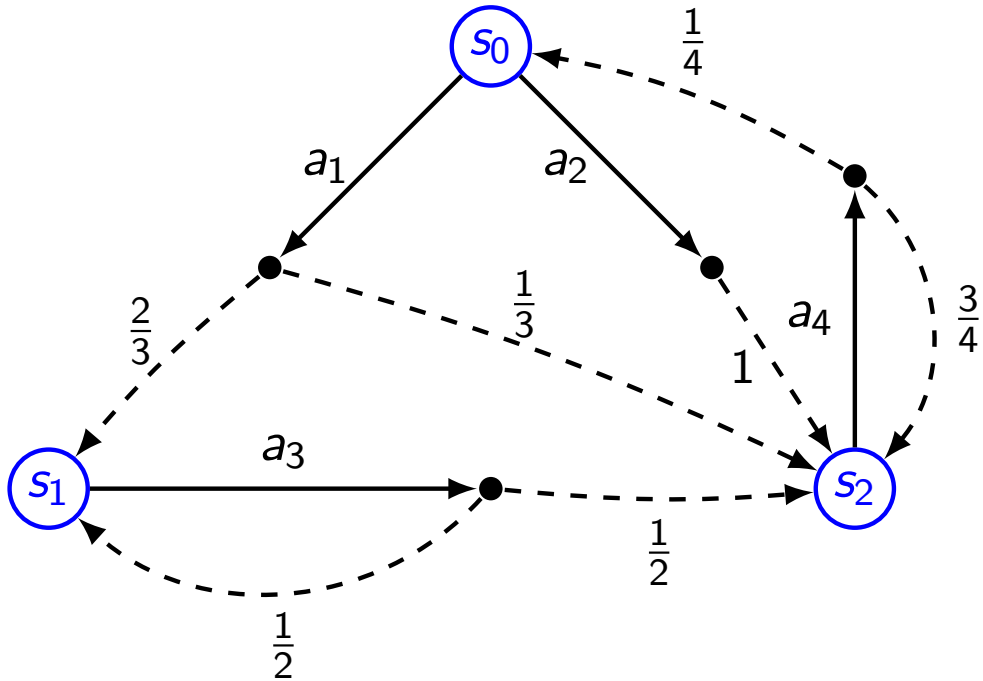
- spécification : formule ϕ en logique probabiliste PCTL

- *model-checking* : étant donné M et ϕ, est-ce que $M \models \phi$?
  - $\rightsquigarrow$ PTIME

- *satisfaisabilité* : étant donné ϕ, est-ce qu'il existe M tel que $M \models \phi$?
  - $\rightsquigarrow$ problème ouvert / indécidable

Processus de décision markovien

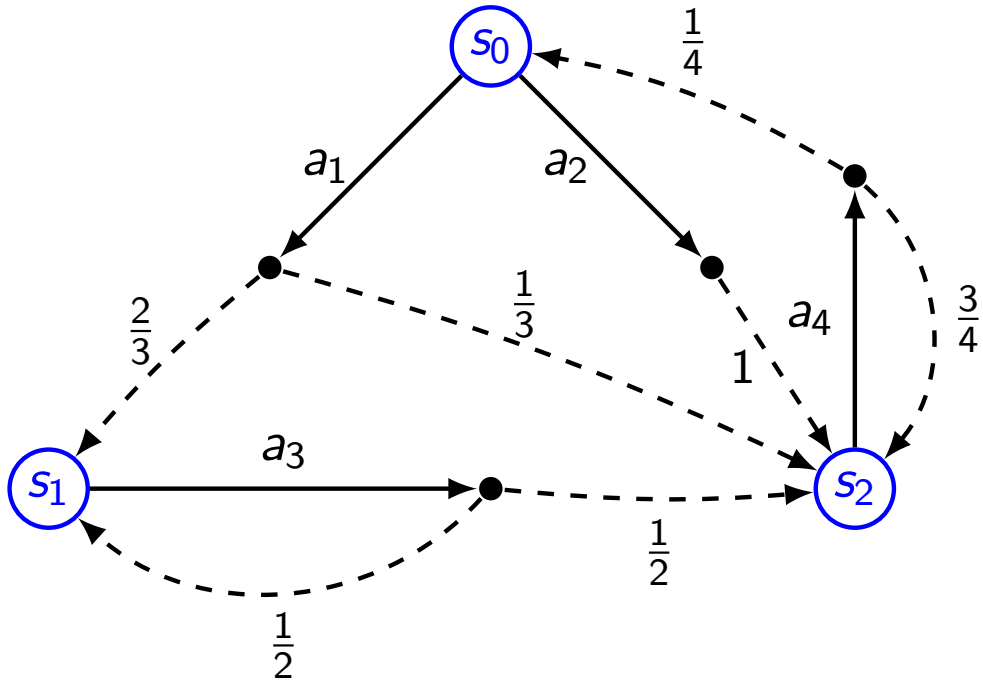
- Synthèse réactive ? non-déterminisme contrôlé ?
- modèle : un MDP $\mathcal{M}$



- spécification : formule ϕ en logique probabiliste

Processus de décision markovien

- Synthèse réactive ? non-déterminisme contrôlé ?
- modèle : un MDP $\mathcal{M}$



- spécification : formule ϕ en logique probabiliste

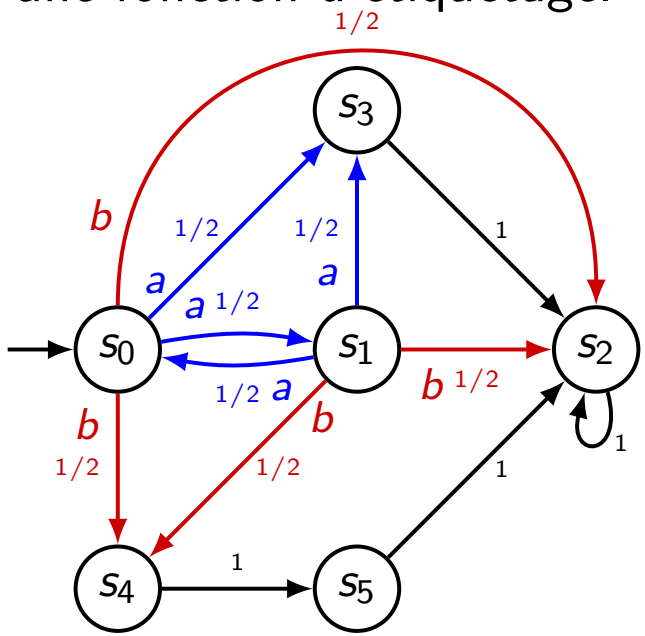
- *synthèse de stratégie* : étant donné $\mathcal{M}$ et ϕ, existe-t'il une stratégie σ de résolution du non-déterminisme telle que $\mathcal{M} \models_\sigma \phi$?

Formalisme

Definition

Un *processus de décision markovien* (MDP) est un tuple $\mathcal{M} = \langle S, A, s_{\text{init}}, \mathbb{P}, \text{PA}, L \rangle$, où

- S est un ensemble fini d'états,
- A est un ensemble fini d'actions,
- $s_{\text{init}} \in S$ est un état initial,
- $\mathbb{P} : S \times A \to \text{Dist}(S)$ 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

- On définit les chemins finis et infinis d'un MDP de la même manière que pour les chaînes de Markov
- différence : les transitions sont maintenant étiquetées par des actions.

Chemins

- On définit les chemins finis et infinis d'un MDP de la même manière que pour les chaînes de Markov
- différence : les transitions sont maintenant étiquetées par des actions.

- Exemple $\rho = s_0 \xrightarrow{a_0} s_1 \xrightarrow{a_1} s_2 \xrightarrow{a_2} \cdots$

Stratégies (ou politiques)

Definition

Une *stratégie* est une fonction $\sigma : S \to A$ qui associe à chaque état s une action $\sigma(s)$.

- déterministe
- sans mémoire

Des MDPs aux chaînes de Markov

Definition

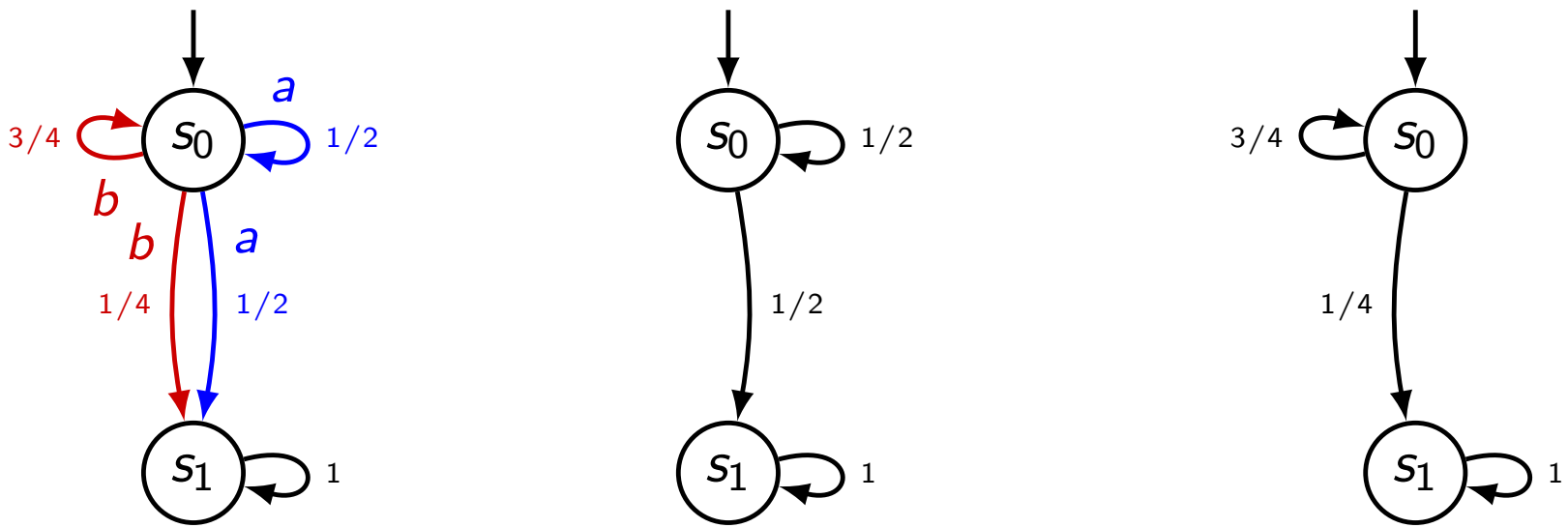
Un MDP $\mathcal{M} = \langle S, A, s_{\text{init}}, \mathbb{P}, \text{PA}, L \rangle$ équipé d'une stratégie σ définit une chaîne de Markov, notée $\mathcal{M}[\sigma]$, obtenue en appliquant les choix d'actions.

Des MDPs aux chaînes de Markov

Definition

Un MDP $\mathcal{M} = \langle S, A, s_{\text{init}}, \mathbb{P}, \text{PA}, L \rangle$ équipé d'une stratégie σ définit une chaîne de Markov, notée $\mathcal{M}[\sigma]$, obtenue en appliquant les choix d'actions.

- Formellement, on remplace la fonction de transition $\mathbb{P} : S \times A \to \text{Dist}(S)$ par $\mathbb{P}_\sigma : S \to \text{Dist}(S)$, avec $\forall s \in S, \mathbb{P}_\sigma(s) = \mathbb{P}(s, \sigma(s))$.



Synthèse de stratégies PCTL

Definition

Le *problème de la synthèse de stratégies* dans un MDP $\mathcal{M}$ et pour une formule PCTL Φ consiste à déterminer s'il existe une stratégie σ telle que $\mathcal{M}[\sigma] \models \Phi$.

Synthèse de stratégies PCTL

Definition

Le *problème de la synthèse de stratégies* dans un MDP $\mathcal{M}$ et pour une formule PCTL Φ consiste à déterminer s'il existe une stratégie σ telle que $\mathcal{M}[\sigma] \models \Phi$.

Proposition

Soit $\mathcal{M}$ un MDP et Φ une formule PCTL. Le problème de la synthèse de stratégies (déterministes et sans mémoire) est NP-complet.

Synthèse PCTL : dans NP

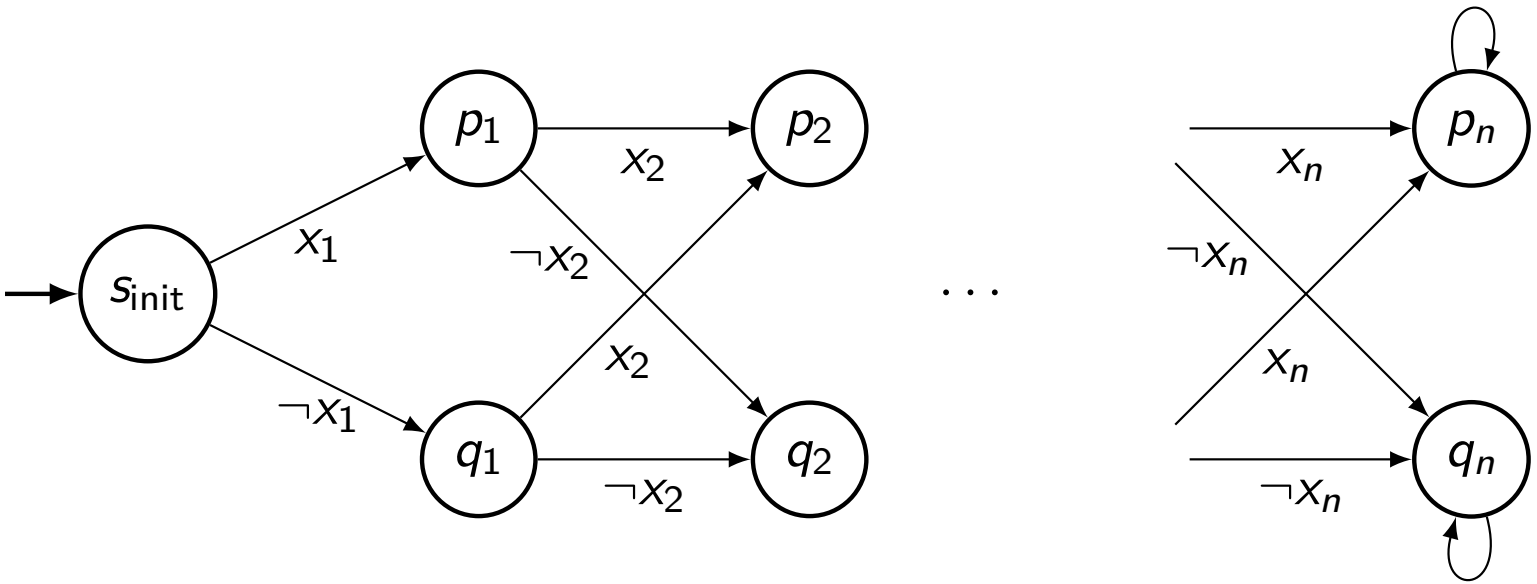
On montre que le problème est dans NP avec la procédure non-déterministe suivante :

Synthèse PCTL : dans NP

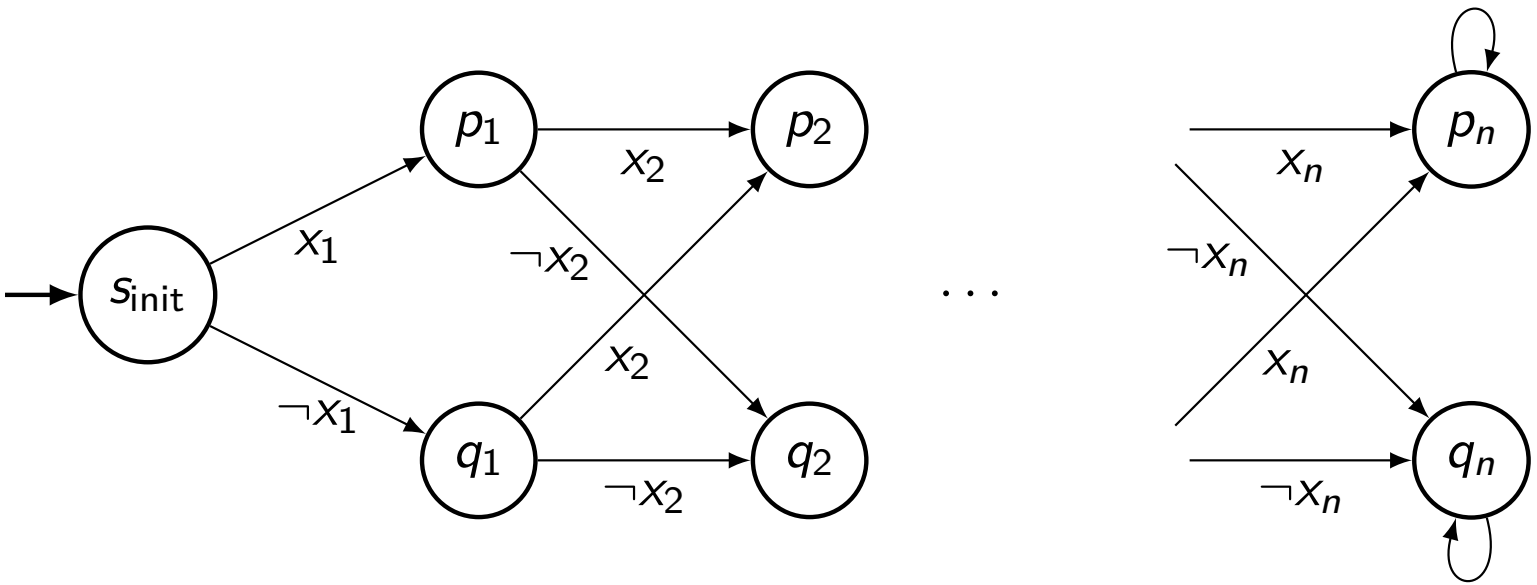
On montre que le problème est dans NP avec la procédure non-déterministe suivante :

- on devine une stratégie $\sigma : S \to A$
- on construit $\mathcal{M}[\sigma]$
- on vérifie que $\mathcal{M}[\sigma] \models \Phi$ en temps polynomial.

Synthèse PCTL : NP-difficile

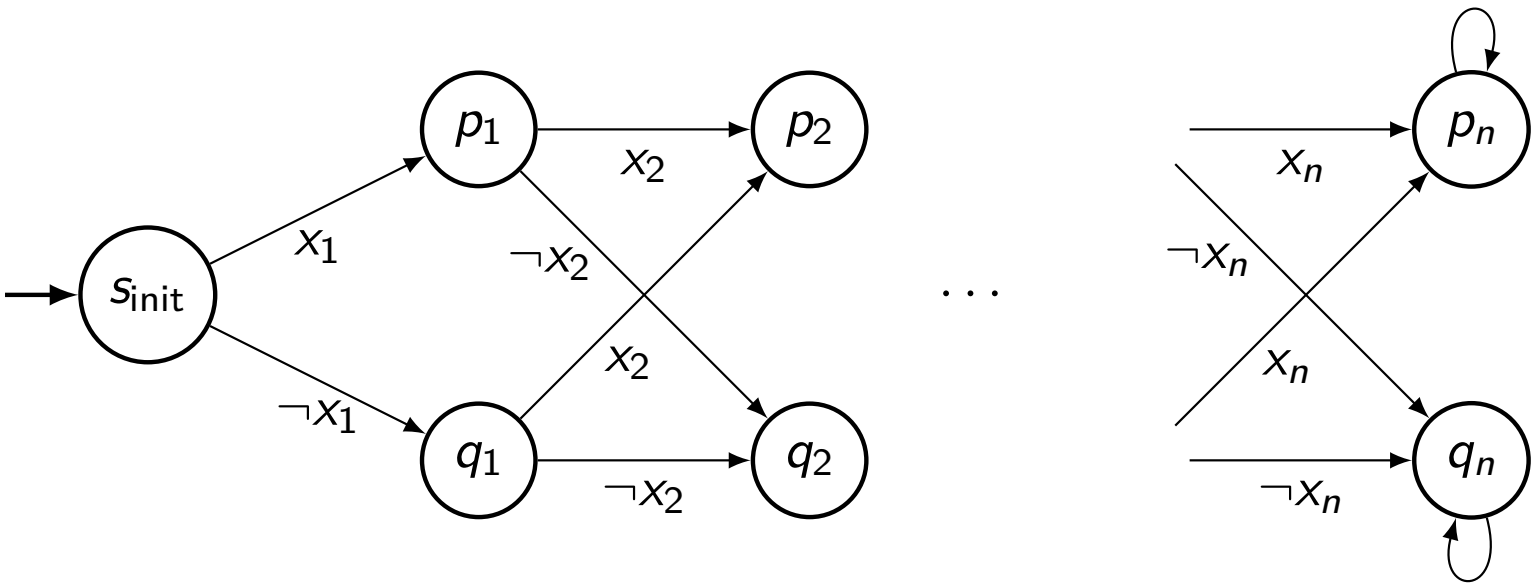


Synthèse PCTL : NP-difficile



- Réduction depuis 3-SAT : étant donné une formule $\bigwedge_{i=1}^{k}(\bigvee_{j=1}^{3} l_{i,j})$,
- On construit le MDP ci-dessus, sans probabilités

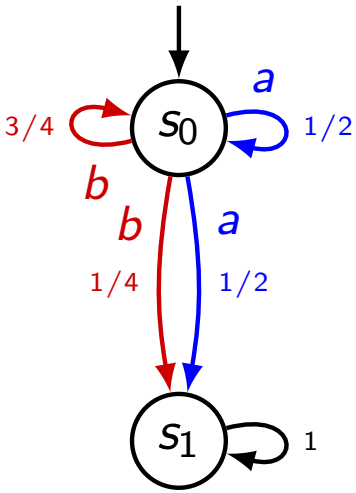
Synthèse PCTL : NP-difficile

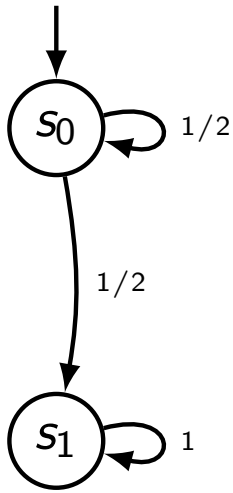


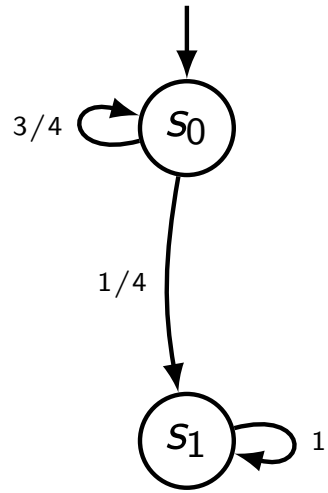
- Réduction depuis 3-SAT : étant donné une formule $\bigwedge_{i=1}^{k}(\bigvee_{j=1}^{3} l_{i,j})$,
- On construit le MDP ci-dessus, sans probabilités
- et la formule PCTL

$$\Phi = \bigwedge_{i=1}^{k}(\bigvee_{j=1}^{3} \mathbb{P}\left[\mathsf{F}\, l_{i,j}\right] = 1)$$

Des stratégies plus puissantes

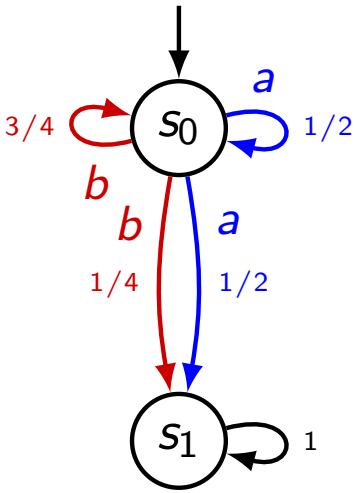






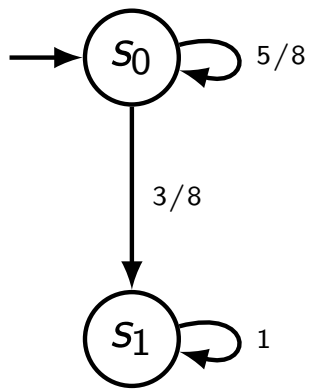
- On considère la formule PCTL $\mathbb{P}[\mathsf{X}\, s_1] > \frac{1}{2} \wedge \mathbb{P}[\mathsf{X}\, s_1] < \frac{1}{4}$
- pas de stratégie qui permette de satisfaire la formule ?

Des stratégies plus puissantes



- On considère la formule PCTL $\mathbb{P}[\mathsf{X}\, s_1] > \frac{1}{2} \wedge \mathbb{P}[\mathsf{X}\, s_1] < \frac{1}{4}$
- pas de stratégie qui permette de satisfaire la formule ?

- solution randomisée : choisir a et b de manière équiprobable



Stratégies stochastiques

Definition

Une *stratégie* (stochastique, sans mémoire) est une fonction $\sigma : S \to \text{Dist}(A)$ qui associe à chaque chemin fini s une distribution sur les actions.

- On définit le problème de synthèse de stratégie associé a cette classe

Stratégies stochastiques

Definition

Une *stratégie* (stochastique, sans mémoire) est une fonction $\sigma : S \to \text{Dist}(A)$ qui associe à chaque chemin fini s une distribution sur les actions.

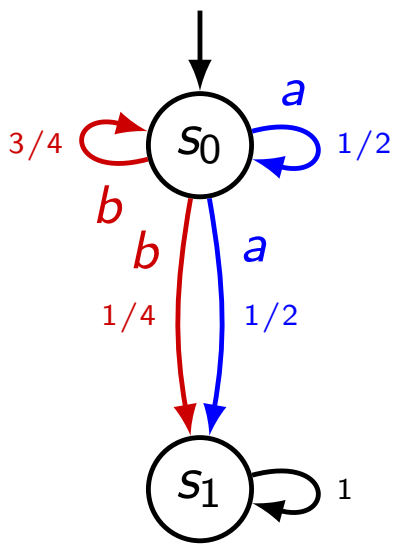
- On définit le problème de synthèse de stratégie associé a cette classe
- Comparaison avec le problème déterministe ?

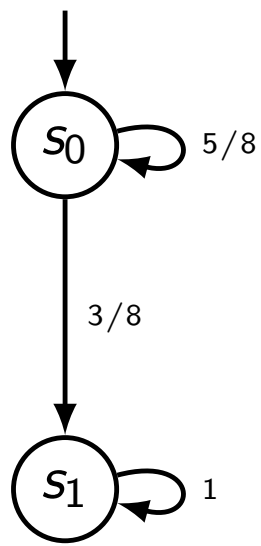
Synthèse PCTL, cas stochastique

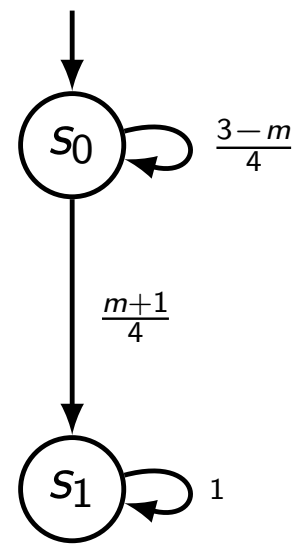
Proposition

Soit $\mathcal{M}$ un MDP et Φ une formule PCTL. Le problème de la synthèse de stratégies (stochastiques et sans mémoire) est dans EXPTIME.

- Idée de preuve : recherche de parametre







Théorie des réels du premier ordre

Definition

La *théorie des réels du premier ordre* (FO-$\mathbb{R}$) est l'ensemble de toutes les phrases bien formées de la logique du premier ordre utilisant :

- des quantificateurs universels et existentiels
- des combinaisons logiques d'égalités et d'inégalités de polynômes
- où les variables représentent des nombre réels.

Théorie des réels du premier ordre

Definition

La *théorie des réels du premier ordre* (FO-$\mathbb{R}$) est l'ensemble de toutes les phrases bien formées de la logique du premier ordre utilisant :

- des quantificateurs universels et existentiels
- des combinaisons logiques d'égalités et d'inégalités de polynômes
- où les variables représentent des nombre réels.

- exemple : $\exists x \forall y, x < 1 \wedge (xy < x \rightarrow y^2 \leq y)$
- généralisation des systèmes d'équations linéaires, ou polynomiales

Élimination des quantificateurs

- par Tarski-Seidenberg, FO-$\mathbb{R}$ est décidable :
  - elle admet une procédure d'élimination des quantificateurs doublement exponentielle
  - exemple : $\exists x, 0 < x \wedge x \leq 1 \rightsquigarrow 0 < 1$

Élimination des quantificateurs

- par Tarski-Seidenberg, FO-$\mathbb{R}$ est décidable :
  - elle admet une procédure d'élimination des quantificateurs doublement exponentielle
  - exemple : $\exists x, 0 < x \wedge x \leq 1 \rightsquigarrow 0 < 1$
- fragment existentiel de FO-$\mathbb{R}$ ($\exists$-$\mathbb{R}$) : décidable en PSPACE
  - des problèmes géométrique de graphes sont complets pour ce problème

Élimination des quantificateurs

- par Tarski-Seidenberg, FO-$\mathbb{R}$ est décidable :
  - elle admet une procédure d'élimination des quantificateurs doublement exponentielle
  - exemple : $\exists x, 0 < x \wedge x \leq 1 \rightsquigarrow 0 < 1$
- fragment existentiel de FO-$\mathbb{R}$ ($\exists$-$\mathbb{R}$) : décidable en PSPACE
  - des problèmes géométrique de graphes sont complets pour ce problème
- alternance bornée de quantificateurs : EXPTIME
  - par exemple $\exists\forall$-$\mathbb{R}$

Encodage de stratégies dans FO-$\mathbb{R}$

- Soit $\sigma : S \to \text{Dist}(A)$ est une stratégie stochastique.
- On défini $\mathcal{X}$ un ensemble fini de variables $x_{s,a}$, avec $s \in S$ et $a \in A$

Encodage de stratégies dans FO-$\mathbb{R}$

- Soit $\sigma : S \to \text{Dist}(A)$ est une stratégie stochastique.
- On défini $\mathcal{X}$ un ensemble fini de variables $x_{s,a}$, avec $s \in S$ et $a \in A$

- La stratégie σ peut être vue comme un point dans l'espace des nombres réels $\mathbb{R}^{\mathcal{X}}$, où $x_{s,a}$ est associé à la probabilité $\sigma(s, a)$.

Encodage de stratégies dans FO-$\mathbb{R}$

- Soit $\sigma : S \to \text{Dist}(A)$ est une stratégie stochastique.
- On défini $\mathcal{X}$ un ensemble fini de variables $x_{s,a}$, avec $s \in S$ et $a \in A$

- La stratégie σ peut être vue comme un point dans l'espace des nombres réels $\mathbb{R}^{\mathcal{X}}$, où $x_{s,a}$ est associé à la probabilité $\sigma(s, a)$.

- Réciproquement, chaque point dans $\mathbb{R}^{\mathcal{X}}$ tel que

$$\forall x \in \mathcal{X}, x \in [0, 1] \wedge \forall s \in S, \sum_{a \in A} x_{s,a} = 1$$

  représente une stratégie σ.

- les points de $\mathbb{R}^{\mathcal{X}}$ qui encodent une stratégie peuvent être décrits par une conjonction finie d'inégalités linéaires

Encodage du problème de la synthèse de stratégie

- On ajoute
  - des variables existentielles $y_{s,\Phi'} \in \{0,1\}$ qui sont vraies si la sous-formule d'état Φ' est satisfaite depuis s,
  - des variables existentielles $z_{s,\varphi} \in [0,1]$ ayant la probabilité que la sous-formule de chemin φ soit satisfaite depuis s.
- On créé ensuite un système d'équations telles que

$$z_{s,\mathsf{F}^\ell\, p} = \sum_{\substack{s \xrightarrow{a} s' \\ p \in L(s')}} x_{s,a}\mathbb{P}(s,a,s') + \sum_{\substack{s \xrightarrow{a} s' \\ p \notin L(s')}} x_{s,a}\mathbb{P}(s,a,s') z_{s',\mathsf{F}^{\ell-1}\, p}\,.$$

- Pour les formules d'états,

$$y_{s,(\mathbb{P}[\varphi] \bowtie c)} = 1 \leftrightarrow z_{s,\varphi} \bowtie c\,.$$

- Enfin, on demande que $y_{s,\Phi} = 1$.

Horizon non borné

- En cas de propriété $\mathsf{F}\, p$, on encode le système d'équations mentionnées précédemment

Horizon non borné

- En cas de propriété $\mathsf{F}\, p$, on encode le système d'équations mentionnées précédemment
- plus petite solution !

Horizon non borné

- En cas de propriété $\mathsf{F}\, p$, on encode le système d'équations mentionnées précédemment

- plus petite solution !
- $\exists z \forall z', z \models E \wedge (z' \models E \rightarrow z \leq z')$

Horizon non borné

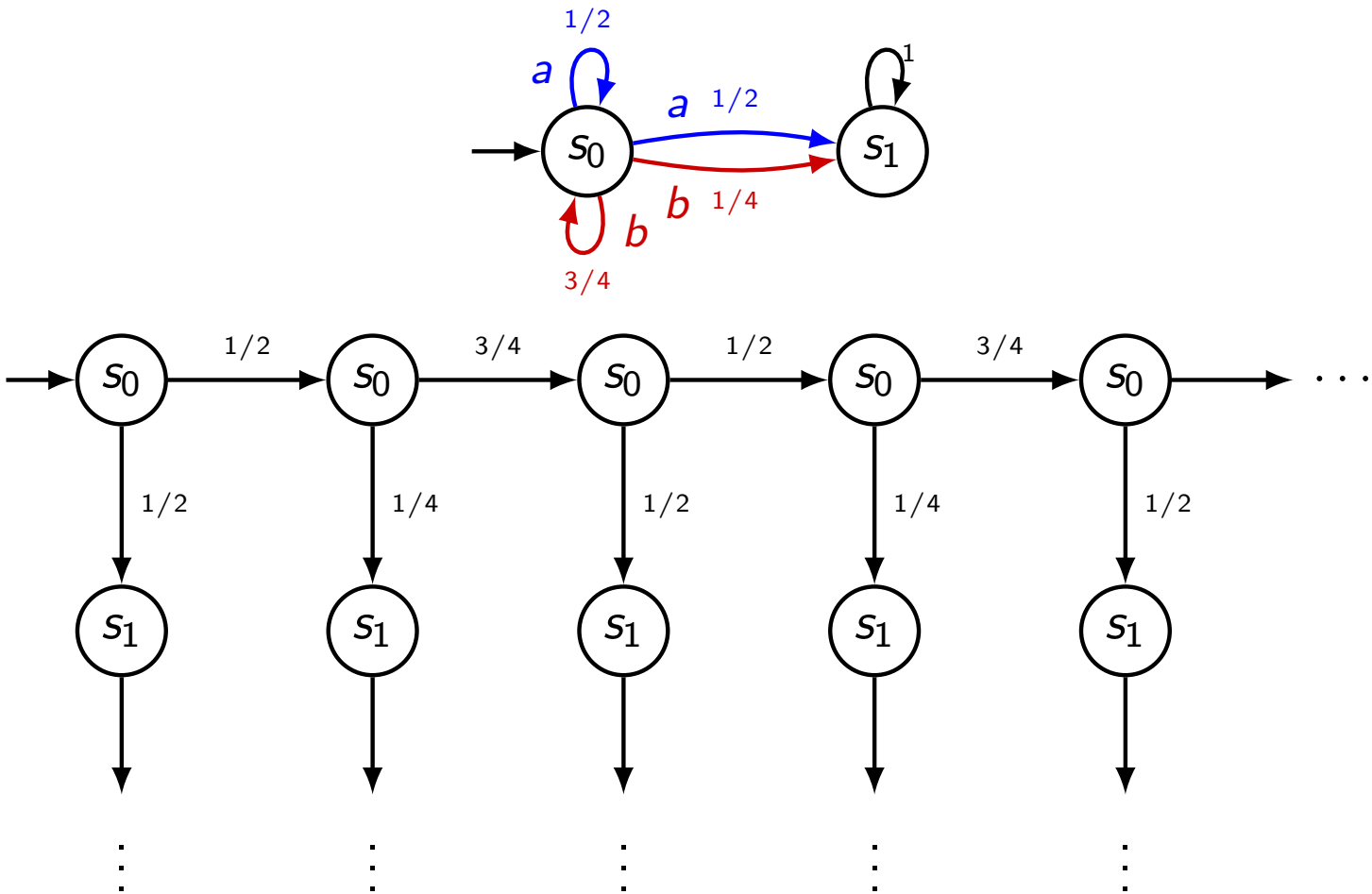
- En cas de propriété $\mathsf{F}\, p$, on encode le système d'équations mentionnées précédemment
- plus petite solution !
- $\exists z \forall z', z \models E \wedge (z' \models E \rightarrow z \leq z')$
- une seule alternance de quantificateurs : EXPTIME

Stratégies avec mémoire

On souhaite pouvoir faire des choix qui dépendent du passé

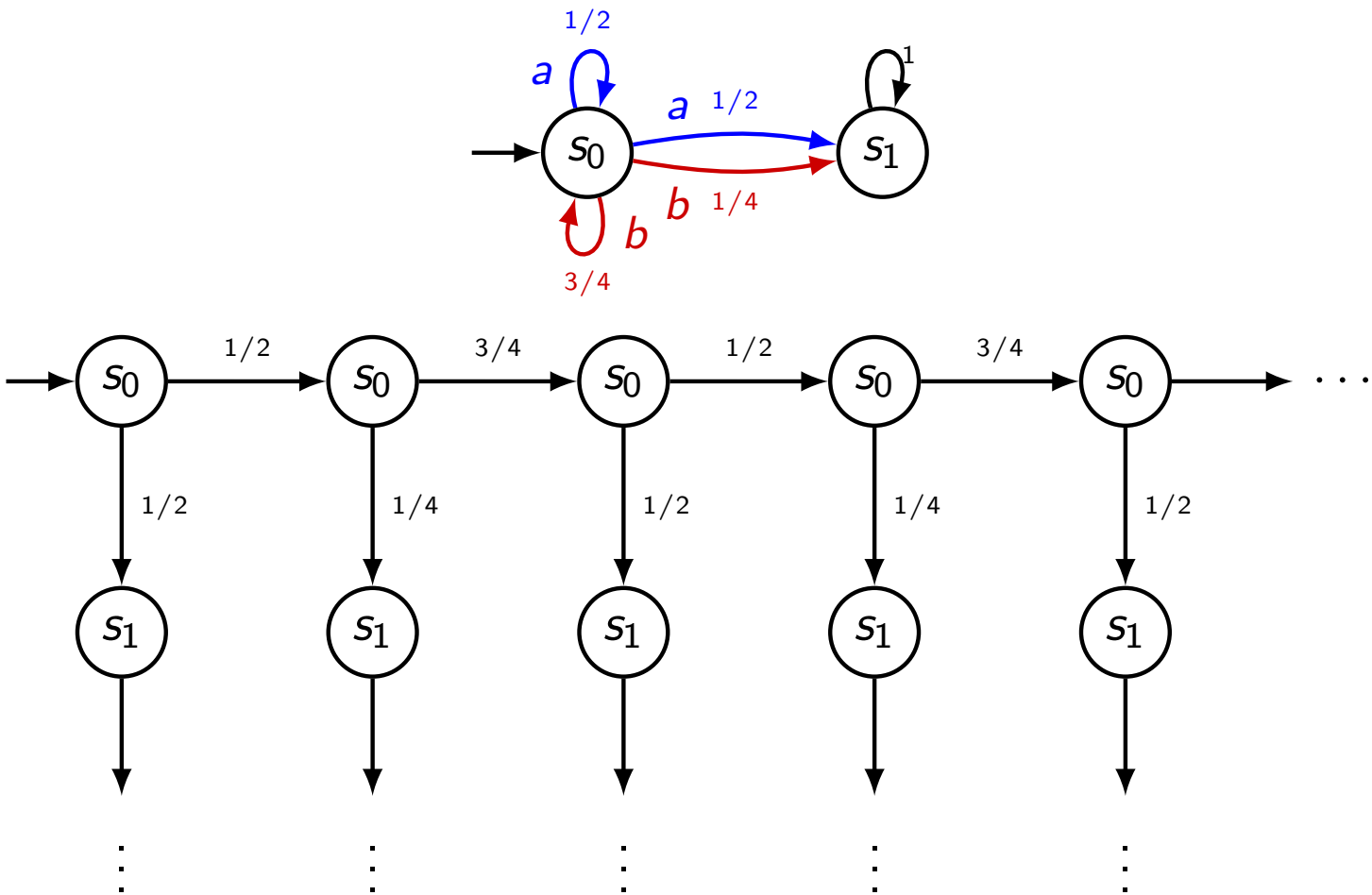
Definition

Une *stratégie* (stochastique, avec mémoire) est une fonction $\sigma : \text{CheminsF}_{\mathcal{M}} \to \text{Dist}(A)$ qui associe à chaque chemin fini ρ une distribution sur les actions.



Exemple

- Soit Φ la formule PCTL
  $(\mathbb{P}\left[\mathsf{F}^2\, s_1\right] = \frac{5}{8}) \wedge (\mathbb{P}\left[\mathsf{X}\, s_1\right] \geq \frac{1}{2} \vee \mathbb{P}\left[\mathsf{X}\, s_1\right] \leq \frac{1}{4})$. On cherche une stratégie pour satisfaire $\mathbb{P}\left[\mathsf{G}\, \Phi\right] = 1$.



Ouch

Malheureusement, ce gain de puissance est accompagné d'un prix notoire :

Proposition

Soit $\mathcal{M}$ un MDP et Φ une formule PCTL. Le problème de la synthèse de stratégies (stochastiques et avec mémoire) est indécidable. Le problème de la synthèse de stratégies (déterministes et avec mémoire) est également indécidable.

Intuition pour l'indécidabilité

- faire une réduction depuis le problème de l'arrêt sur une Machine à compteurs :

Intuition pour l'indécidabilité

- faire une réduction depuis le problème de l'arrêt sur une Machine à compteurs :
- on contruit un MDP $\mathcal{M}$ et une formule PCTL Φ tels que $\mathcal{M}$ n'admet qu'une seule stratégie pour satisfait Φ, qui est déterministe.
- Pour cette stratégie, $\mathcal{M}[\sigma]$ est une chaîne de Markov qui représente l'exécution de la machine à compteur.

Intuition pour l'indécidabilité

- faire une réduction depuis le problème de l'arrêt sur une Machine à compteurs :
- on contruit un MDP $\mathcal{M}$ et une formule PCTL Φ tels que $\mathcal{M}$ n'admet qu'une seule stratégie pour satisfait Φ, qui est déterministe.
- Pour cette stratégie, $\mathcal{M}[\sigma]$ est une chaîne de Markov qui représente l'exécution de la machine à compteur.

- En particulier, la valeur des compteurs est hard-codées dans la structure de $\mathcal{M}[\sigma]$
  - c'est une structure arborescente, où une sous-branche de longeur k représente le fait que le compteur contiens la valeur k à ce moment là

Complexité de la synthèse de stratégies pour PCTL

stratégies :	Sans mémoire	Avec Mémoire
Déterministe	NP-complet	Indécidable
Stochastique	EXPTIME SQRT-SUM-difficile	Indécidable

Pour aller plus loin

- limiter les constantes apparaissant dans les formules PCTL à 0 et 1.
  - fragment *qualitatif* de PCTL

Pour aller plus loin

- limiter les constantes apparaissant dans les formules PCTL à 0 et 1.
  - fragment *qualitatif* de PCTL

- problème de la *satisfaisabilité* d'une formule PCTL

Pour aller plus loin

- limiter les constantes apparaissant dans les formules PCTL à 0 et 1.
  - fragment *qualitatif* de PCTL
- problème de la *satisfaisabilité* d'une formule PCTL
- Pour regagner de la décidabilité : fragments de PCTL
  - où se situe la frontière de la décidabilité
  - pour quelles stratégies ?

Pour aller plus loin

- limiter les constantes apparaissant dans les formules PCTL à 0 et 1.
  - fragment *qualitatif* de PCTL
- problème de la *satisfaisabilité* d'une formule PCTL
- Pour regagner de la décidabilité : fragments de PCTL
  - où se situe la frontière de la décidabilité
  - pour quelles stratégies ?
- *hyperlogiques probabilistes*
  - hautement indécidables.
  - gain en expressivité, pour formaliser par exemple la non-interférence probabiliste.

Fin partie 2