Une théorie des processus probabilistes continus: équivalence et distance

Richard Blute, Abbas Edalat,
Josée Desharnais, **Prakash Panangaden**,
Vineet Gupta, Radha Jagadeesan

Prix test-of-time LICS 2017 et LICS 2020

Bisimulation for Labelled Markov Processes. LICS 1997.

The Metric Analogue of Weak Bisimulation for Probabilistic Processes. LICS 2002.

Outline

Problématique générale – systèmes interactifs

- Étant donné un contexte $C[\cdot]$, et sachant qu'une composante approxime un comportement idéal, peut-on comparer C[composante] et C[idéal] ?

Problématique générale – systèmes interactifs

- Étant donné un contexte $C[\cdot]$, et sachant qu'une composante approxime un comportement idéal, peut-on comparer C[composante] et C[idéal] ?
- Substitution sécuritaire : peut-on substituer une composante dans un programme sans augmenter la possibilité de perte d'information ?

$$d(c, c') < \epsilon \Rightarrow |\text{perte}(C[c]) - \text{perte}(C[c'])| < \delta$$

Problématique générale – systèmes interactifs

- Étant donné un contexte $C[\cdot]$, et sachant qu'une composante approxime un comportement idéal, peut-on comparer C[composante] et C[idéal] ?
- Substitution sécuritaire : peut-on substituer une composante dans un programme sans augmenter la possibilité de perte d'information ?

$$d(c, c') < \epsilon \Rightarrow |\text{perte}(C[c]) - \text{perte}(C[c'])| < \delta$$

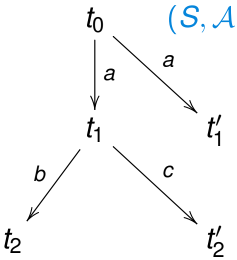
- Pour analyser des systèmes ayant un nombre d'états infini, non dénombrable, on veut une représentation qui garde toutes les informations – quite à approximer ou discrétiser par la suite.

D'abord les modéliser/décrire/représenter

On veut modéliser les systèmes

- interactifs, concourants
- non déterministes
- probabilistes
- à états possiblement infinis

$(S, \mathcal{A}, \rightarrow)$

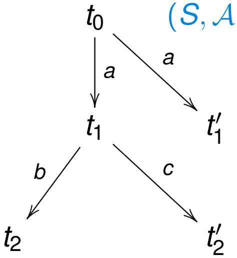


D'abord les modéliser/décrire/représenter

On veut modéliser les systèmes

- interactifs, concourants
- non déterministes
- probabilistes
- à états possiblement infinis

$(S, \mathcal{A}, \longrightarrow)$



Savoir les

- combiner : synchronisation sur étiquettes/actions $\mathcal{A}$
- comparer : équivalence, distance

Bisimulation [Park et Milner ’80]

Bisimulation : équivalence selon un observateur qui interagit.

Exemple typique (fini non probabiliste) : $(S, \mathcal{A}, \rightarrow)$

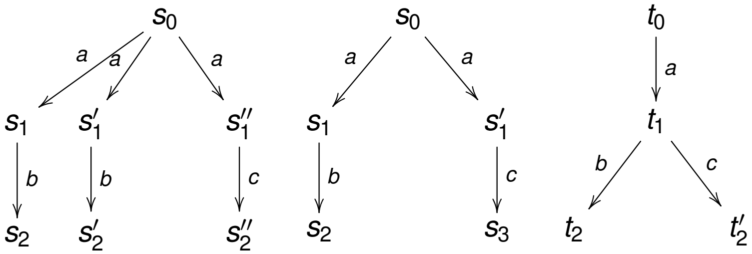
$$
\begin{tikzcd}
 & & s_0 \arrow[dll, "a"'] \arrow[dl, "a"] \arrow[d, "a"] \\
s_1 \arrow[d, "b"] & s_1' \arrow[d, "b"] & s_1'' \arrow[d, "c"] \\
s_2 & s_2' & s_2''
\end{tikzcd}
\qquad
\begin{tikzcd}
 & s_0 \arrow[dl, "a"'] \arrow[dr, "a"] & \\
s_1 \arrow[d, "b"] & & s_1' \arrow[d, "c"] \\
s_2 & & s_3
\end{tikzcd}
$$

- acceptent le même langage/les mêmes traces

Bisimulation [Park et Milner '80]

Bisimulation : équivalence selon un observateur qui interagit.

Exemple typique (fini non probabiliste) : $(S, \mathcal{A}, \rightarrow)$

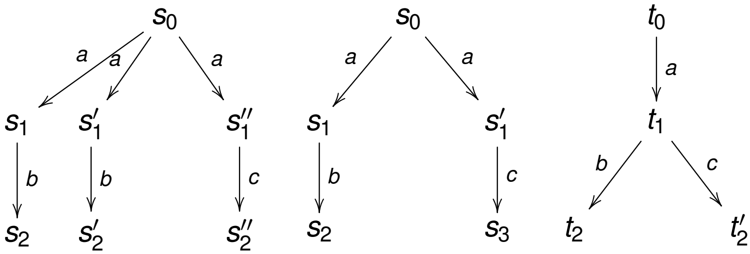


- acceptent le même langage/les mêmes traces

Bisimulation [Park et Milner ’80]

Bisimulation : équivalence selon un observateur qui interagit.

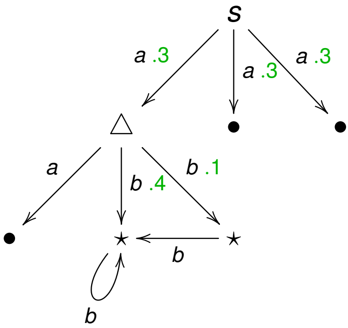
Exemple typique (fini non probabiliste) : $(S, \mathcal{A}, \longrightarrow)$



- acceptent le même langage/les mêmes traces
- ne sont pas interchangeables du point de vue de l’interaction

Modélisation et bisimulation Larsen-Skou '93

Système de transitions probabiliste $(S, \mathcal{A}, \{P_a\}_{a\in\mathcal{A}})$

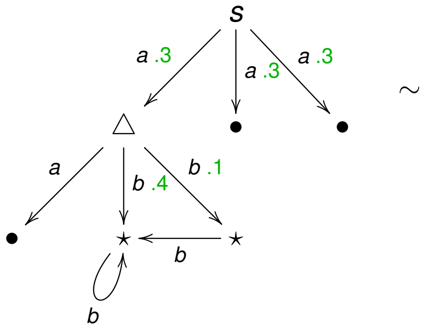


$\sim$

Modélisation et bisimulation Larsen-Skou '93

Système de transitions probabiliste $(S, \mathcal{A}, \{P_a\}_{a \in \mathcal{A}})$

- $P_a : S \times S \to [0, 1]$ satisfaisant $\sum_{t \in S} P_a(s, t) \leq 1$.

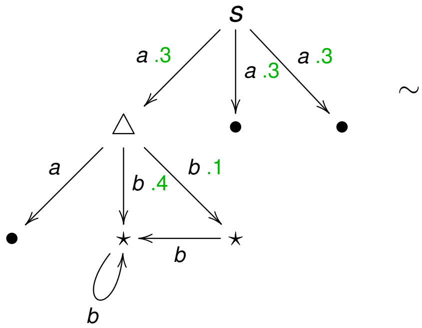


Modélisation et bisimulation Larsen-Skou '93

Système de transitions probabiliste $(S, \mathcal{A}, \{P_a\}_{a \in \mathcal{A}})$

- $P_a : S \times S \to [0,1]$ satisfaisant $\sum_{t \in S} P_a(s,t) \leq 1$.

Une bisimulation est une relation d'équivalence qui préserve les probabilités sur les classes d'équivalences.

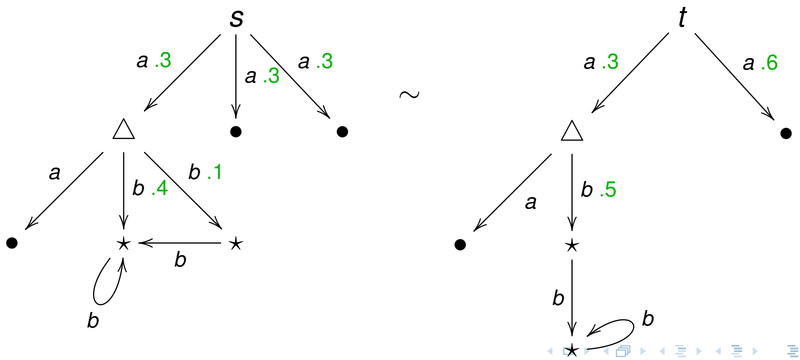


Modélisation et bisimulation Larsen-Skou '93

Système de transitions probabiliste $(S, \mathcal{A}, \{P_a\}_{a \in \mathcal{A}})$

- $P_a : S \times S \to [0, 1]$ satisfaisant $\sum_{t \in S} P_a(s, t) \leq 1.$

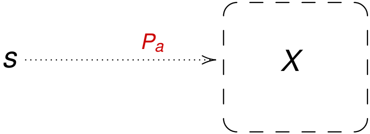
Une bisimulation est une relation d'équivalence qui préserve les probabilités sur les classes d'équivalences.



LICS97 LMP : Labelled Markov Processes

Et si l'ensemble d'états est infini continu ?

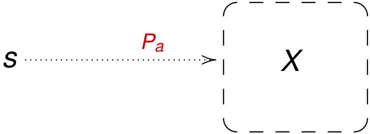
- alors la probabilité d'un point est nulle !



LICS97 LMP : Labelled Markov Processes

Et si l'ensemble d'états est infini continu ?

- alors la probabilité d'un point est nulle !
- On doit utiliser des mesures



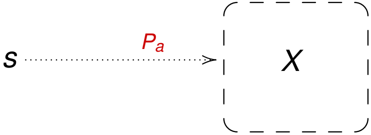
LICS97 LMP : Labelled Markov Processes

Et si l'ensemble d'états est infini continu ?

- alors la probabilité d'un point est nulle !
- On doit utiliser des mesures

Un système de Markov étiqueté $(S, \Sigma, \mathcal{A}, \{P_a\}_{a \in \mathcal{A}})$

- $P_a : S \times \Sigma \longrightarrow [0, 1]$ un noyau stochastique,



$P_a(s, S) \leq 1$

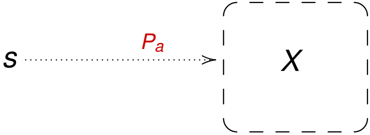
LICS97 LMP : Labelled Markov Processes

Et si l'ensemble d'états est infini continu ?

- alors la probabilité d'un point est nulle !
- On doit utiliser des mesures

Un système de Markov étiqueté $(S, \Sigma, \mathcal{A}, \{P_a\}_{a \in \mathcal{A}})$

- (S, Σ) un ensemble d'états (espace analytique)
- $P_a : S \times \Sigma \longrightarrow [0, 1]$ un noyau stochastique,



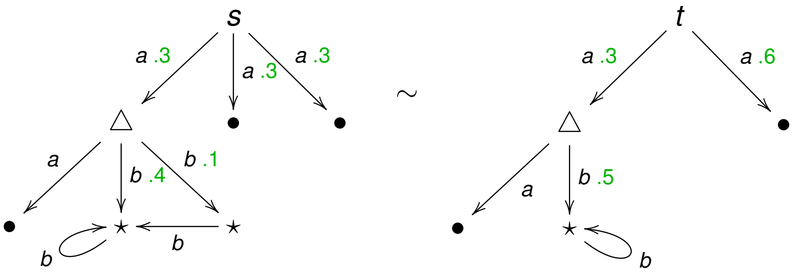
$P_a(s, S) \leq 1$

Bisimulation entre LMP (S, Σ, P)

Definition

Une relation d'équivalence R est une bisimulation sur S si

si $s\,R\,s'$, et si X est un ensemble R-clos de Σ, alors
$P_a(s, X) = P_a(s', X)$ pour tout $a \in \mathcal{A}$



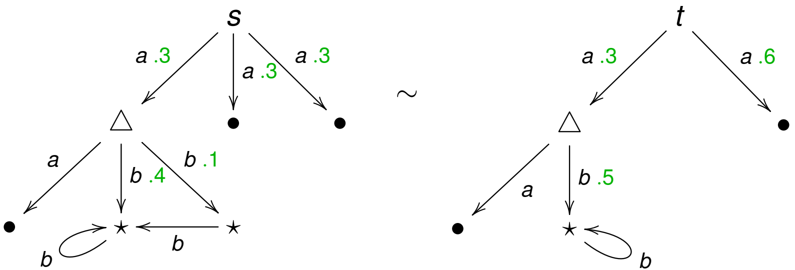
Bisimulation entre LMP (S, Σ, P)

Un ensemble est R-clos si si $s \in X$ and sRs' alors $s' \in X$.

Definition

Une relation d'équivalence R est une bisimulation sur S si

si $s\,R\,s'$, et si X est un ensemble R-clos de Σ, alors
$P_a(s, X) = P_a(s', X)$ pour tout $a \in \mathcal{A}$



Ici termine le contenu de
Richard Blute, Abbas Edalat, Josée Desharnais, Prakash Panangaden, *Bisimulation for Labelled Markov Processes*. LICS 1997.
Prix test-of-time LICS 2017

- Définition des LMP
- Définition (catégorique) de bisimulation
- Démonstration que c'est bien une équivalence
- Transitivité de bisimilation difficile !

Les LMP en main, on veut aussi

- se donner un langage pour décrire des propriétés
- déterminer si une propriété est satisfaite par un état/système

Les LMP en main, on veut aussi

- se donner un langage pour décrire des propriétés
- déterminer si une propriété est satisfaite par un état/système
- démontrer que les propriétés sont complètes pour la bisimulation, c.-à-d. :

Théorème

Deux LMP sont bisimilaires ssi ils satisfont exactement les mêmes formules.

Logique : syntaxe et sémantique

$$\mathcal{L} ::== \mathsf{T} \mid \phi_1 \wedge \phi_2 \mid \langle a \rangle_q \phi \qquad q \in \mathbb{Q} \cap [0,1]$$

$$s \models \langle a \rangle_q \phi \quad \text{ssi} \quad P_a(s, [\![\phi]\!]) \geq q$$

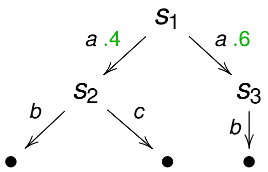
$$\text{où } [\![\phi]\!] := \{s \in S \mid s \models \phi\} \in \Sigma$$

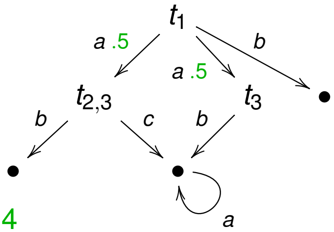
Logique : syntaxe et sémantique

$$\mathcal{L} ::== \top \mid \phi_1 \wedge \phi_2 \mid \langle a \rangle_q \phi \qquad q \in \mathbb{Q} \cap [0,1]$$

$$s \models \langle a \rangle_q \phi \quad \text{ssi} \quad P_a(s, [\![\phi]\!]) \geq q$$

$$\text{où } [\![\phi]\!] := \{s \in S \mid s \models \phi\} \in \Sigma$$





$$s_1 \models \langle a \rangle_x \langle b \rangle_1 \top \text{ pour } x \geq .4$$
$$\models \langle a \rangle_{.4} (\langle b \rangle_1 \top \wedge \langle c \rangle_1 \top)$$

$$t_1 \models \langle a \rangle_{.5} \langle b \rangle_1 \langle a \rangle_1 \langle a \rangle_1 \top$$

Logique : syntaxe et sémantique

$$\mathcal{L} ::== \mathrm{T} \mid \phi_1 \wedge \phi_2 \mid \langle a \rangle_q \phi \qquad q \in \mathbb{Q} \cap [0, 1]$$

$$s \models \langle a \rangle_q \phi \quad \text{ssi} \quad P_a(s, [\![\phi]\!]) \geq q$$

$$\text{où } [\![\phi]\!] := \{s \in S \mid s \models \phi\} \in \Sigma$$

Théorème (DEP, LICS 1998, I & C 2002)

Deux LMP sont bisimilaires ssi ils satisfont les mêmes formules de $\mathcal{L}$.

Quoi ? ? ?

$$\mathcal{L} ::== \top \mid \phi_1 \wedge \phi_2 \mid \langle a \rangle_q \phi \qquad q \in \mathbb{Q} \cap [0, 1]$$

Ce résultat a beaucoup surpris. Cette logique :

- ne contient pas de négation (ni de ou)
- ne contient pas de conjonction infinie

Dans le cas non probabiliste ces éléments sont nécessaires

Quoi ? ? ?

$$\mathcal{L} ::== \top \mid \phi_1 \wedge \phi_2 \mid \langle a \rangle_q \phi \qquad q \in \mathbb{Q} \cap [0,1]$$

Ce résultat a beaucoup surpris. Cette logique :

- ne contient pas de négation (ni de ou)
- ne contient pas de conjonction infinie

Dans le cas non probabiliste ces éléments sont nécessaires

$$\begin{tikzcd}
 & s_0 \arrow[dl, "a"'] \arrow[dr, "a"] & & t_0 \arrow[d, "a"] \\
s_1 & & s_2 \arrow[d, "b"] & t_1 \arrow[d, "b"] \\
 & & s_3 & t_2
\end{tikzcd}$$

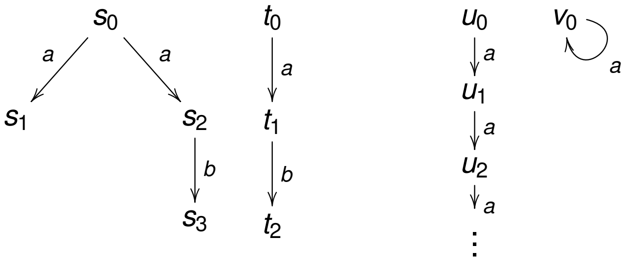
Quoi ? ? ?

$$\mathcal{L} ::== \mathrm{T} \mid \phi_1 \wedge \phi_2 \mid \langle a \rangle_q \phi \qquad q \in \mathbb{Q} \cap [0,1]$$

Ce résultat a beaucoup surpris. Cette logique :

- ne contient pas de négation (ni de ou)
- ne contient pas de conjonction infinie

Dans le cas non probabiliste ces éléments sont nécessaires



Le non déterminisme est différent du stochastique

Dans le cas probabiliste, les contre-exemples tombent !

$$
\begin{tikzcd}
 & s_0 \arrow[dl, "{a[p]}"'] \arrow[dr, "{a[q]}"] & \\
s_1 & & s_2 \arrow[d, "b"] \\
 & & s_3
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
t_0 \arrow[d, "{a[r]}"] \\
t_1 \arrow[d, "b"] \\
t_2
\end{tikzcd}
$$

- si $p+q<r$ ou $p+q>r$, alors un $\langle a\rangle_x\top$ les distingue.
- si $p+q=r$ et $p>0$ alors $q<r$ donc $\langle a\rangle_r\langle b\rangle_1\top$ les distingue.

La bisimulation est trop forte !

La bisimulation est utile

- comme notion théorique d'**égalité** (valider autres notions)
- pour réduire la taille de l'espace des états
- voir si un processus continu est équivalent à un fini

La bisimulation est trop forte !

La bisimulation est utile

- comme notion théorique d'**égalité** (valider autres notions)
- pour réduire la taille de l'espace des états
- voir si un processus continu est équivalent à un fini

Mais est trop forte :

- petite différence de probabilités $\Rightarrow$ non-bisimilaires
- souvent les probabilités sont des valeurs approximatives
- spécification finie pour un système infini : comment valider ?

La bisimulation est trop forte !

La bisimulation est utile

- comme notion théorique d'**égalité** (valider autres notions)
- pour réduire la taille de l'espace des états
- voir si un processus continu est équivalent à un fini

Mais est trop forte :

- petite différence de probabilités $\Rightarrow$ non-bisimilaires
- souvent les probabilités sont des valeurs approximatives
- spécification finie pour un système infini : comment valider ?

Solutions : ϵ-bisimulation, simulation (notion de $\leq$), distance

Distance entre les processus – propriétés

- $d(\mathcal{P}, \mathcal{Q}) = 0$ ssi $\mathcal{P}$ et $\mathcal{Q}$ sont bisimilaires
- Convergence en probabilité : On veut $a_{r-\epsilon}.P \xrightarrow[\epsilon \to 0]{} a_r.P$.

  Et de façon plus générale $d(a_{r-\epsilon_1}.P, a_{r-\epsilon_2}.P) \leq |\epsilon_1 - \epsilon_2|$.
- Convergence en profondeur. On veut $a^n.1 \xrightarrow[n \to \infty]{} a^\infty$
- Convergence en logique
- Non-expansion par rapport aux opérateurs de l'algèbre de processus. Ex. : $d(\mathcal{P}||\mathcal{R}, \mathcal{Q}||\mathcal{R}) \leq d(\mathcal{P}, \mathcal{Q})$.

Implémentée à l'aide de la programmation linaire [VanBreugel]

Dernier Prix test-of-time LICS 2022
Josée Desharnais, Vineet Gupta, Prakash Panangaden, Radha Jagadeesan. *The Metric Analogue of Weak Bisimulation for Probabilistic Processes*. LICS 2002.

This landmark paper is a tour de force, applying new techniques in novel ways to support what constitutes groundbreaking research into how to analyse probabilistic processes and their applications, in varied domains such as security (including privacy and information flow), fuzzy systems, control systems, mobile process theory, software engineering, programming language theory, formal methods, and coalgebraic process theory, among others.


The authors: Josée, Vineet, Radha and Prakash