Méthodes Formelles Approche Probabiliste

Arnaud Sangnier

IRIF - Université de Paris

Cours 1

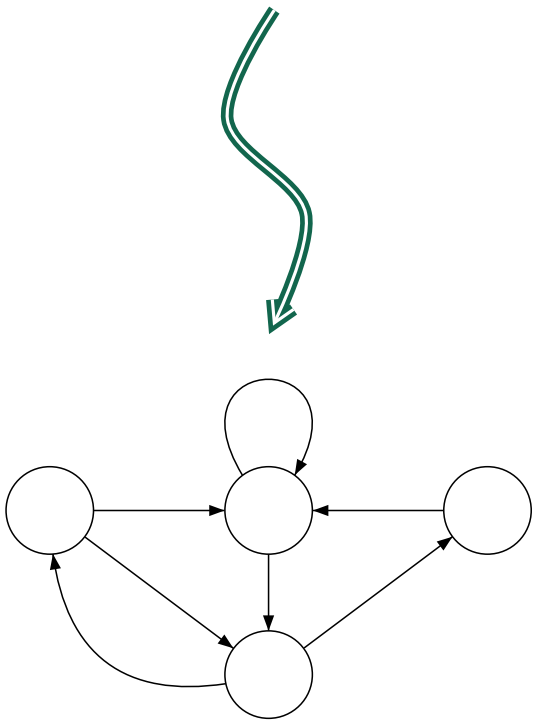
Vérification de systèmes

But :

- Définir des modèles mathématiques pour représenter le comportement de systèmes $\Rightarrow$ **Modèle**
- Définir des langages mathématiques pour décrire le comportement attendu des systèmes $\Rightarrow$ **Spécification**
- Trouver un algorithme de vérification pour dire si le modèle satisfait la spécification $\Rightarrow$ **Algorithme de model-checking**

Principe du model-checking

Un système **satisfait-il** **une spécification ?**



$\models$ Φ ?

algorithme de model-checking

Modèle **Formule**

Quelques remarques

- Les modèles peuvent être différents selon les caractéristiques du système que l'on souhaite prendre en compte
- Les spécifications dépendent aussi de ce que l'on souhaite vérifier
- Il n'existe pas toujours d'algorithme de vérification. Certains problèmes sont indécidables. Par exemple, on ne sait pas décider l'arrêt des machines de Türing.

Plan du cours

1. Vérification de systèmes de transitions (systèmes non-déterministes sans probabilité)
2. Vérification de chaînes de Markov (systèmes probabilistes sans non-déterminisme)
3. Vérfication de processsus de décision markovien (systèmes non-déterministes avec probabilité)

Systèmes de transitions - I

- Les systèmes de transitions sont simplement des graphes où les sommets représentent les états des systèmes et les arcs représentent les transitions, c'est-à-dire les changements d'états

Définition

Un système de transition ST est un n-uplet $(S, \rightarrow, s_{in}, PA, L)$ où :

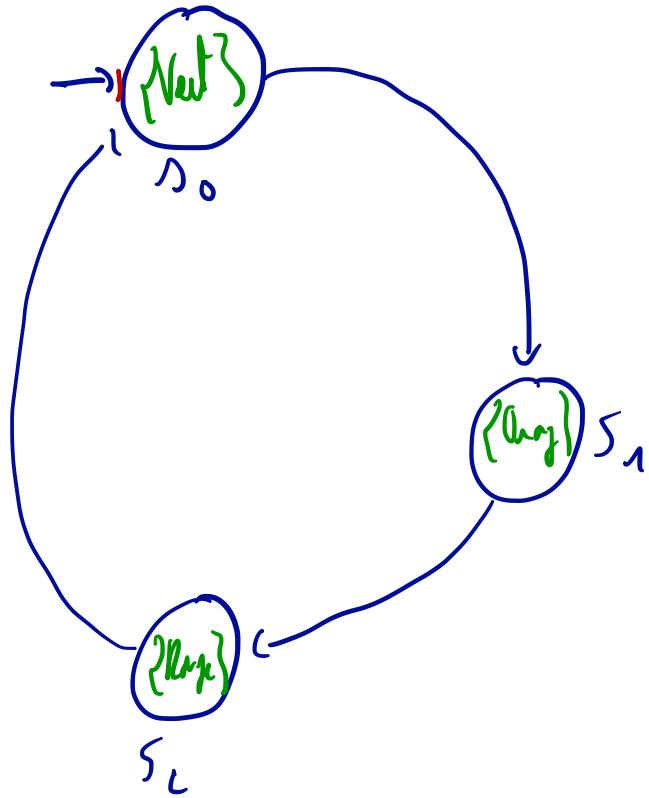
- S est l'ensemble des états
- $\rightarrow \subseteq S \times S$ est la relation de transition
- $s_{in} \in S$ est l'état initial
- PA est l'ensemble des propositions atomiques
- $L : S \mapsto 2^{PA}$ est la fonction d'étiquetage

Systèmes de transitions - II

Remarques :

- 2^{PA} est l'ensemble des sous-ensembles de PA
- Pour chaque état $s \in S$, $L(s) \subseteq PA$ est un ensemble de propositions atomiques vraies dans cet état. Cet ensemble peut-être vide.
- Deux états différents s et s' peuvent avoir les mêmes étiquettes, c'est-à-dire $s \neq s'$ et $L(s) = L(s')$ est possible.
- À la place de $(s, s') \in \rightarrow$, on écrira souvent $s \rightarrow s'$

Systèmes de transitions - Exemple 1



$S = \{s_0, s_1, s_2\}$

$\rightarrow = \{(s_0, s_1), (s_1, s_2), (s_2, s_0)\}$

$s_{in} = s_0$

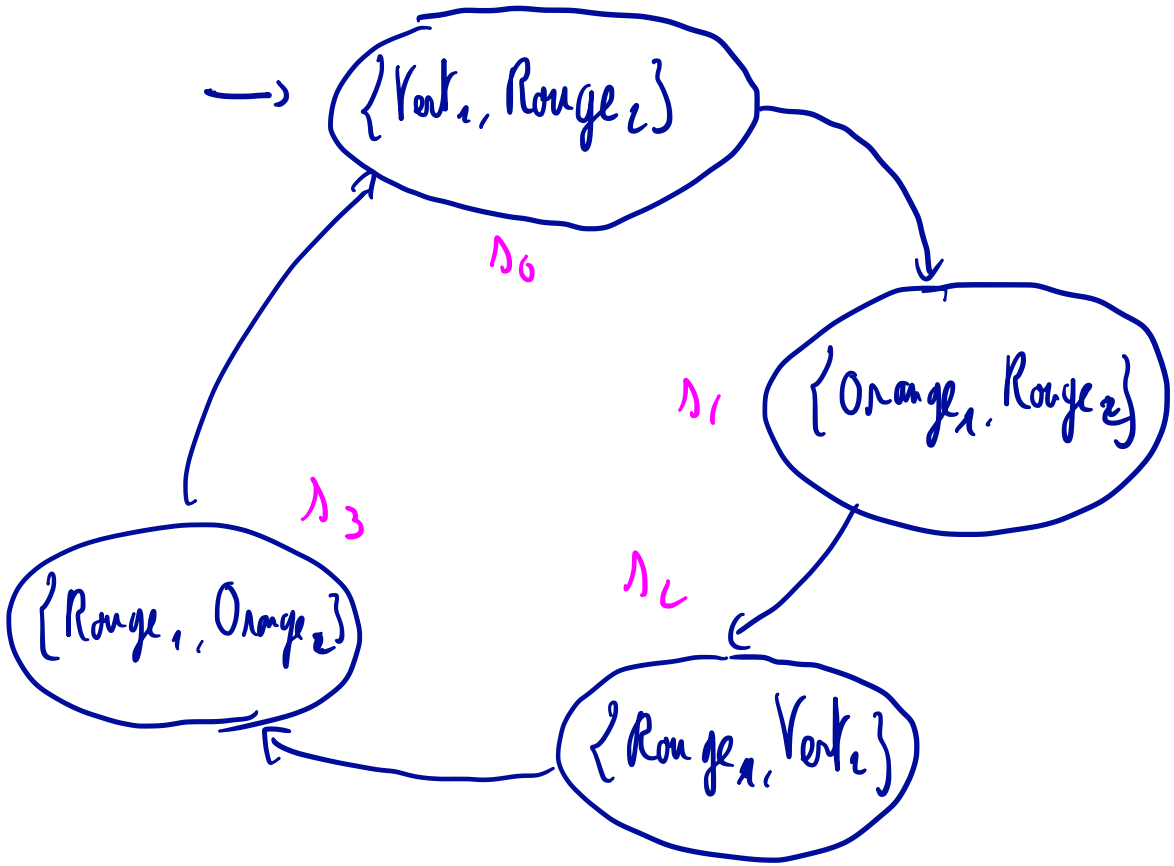
PA = {Vert, Orange, Rouge}

$L(s_0) = \{Vert\}$

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

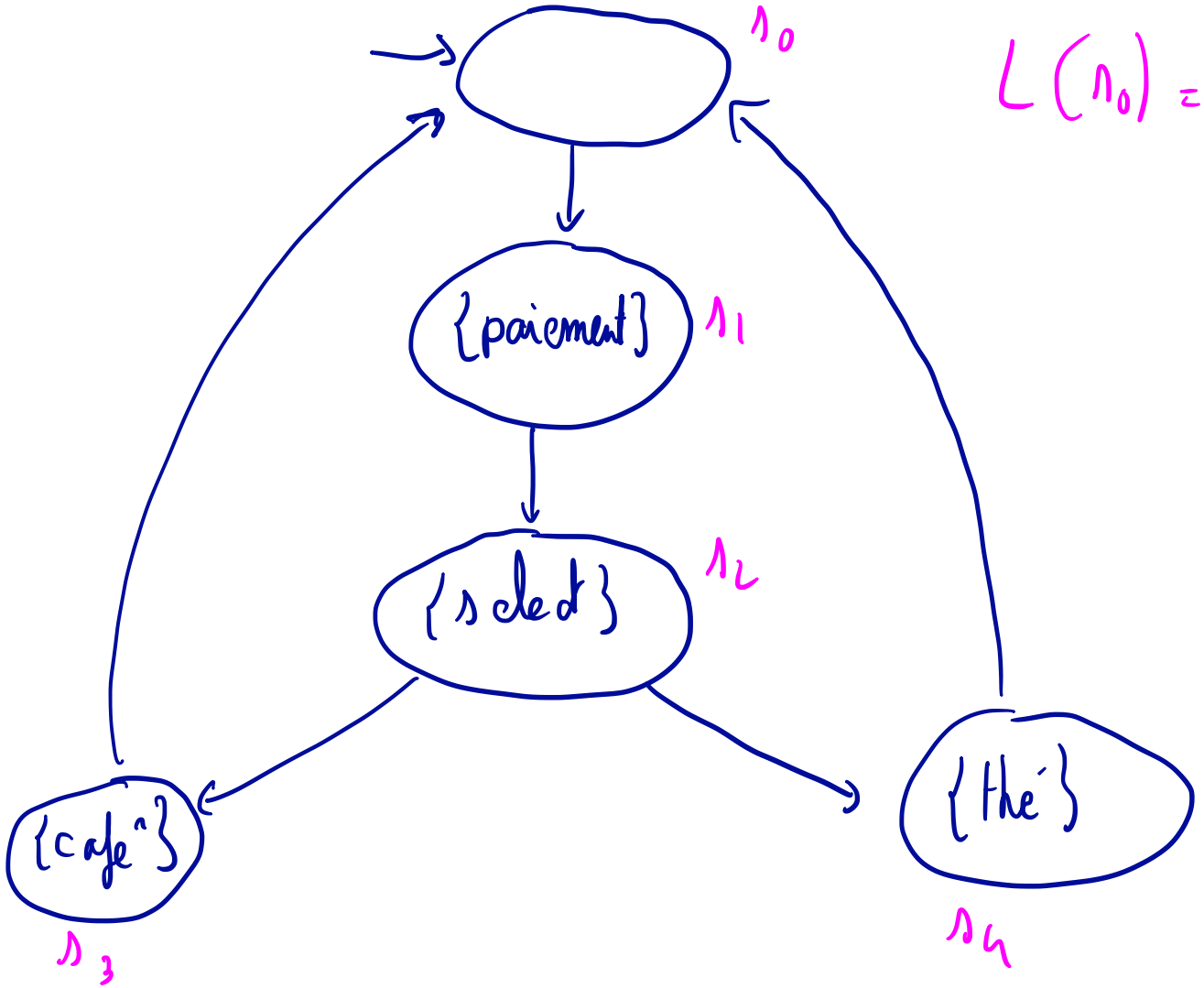
$L(s_2) = \{Rouge\}$

Systèmes de transitions - Exemple 2



PA : {Vert1, Orange1, Rouge1, Vert2, Orange2, Rouge2}

Systèmes de transitions - Exemple 3



Quelques définitions supplémentaires

Soit $ST = (S, \rightarrow, s_{in}, PA, L)$ un système de transitions et $s \in S$.

- $Post(s) = \{s' \in S \mid s \rightarrow s'\}$ (dans ce cours, on supposera qu'il n'y a pas d'état $s \in S$ tel que $Post(s) = \emptyset$)
- $Pre(s) = \{s' \in S \mid s' \rightarrow s\}$
- 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 $s_i \rightarrow s_{i+1}$
- 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 $s_i \rightarrow s_{i+1}$
- Une **exécution** est un chemin infini $s_0 s_1 s_2 \ldots$ tel que $s_0 = s_{in}$
- On note $Exec(ST)$ l'ensemble des exécutions de ST