On the Semantics of Markov Automata

Matthew Hennessy

(joint work with Yuxin Deng)

FMG, TCD March 2011

TRINITY COLLEGE DUBLIN
COLÁISTE NA TRÍONÓIDE, BAILE ÁTHA CLIATH

Adding time to process descriptions

Pervasive:

- all actions have duration: $a^{3.5}.P \;+\; \mathbf{delay}(1.3).Q \mid b^{2.1}.R$
- Semantic theory very sensitive to timing

Maximal progress:

- only passage of time has duration
- all other actions are instantaneous
- time only passes when no more actions are possible: $\mathbf{delay}(d_1).Q_1 + b.(\mathbf{delay}(d_2).Q_2 + c.R) \;\mid\; \overline{b}.\overline{a}.P$
- Semantic theory does not measure passage of time directly

Nature of time

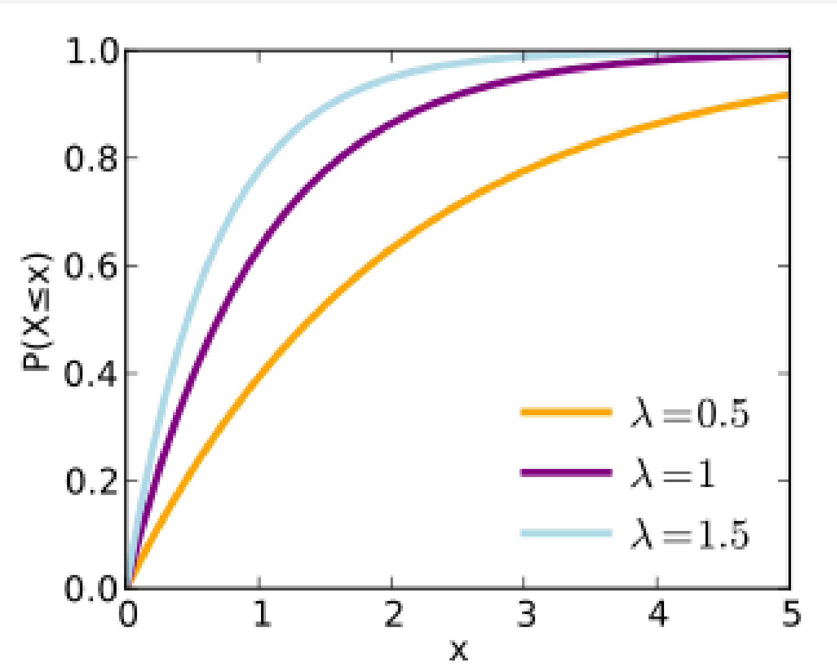
- discrete time: $\textbf{delay}(3).Q_1 + b.(\textbf{delay}(2).Q_2 + c.R) \;\mid\; \overline{b}.\overline{a}.P$
- real-time:
  $\textbf{delay}(3.223).Q_1 + b.(\textbf{delay}(1.567).Q_2 + c.R) \;\mid\; \overline{b}.\overline{a}.P$
- probabilistic time:
  $\textbf{delay}(d_1).Q_1 + b.(\textbf{delay}(d_2).Q_2 + c.R) \;\mid\; \overline{b}.\overline{a}.P$

Timing of events $\textbf{delay}(d_i)$ governed by probability distributions d_i

Poisson processes

Probability that event has happened by time x:

$$P(x) = (1 - e^{-\lambda x})$$



Poisson processes

$$P(x) = (1 - e^{-\lambda x})$$

Rates:

Characteristics completely determined by *rate* λ

- Memoryless: useful for interpreting parallel construct: $\mathbf{delay}(\lambda).Q_1 \mid \mathbf{delay}(\beta).Q_2$
- Race law: $\mathbf{delay}(\lambda).Q_1 + \mathbf{delay}(\beta).Q_2$
  - probability that Q_1 wins: $\frac{\lambda}{\lambda+\beta}$
  - probability that Q_2 wins: $\frac{\beta}{\lambda+\beta}$

Markov automata

$$\langle S, \mathrm{Act}_\tau, \rightarrow, \mapsto, \rangle,$$

where

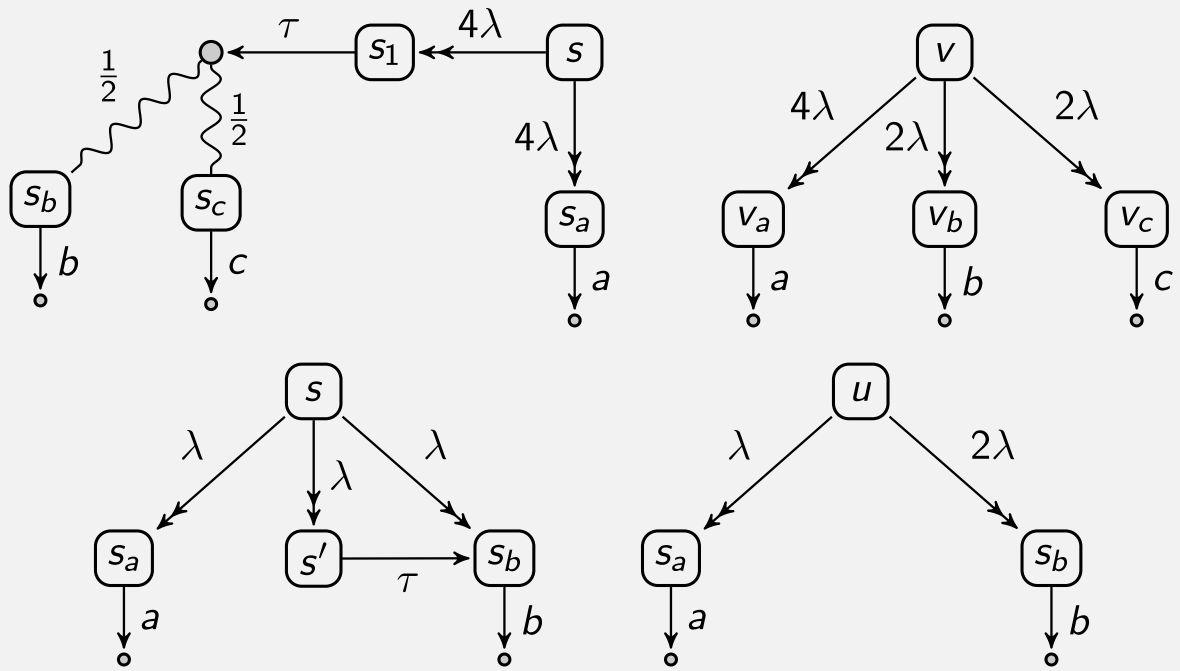
(i) S is a set of states
(ii) Act_τ is a set of transition labels, with distinguished element τ
(iii) the relation $\mapsto$ is a subset of $S \times (\mathbb{R}^+ \cup \{\delta\}) \times \mathcal{D}(S)$

satisfying

(a) $s \overset{\mathbf{d}}{\mapsto} \Delta$ implies $s \overset{\tau}{\not\rightarrow}$ $\mathbf{d} = \lambda$ or δ
(b) $s \overset{\delta}{\mapsto} \Delta_1$ and $s \overset{\delta}{\mapsto} \Delta_2$ implies $\Delta_1 = \Delta_2$

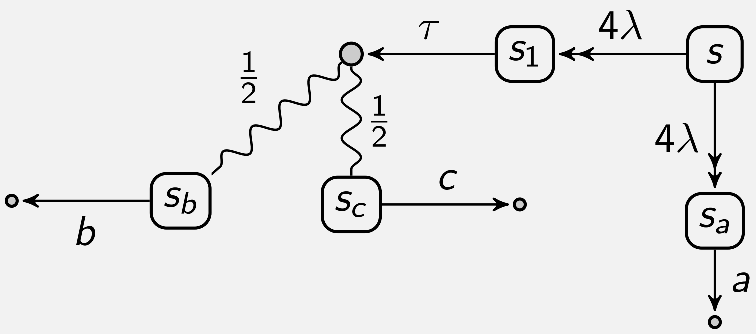
- $s \overset{\lambda}{\mapsto} \Delta$: definite time delay, governed by rate $\lambda \in \mathbb{R}^+$
- $s \overset{\delta}{\mapsto} \Delta$ indefinite time delay
- (a) is maximal progress

Examples

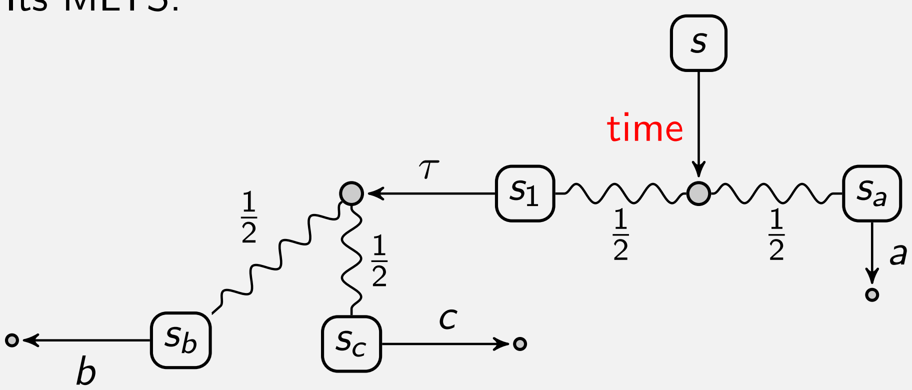


From time to probabilities

An MA:

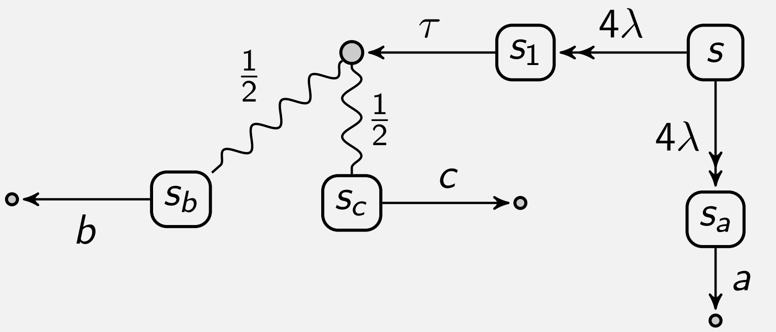


Its MLTS:

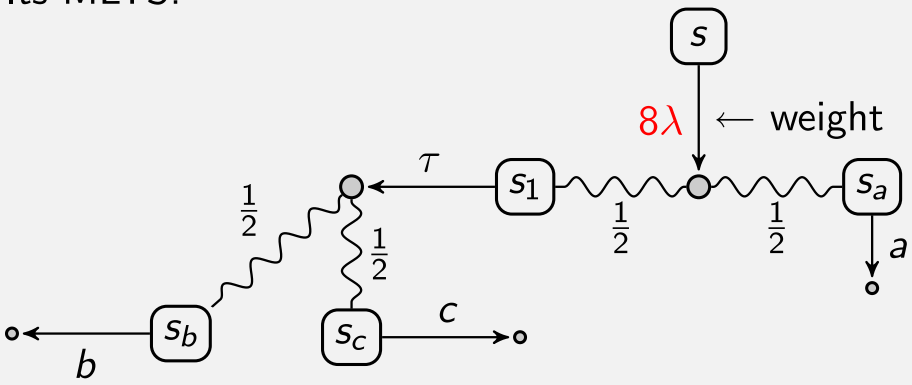


From time to probabilities

An MA:

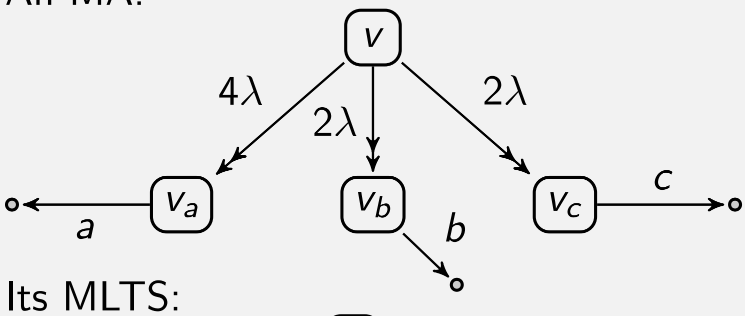


Its MLTS:

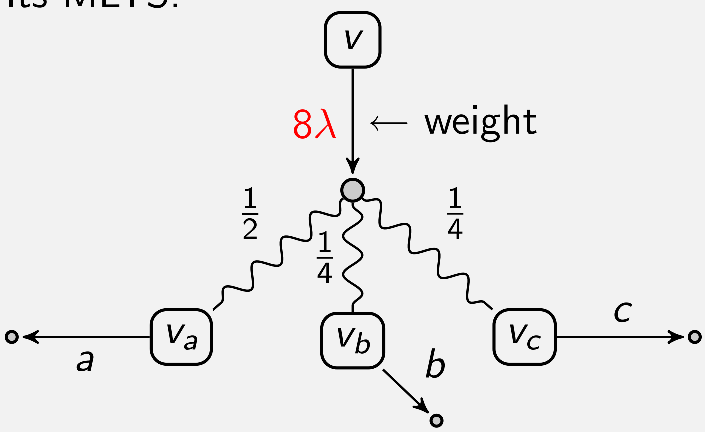


From time to probabilities

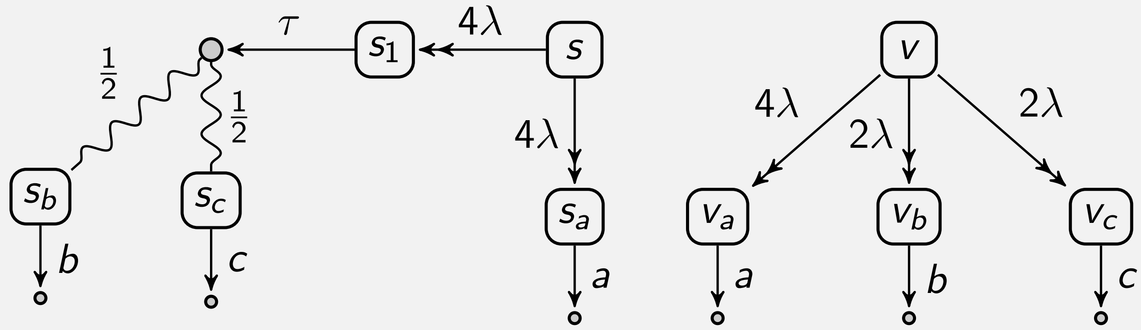
An MA:



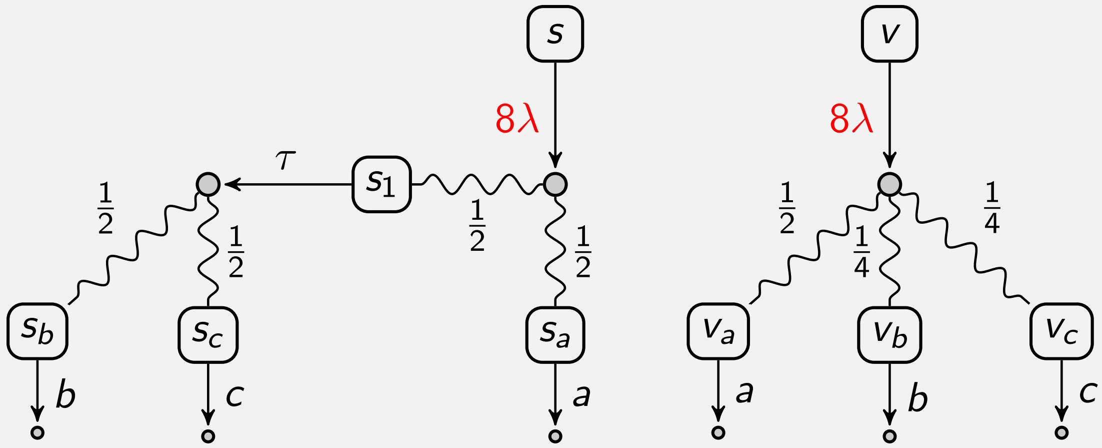
Its MLTS:



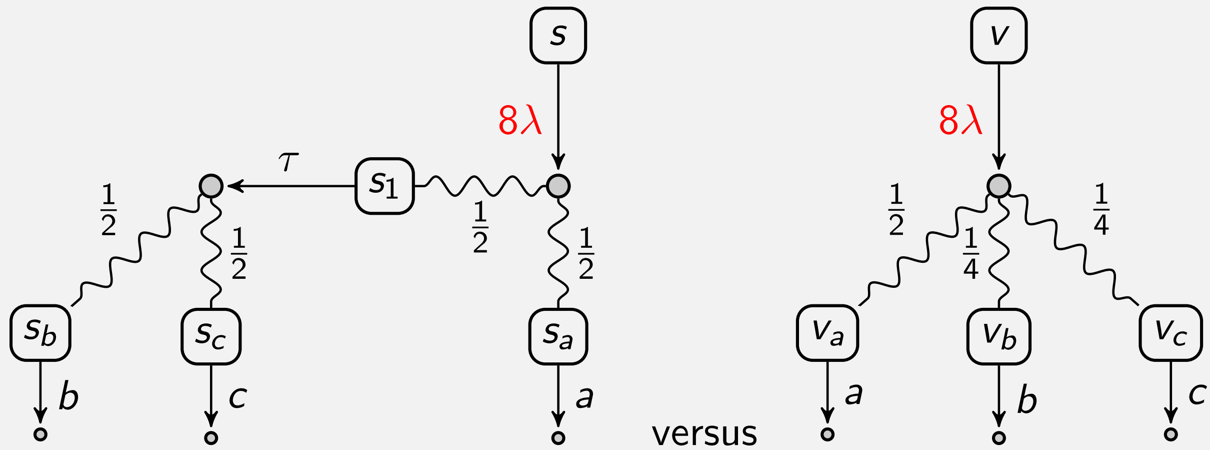
Semantically equivalent?



Semantically equivalent MLTSs?:



Semantically equivalent?



- Not according to existing definitions of *bisimulation equivalence*
- Can a revised version of *bisimulation equivalence* be formulated?
- Is this revision justifiable?

Lifting relations

From $\mathcal{R} \subseteq S \times \mathcal{D}(S)$, to $\text{lift}(\mathcal{R}) \subseteq \mathcal{D}(S) \times \mathcal{D}(S)$

$\Delta \ \text{lift}(\mathcal{R})\ \Theta$ whenever

- $\Delta = \sum_{i \in I} p_i \cdot s_i$, I a finite index set
- For each $i \in I$ there is a distribution Θ_i s.t. $s_i \ \mathcal{R} \ \Theta_i$
- $\Theta = \sum_{i \in I} p_i \cdot \Theta_i$
- $\sum_{i \in I} p_i = 1$

Many different formulations
Note: in decomposition $\sum_{i \in I} p_i \cdot s_i$ states s_i are not necessarily unique

Lifting actions: from $s \xrightarrow{\mu} \Theta$ to $\Delta \xrightarrow{\mu} \Theta$

$$\Delta \xrightarrow{\mu} \Theta$$

- Δ represents a cloud of possible process states
- each possible state must be able to perform μ
- all possible residuals combine to Θ

Examples:

- $(a.b + a.c)\ {}_{\frac{1}{2}}\!\oplus\ a.d \xrightarrow{a} b\ {}_{\frac{1}{2}}\!\oplus\ d$
- $(a.b + a.c)\ {}_{\frac{1}{2}}\!\oplus\ a.d \xrightarrow{a} (b\ {}_{\frac{1}{2}}\!\oplus\ c)\ {}_{\frac{1}{2}}\!\oplus\ d$
- $(a.b + a.c)\ {}_{\frac{1}{2}}\!\oplus\ a.d \xrightarrow{a} (b\ {}_{p}\!\oplus\ c)\ {}_{\frac{1}{2}}\!\oplus\ d$
- $(\tau.a + \tau.b)\ {}_{\frac{1}{2}}\!\oplus\ (\tau.a + \tau.c) \xrightarrow{\tau} a\ {}_{\frac{1}{2}}\!\oplus\ (b\ {}_{\frac{1}{2}}\!\oplus\ c)$

Bisimulations in an MLTS

$$\Delta \approx_{bis} \Theta$$

if, for each $\mu \in \mathsf{Act}_{\tau,\delta} \cup \mathbb{R}^+$ and all finite sets of probabilities $\{ p_i \mid i \in I \}$ satisfying $\sum_{i \in I} p_i = 1$,

(i) whenever $\Delta \stackrel{\mu}{\Longrightarrow} \sum_{i \in I} p_i \cdot \Delta_i$, there is some $\Theta \stackrel{\mu}{\Longrightarrow} \sum_{i \in I} p_i \cdot \Theta_i$, such that $\Delta_i \approx_{bis} \Theta_i$ for each $i \in I$

(ii) symmetrically, whenever $\Theta \stackrel{\mu}{\Longrightarrow} \sum_{i \in I} p_i \cdot \Theta_i$, there exists some $\Delta \stackrel{\mu}{\Longrightarrow} \sum_{i \in I} p_i \cdot \Delta_i$, such that $\Delta_i \approx_{bis} \Theta_i$ for each $i \in I$

Properties:

- $\approx_{bis}$ is an equivalence relation
- $\Theta \stackrel{\tau}{\Longrightarrow} \Theta'$ such that $\Delta\ \mathsf{lift}(\approx_{bis})\ \Theta'$

Simple bisimulations

$$\Delta \approx_{sbis} \Theta$$

if, for each $\mu \in \mathsf{Act}_{\tau,\delta} \cup \mathbb{R}^+$,

(i) whenever $s \stackrel{\mu}{\longrightarrow} \Delta'$, there is some $\Theta \stackrel{\mu}{\Longrightarrow} \Theta'$, such that $\Delta'\ \mathsf{lift}(\approx_{sbis})\ \Theta'$

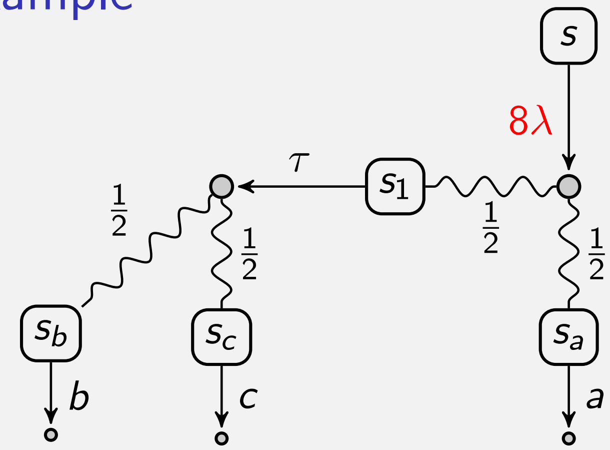
(ii) there exists some $\Delta \in \mathcal{D}(S)$ such that $\overline{s} \stackrel{\tau}{\Longrightarrow} \Delta$ and $\Theta\ \mathsf{lift}(\approx_{sbis})\ \Delta$.

Theorem:

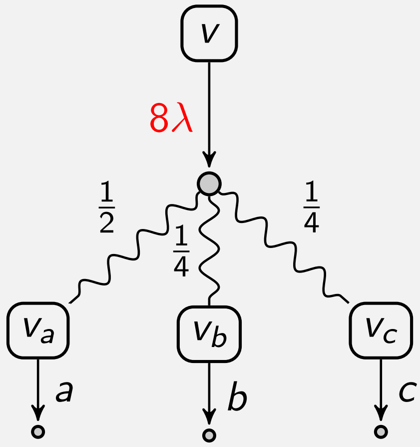
In a finitary MLTS

- $\Delta\,\mathsf{lift}(\approx_{sbis})\,\Theta$ implies $\Delta \approx_{bis} \Theta$
- $\Delta \approx_{bis} \Theta$ implies $\Delta\ \mathsf{lift}(\approx_{sbis})\ \Theta'$, where $\Theta \stackrel{\tau}{\Longrightarrow} \Theta'$

Example



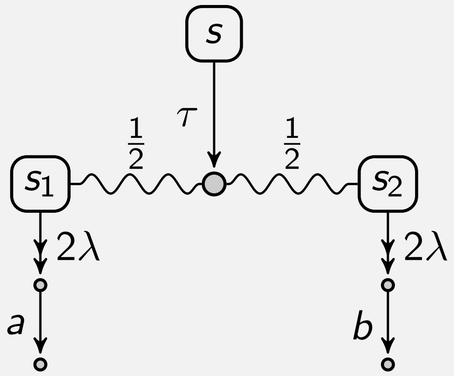
versus

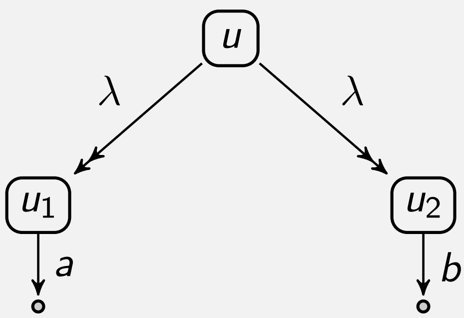


Yes: $s \approx_{sbis} \overline{v}$ because of simple bisimulation

$$s \leftrightarrow \overline{v}$$
$$s_1 \leftrightarrow \frac{1}{2} \cdot \overline{v_b} + \frac{1}{2} \cdot \overline{v_c}$$
$$s_* \leftrightarrow \overline{v_*}$$
$$v \leftrightarrow \overline{s}$$
$$v_* \leftrightarrow \overline{s_*}$$

Example (MAs)





No: $s \not\approx_{sbis} \overline{u}$ because

$$s \xrightarrow{\tau} \frac{1}{2} \cdot \overline{s_1} + \frac{1}{2} \cdot \overline{s_2}$$

can not be matched by $\overline{u}$

Markovian CCS

$$
\begin{array}{lll}
P, Q & ::= & \mathbf{0} \;\mid\; \delta.P \;\mid\; \lambda.D,\; \lambda \in \mathbb{R}^{+} \;\mid\; \mu{:}D,\; \mu \in \mathsf{Act}_\tau \\
 & ::= & \;\mid\; P + Q \;\mid\; P \mid Q \;\mid\; A \qquad \text{declared definitions} \\
D & ::= & (\oplus_{i \in I} p_i \cdot P_i)
\end{array}
$$

Intensional semantics: an MA

- states: terms P, Q
- arrows: $P \xrightarrow{\mu} \Delta$ and $P \overset{\mathbf{d}}{\mapsto} \Delta$ defined inductively

Rules for parallel

(PAR.L)
$$\frac{s \xrightarrow{\mu} \Delta}{s \mid t \xrightarrow{\mu} \Delta \mid \overline{t}}$$

(PAR.R)
$$\frac{t \xrightarrow{\mu} \Theta}{s \mid t \xrightarrow{\mu} \overline{s} \mid \Theta}$$

(PAR.I)
$$\frac{s \xrightarrow{a} \Delta,\; t \xrightarrow{\overline{a}} \Theta}{s \mid t \xrightarrow{\tau} \Delta \mid \Theta}$$

(PAR.L.T)
$$\frac{s \overset{\mathbf{d}}{\mapsto} \Delta,\; t \overset{\delta}{\mapsto} \Theta,\; s \mid t \not\xrightarrow{\tau}}{s \mid t \overset{\mathbf{d}}{\mapsto} \Delta \mid \Theta}$$

(PAR.R.T)
$$\frac{s \overset{\delta}{\mapsto} \Delta, t \overset{\mathbf{d}}{\mapsto} \Theta,\; s \mid t \not\xrightarrow{\tau}}{s \mid t \overset{\mathbf{d}}{\mapsto} \Delta \mid \Theta} \qquad \mathbf{d} = \delta, \lambda$$

$P \mid Q \overset{\mathbf{d}}{\mapsto} \Delta$ only if

- both P and Q can delay
- at least one has to perform indefinite delay δ

Example: $Q = (\lambda_1.P_1 \mid \lambda_2.P_2)$

- $Q \overset{\lambda_1}{\mapsto} (P_1 \mid \lambda_2.P_2)$ because of $\lambda_1.P_1 \overset{\lambda_1}{\mapsto} P_1$ and $\lambda_2.P_2 \overset{\delta}{\mapsto} \lambda_2.P_2$
- $Q \overset{\lambda_2}{\mapsto} (\lambda_1 P_2 \mid P_2)$ because of $\lambda_1.P_1 \overset{\delta}{\mapsto} \lambda_1.P$ and $\lambda_2.P_2 \overset{\lambda_2}{\mapsto} P_2$
- $Q \overset{\delta}{\mapsto} Q$ because of $\lambda_1.P_1 \overset{\delta}{\mapsto} \lambda_1.P_1$ and $\lambda_1.P_1 \overset{\delta}{\mapsto} \lambda_1.P_1$.

some Other rules

(ACTION)
$\mu{:}D \xrightarrow{\mu} [\![D]\!]$

(DELAY)
$\lambda.D \overset{\lambda}{\mapsto} [\![D]\!],$

(D.δ)
$\lambda.D \overset{\delta}{\mapsto} \overline{\lambda.D}$

(δ.E)
$$\frac{P \xrightarrow{\mu} \Delta}{\delta.P \xrightarrow{\mu} \Delta}$$

(δ.D)
$$\frac{P \not\xrightarrow{\tau}}{\delta.P \overset{\delta}{\mapsto} \overline{P}}$$

(EXT)
$$\frac{P \overset{\delta}{\mapsto} \Delta_1,\ Q \overset{\delta}{\mapsto} \Delta_2}{P + Q \overset{\delta}{\mapsto} \Delta_1 + \Delta_2}$$

(EXT.D.L)
$$\frac{P \overset{\delta}{\mapsto} \Delta,\ Q \overset{\delta}{\not\mapsto},\ Q \not\xrightarrow{\tau}}{P + Q \overset{\delta}{\mapsto} \Delta}$$

External actions are insistent

- $(\lambda.Q \mid a{:}P)$ can not delay because
  - $a{:}P \not\overset{\mathbf{d}}{\longmapsto}$
- $\lambda.Q \mid a.P \overset{\lambda}{\longmapsto} Q \mid a.P$ because
  - $\lambda.Q \overset{\lambda}{\longmapsto} Q$
  - $a.P \overset{\delta}{\longmapsto} a.P$

Lazy $a.P$ is defined recursively by

$$a.P \Leftarrow a{:}P + \delta.a.P$$

Compositionality

Theorem:
In a finitary MA, $\Delta \approx_{bis} \Theta$ implies $\Delta \mid \Gamma \approx_{bis} \Theta \mid \Gamma$

A very general semantic equivalence

$P \approx_{rbc} Q$ is the largest relation which is

- compositional
  - preserved by some natural parallel operator on systems
- reduction-closed
  - preserved in some manner internal nondeterministic choices
- preserves barbs
  - some primitive observations

Has been defined for

- process calculi(CCS, CSP, ...), object languages, λ-calculus, higher-order processes, ...

In each case a variation on *bisimulations* have been justified as a proof methodology

Thesis

- A bisimulation equivalence provides a proof method for the natural semantic equivalence, $\approx_{rbc}$
- It is *sound* if $P \approx_{bis} Q$ implies $P \approx_{rbc} Q$
  - to prove a semantic identity it is sufficient to provide a witness bisimulation
- It is *complete* if $P \approx_{rbc} Q$ implies $P \approx_{bis} Q$
  - if a semantic identity is true it is possible to demonstrate it

Theorem:
In mCCS, our bisimulations are sound and complete

Barbs

$\Delta \Downarrow_a^{\geq p}$ whenever

- $\Delta \stackrel{\tau}{\Longrightarrow} \Delta'$
- probability of Δ' performing external action a is at least p.

$\mathcal{R}$ is barb-preserving if whenever $\Delta \ \mathcal{R} \ \Theta$

- $\Delta \Downarrow_a^{\geq p}$ iff $\Theta \Downarrow_a^{\geq p}$

Reduction-closure

$\Delta \Longrightarrow\!\!\!\!\blacktriangleright \Delta'$
whenever Δ can evolve to Δ' via

- internal computations $\stackrel{\tau}{\Longrightarrow}$
- passage of time

$\mathcal{R}$ is reduction-closed if whenever $\Delta \ \mathcal{R} \ \Theta$

- if $\Delta \Longrightarrow\!\!\!\!\blacktriangleright \Delta'$, there is a $\Theta \Longrightarrow\!\!\!\!\blacktriangleright \Theta'$ such that $\Delta' \ \mathcal{R} \ \Theta'$
- if $\Theta \Longrightarrow\!\!\!\!\blacktriangleright \Theta'$, there is a $\Delta \Longrightarrow\!\!\!\!\blacktriangleright \Delta'$ such that $\Delta' \ \mathcal{R} \ \Theta'$.

Future work

- A modal logic which characterises $\approx_{bis}$?
- A polynomial-time algorithm for checking if $\Delta \approx_{bis} \Theta$?
- which returns a distinguishing formula if $\Delta \not\approx_{bis} \Theta$?
- Model-checking algorithms?
- Algebraic characterisation for finite terms in mCCS?
- Categorical justification for $\approx_{bis}$?