SOS rule formats for convex and abstract probabilistic bisimulations

Pedro R. D'Argenio[1,2]   Matias D. Lee[1,2]   Daniel Gebler[3]

[1]FaMAF, Universidad Nacional de Córdoba, Argentina
[2]CONICET, Argentina
[3]VU, Amsterdam, The Netherlands

EXPRESS/SOS
Madrid, Spain - August 2015

Outline

Motivation: Where are our contributions

Four different semantics for probabilistic transition systems

Logical characterizations

Probabilistic transition systems specification

Rules Formats

Future Works

Outline

Motivation: Where are our contributions

Four different semantics for probabilistic transition systems

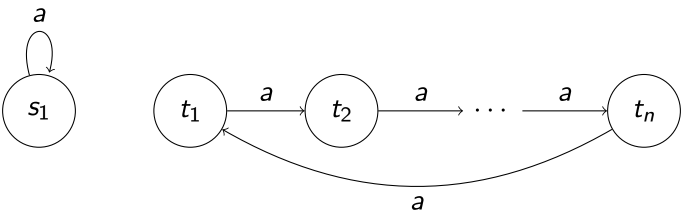
Logical characterizations

Probabilistic transition systems specification

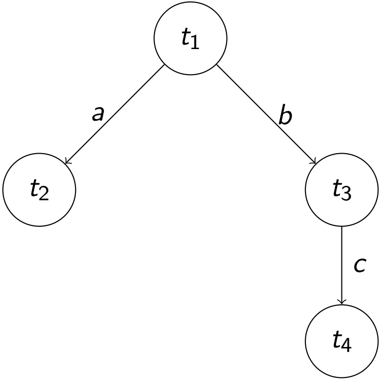
Rules Formats

Future Works

Process Semantics

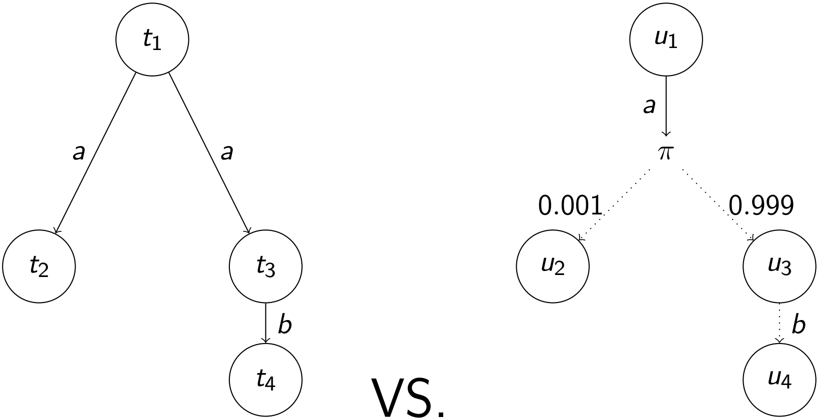


Languages to describe processes



$$a + b.c$$

Models with probabilities: a way to improve the process descriptions.



Outline

Motivation: Where are our contributions

Four different semantics for probabilistic transition systems

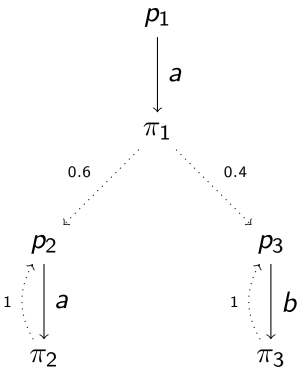
Logical characterizations

Probabilistic transition systems specification

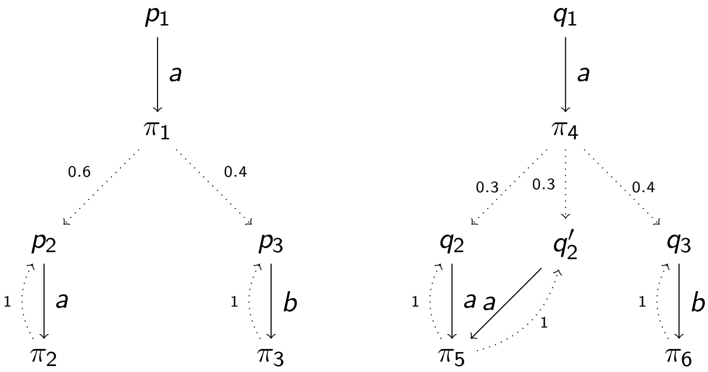
Rules Formats

Future Works

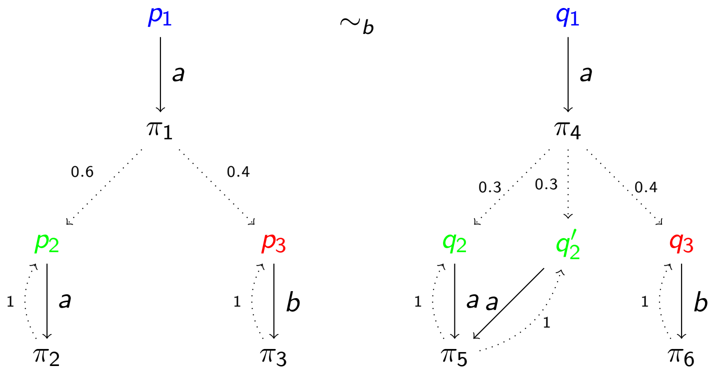
Probabilistic transition systems and bisimulation ($\sim_b$)



Probabilistic transition systems and bisimulation ($\sim_b$)

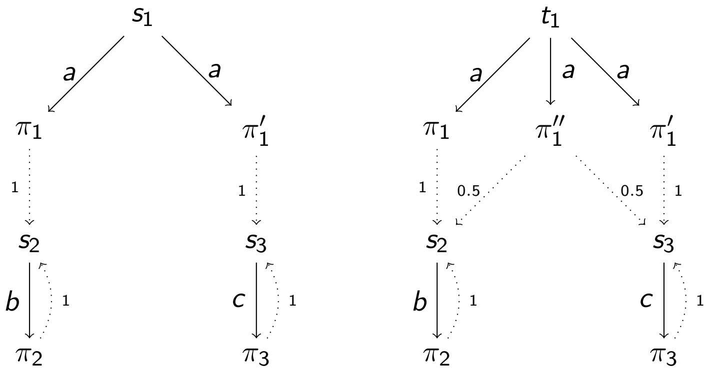


Probabilistic transition systems and bisimulation ($\sim_b$)



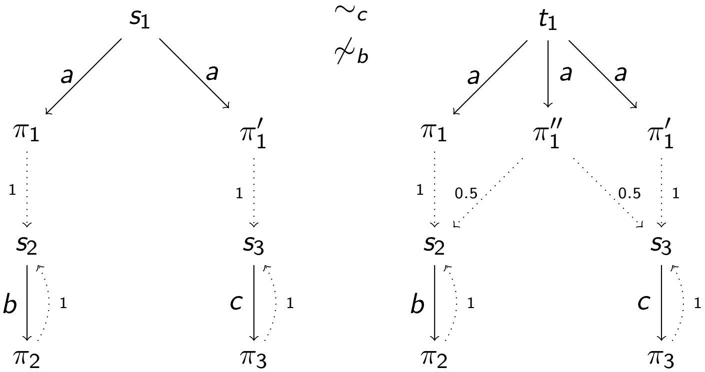
Convex bisimulation ($\sim_c$)

A context with scheduler



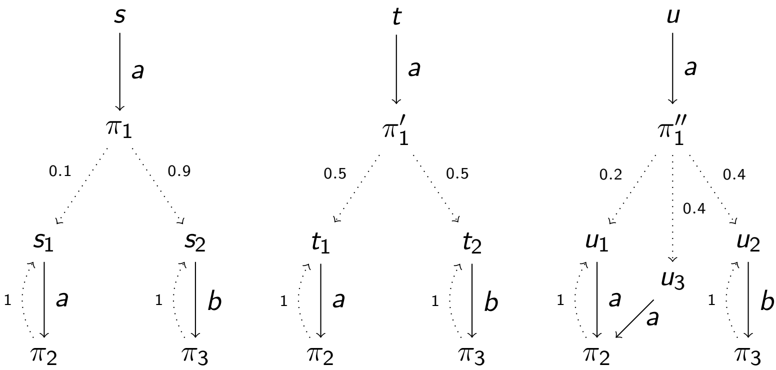
Convex bisimulation ($\sim_c$)

A context with scheduler



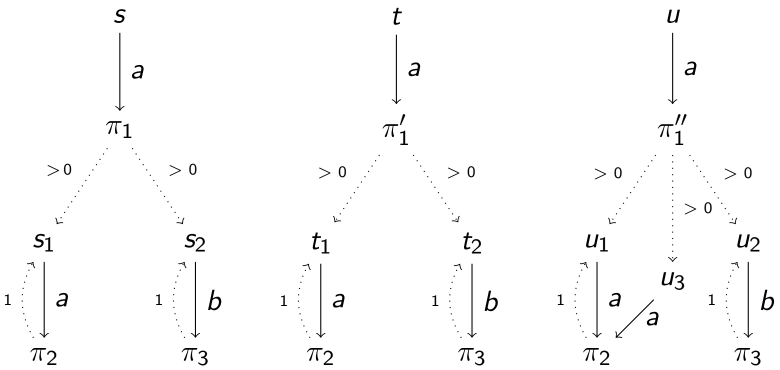
Abstract bisimulation ($\sim_a$)

Only check if the probabilities are greater than zero



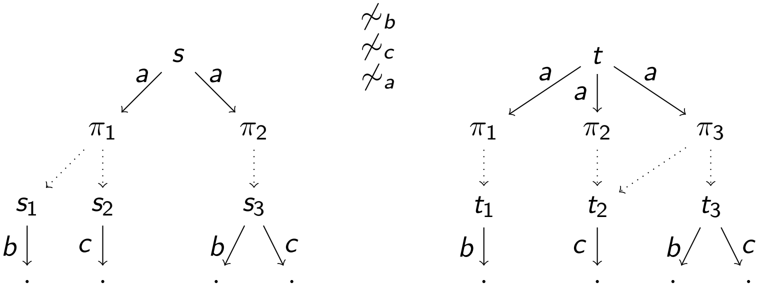
Abstract bisimulation ($\sim_a$)

Only check if the probabilities are greater than zero



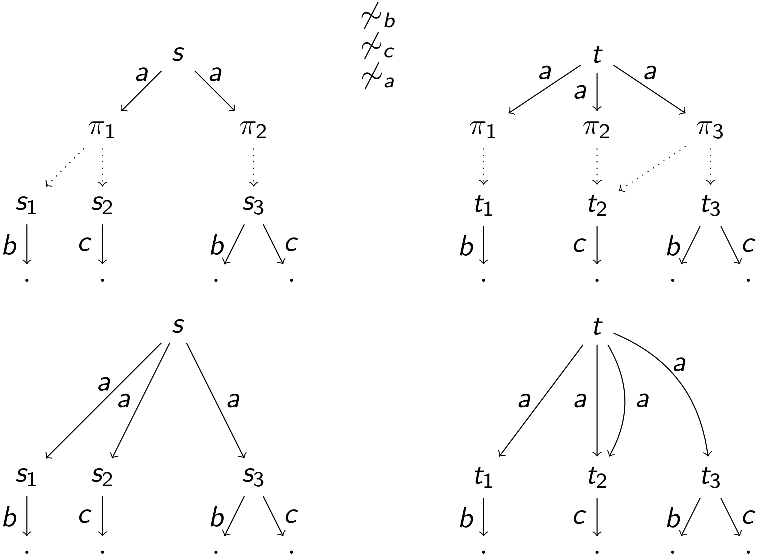
Probability obliterated bisimulations ($\sim_o$)

Forget the distributions



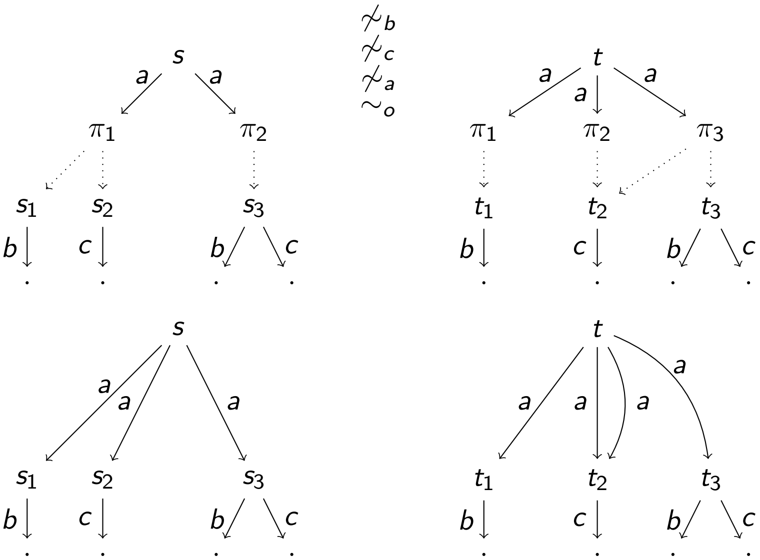
Probability obliterated bisimulations ($\sim_o$)

Forget the distributions

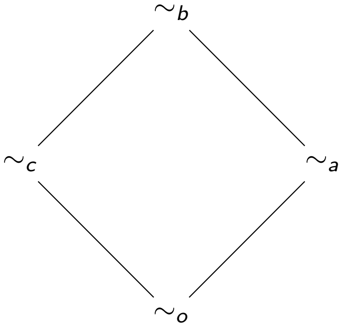


Probability obliterated bisimulations ($\sim_o$)

Forget the distributions



The relation between the semantics



Outline

A logic for each semantic

- The logic $\mathcal{L}_b$ characterizes bisimulation.
- The logic $\mathcal{L}_c$ characterizes convex bisimulation.
- The logic $\mathcal{L}_a$ characterizes probability abstracted bisimulation.
- The logic $\mathcal{L}_o$ characterizes probability obliterated bisimulation.

The Logic $\mathcal{L}_b$

$$\phi := \top \mid \langle a \rangle \psi \mid \langle a \rangle_c \psi \mid \bigwedge_{i \in I} \phi_i \mid \neg \phi$$

$$\psi := [\phi]_p \mid \bigsqcap_{i \in I} \psi_i$$

The semantics of $\mathcal{L}_b$ is defined with the satisfaction relation $\models$

(i)	$t \models \top$	for all $t \in \mathrm{T}(\Sigma_s)$
(ii)	$t \models \langle a \rangle \psi$	if there is $t \xrightarrow{a} \pi$ s.t. $\pi \models \psi$
(iii)	$t \models \langle a \rangle_c \psi$	if there is $t \xrightarrow{a}_c \pi$ s.t. $\pi \models \psi$
(iv)	$t \models \bigwedge_{i \in I} \phi_i$	if $t \models \phi_i$ for all $i \in I$
(v)	$t \models \neg \phi$	if $t \not\models \phi$
(vi)	$\pi \models [\phi]_p$	if $\pi(\{t \in \mathrm{T}(\Sigma_s) \mid t \models \phi\}) > p$
(vii)	$\pi \models \bigsqcap_{i \in I} \psi_i$	if $\pi \models \psi_i$ for all $i \in I$

The Logic $\mathcal{L}_c$

$$\phi := \top \mid \langle a \rangle \psi \mid \langle a \rangle_c \psi \mid \bigwedge_{i \in I} \phi_i \mid \neg \phi$$

$$\psi := [\phi]_p \mid \bigsqcap_{i \in I} \psi_i$$

The semantics of $\mathcal{L}_b$ is defined with the satisfaction relation $\models$

(i)	$t \models \top$	for all $t \in \mathrm{T}(\Sigma_s)$
(iii)	$t \models \langle a \rangle_c \psi$	if there is $t \xrightarrow{a}_c \pi$ s.t. $\pi \models \psi$
(iv)	$t \models \bigwedge_{i \in I} \phi_i$	if $t \models \phi_i$ for all $i \in I$
(v)	$t \models \neg \phi$	if $t \not\models \phi$
(vi)	$\pi \models [\phi]_p$	if $\pi(\{t \in \mathrm{T}(\Sigma_s) \mid t \models \psi\}) > p$
(vii)	$\pi \models \bigsqcap_{i \in I} \psi_i$	if $\pi \models \psi_i$ for all $i \in I$

The Logic $\mathcal{L}_a$

$$\phi := \top \mid \langle a \rangle \psi \mid \langle a \rangle_c \psi \mid \bigwedge_{i \in I} \phi_i \mid \neg \phi$$

$$\psi := [\phi]_0 \mid \bigsqcap_{i \in I} \psi_i$$

The semantics of $\mathcal{L}_b$ is defined with the satisfaction relation $\models$

(i)	$t \models \top$	for all $t \in \mathsf{T}(\Sigma_s)$
(ii)	$t \models \langle a \rangle \psi$	if there is $t \xrightarrow{a} \pi$ s.t. $\pi \models \psi$
(iv)	$t \models \bigwedge_{i \in I} \phi_i$	if $t \models \phi_i$ for all $i \in I$
(v)	$t \models \neg \phi$	if $t \not\models \phi$
(vi)	$\pi \models [\phi]_p$	if $\pi(\{t \in \mathsf{T}(\Sigma_s) \mid t \models \psi\}) > p$
(vii)	$\pi \models \bigsqcap_{i \in I} \psi_i$	if $\pi \models \psi_i$ for all $i \in I$

The Logic $\mathcal{L}_o$

$$\phi := \top \mid \langle a \rangle \psi \mid \langle a \rangle_c \psi \mid \bigwedge_{i \in I} \phi_i \mid \neg \phi$$

$$\psi := [\phi]_0 \mid \bigsqcap_{i \in I} \psi_i$$

The semantics of $\mathcal{L}_b$ is defined with the satisfaction relation $\models$

(i)	$t \models \top$	for all $t \in \mathrm{T}(\Sigma_s)$
(ii)	$t \models \langle a \rangle \psi$	if there is $t \xrightarrow{a} \pi$ s.t. $\pi \models \psi$
(iv)	$t \models \bigwedge_{i \in I} \phi_i$	if $t \models \phi_i$ for all $i \in I$
(v)	$t \models \neg \phi$	if $t \not\models \phi$
(vi)	$\pi \models [\phi]_p$	if $\pi(\{t \in \mathrm{T}(\Sigma_s) \mid t \models \psi\}) > p$
(vii)	$\pi \models \bigsqcap_{i \in I} \psi_i$	if $\pi \models \psi_i$ for all $i \in I$

Theorem [Logical characterizations]

For all $\chi \in \{b, c, a, o\}$ and for all t_1, t_2,

$$t_1 \sim_\chi t_2 \quad \text{if and only if} \quad t_1 \sim_{\mathcal{L}_\chi} t_2$$

where

- $\mathcal{L}_\chi(t) = \{\phi \in \mathcal{L}_\chi \mid t \models \phi\}$,
- $\mathcal{L}_\chi(\pi) = \{\psi \in \mathcal{L}_\chi \mid \pi \models \psi\}$,
- $t_1 \sim_{\mathcal{L}_\chi} t_2$ iff $\mathcal{L}_\chi(t_1) = \mathcal{L}_\chi(t_2)$ and
- $\pi_1 \sim_{\mathcal{L}_\chi} \pi_2$ iff $\mathcal{L}_\chi(\pi_1) = \mathcal{L}_b(\pi_2)$.

Outline

Transitions System Specification (TSS) (Σ, A, R)

- A signature Σ.

$$\Sigma = \{0, a.\_, b.\_, \_ + \_\}$$

- A set of actions A.

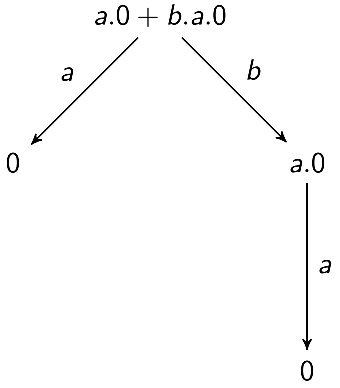
$$A = \{a, b\}$$

- A set of rules R.

$$\frac{}{a.x \xrightarrow{a} x} \qquad \frac{x \xrightarrow{a} x'}{x + y \xrightarrow{a} x'} \qquad \frac{y \xrightarrow{a} y'}{x + y \xrightarrow{a} y'}$$

Given a TSS, each term defines a transition system

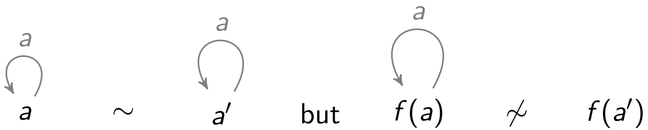
$$\frac{}{a.x \xrightarrow{a} x} \qquad \frac{}{b.x \xrightarrow{b} x} \qquad \frac{x \xrightarrow{a} x'}{x + y \xrightarrow{a} x'} \qquad \frac{y \xrightarrow{a} y'}{x + y \xrightarrow{a} y'}$$



Not every TSS defines compositional operators

- Signature: $\Sigma = \{a, a', f(\_)\}$
- Label: $A = \{a\}$
- Rules R:

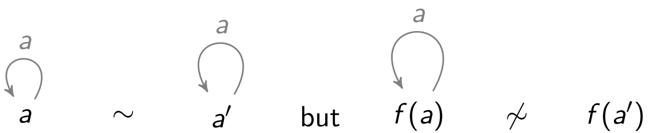
$$\frac{}{a \xrightarrow{a} a} \qquad \frac{}{a' \xrightarrow{a} a'} \qquad \frac{x \xrightarrow{a} a}{f(x) \xrightarrow{a} f(x)}$$



Not every TSS defines compositional operators

- Signature: $\Sigma = \{a, a', f(\_)\}$
- Label: $A = \{a\}$
- Rules R:

$$\frac{}{a \xrightarrow{a} a} \qquad \frac{}{a' \xrightarrow{a} a'} \qquad \frac{x \xrightarrow{a} a}{f(x) \xrightarrow{a} f(x)}$$



A solution: Define a rule format (rules with a particular shape) that only allows to define good specification languages.

Probabilities are Cool

Probabilities are Cool

Probabilistic Transition System Specifications (PTSS)
are used to define languages to describes PTS

Definition (PTSS)

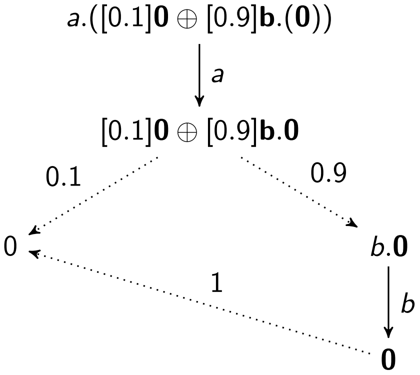
A probabilistic transition system specification (PTSS) is a triple $P = (\Sigma, A, R)$ where Σ is a probabilistically lifted signature, A is a set of labels, and R is a set of rules of the form:

$$\frac{\{t_k \xrightarrow{a_k} \theta_k \mid k \in K\} \cup \{t_l \stackrel{b_l}{\not\longrightarrow} \mid l \in L\} \cup \{\theta_j(T_j) \bowtie_j q_j \mid j \in J\}}{t \xrightarrow{a} \theta}$$

where K, L, J are index sets, $t, t_k, t_l \in \mathbb{T}(\Sigma_s)$, $a, a_k, b_l \in A$, $T_j \subseteq \mathsf{T}(\Sigma_s)$, $\bowtie_j \in \{>, \geq, <, \leq\}$, $q_j \in [0, 1]$ and $\theta_j, \theta_k, \theta \in \mathbb{T}(\Sigma_d)$.

Given a PTSS, each term defines a PTS

$$\frac{}{a.\mu \xrightarrow{a} \mu} \qquad \frac{}{b.\mu \xrightarrow{b} \mu} \qquad \frac{x_1 \xrightarrow{a} \mu_1}{x_1 + x_2 \xrightarrow{a} \mu_1} \qquad \frac{x_2 \xrightarrow{a} \mu_2}{x_2 + x_2 \xrightarrow{a} \mu_2}$$



Outline

Main contribution

For each semantic,

we have defined a rule format

or a specification format

(a rule format with restrictions over the set of rules)

to define compositional languages to specify

probabilistic transition systems.

How to define a format - ROUGHLY

- Each rule format has to fit in well with the particularities of each semantic.

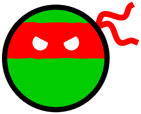
How to define a format - ROUGHLY

- Each rule format has to fit in well with the particularities of each semantic.
- For example, the format for probability abstracted bisimulation only allows quantitative premises with the following form

  $$\theta(Y) > 0$$

  Otherwise, we could check the probability of reaching a particular set of states.

A format can be “complex”...



$nt\mu f\theta / nt\mu x\theta$ format (1/2)

A rule $r \in R$ is in <u>$nt\mu f\theta$ format</u> if it has the following form

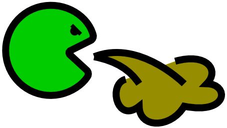
$$\frac{\bigcup_{m\in M}\{t_m(\vec{z}) \xrightarrow{a_m} \mu_m^{\vec{z}} \mid \vec{z} \in \mathcal{Z}\} \;\cup\; \bigcup_{n\in N}\{t_n(\vec{z}) \stackrel{b_n}{\not\longrightarrow} \mid \vec{z} \in \mathcal{Z}\} \cup \{\theta_l(Y_l) \trianglerighteq_{l,k} p_{l,k} \mid l \in L, k \in K_l\}}{f(\zeta_1, \ldots, \zeta_{\mathrm{rk}(f)}) \xrightarrow{a} \theta}$$

with $\trianglerighteq_{l,k} \in \{>, \geq\}$ for all $l \in L$ and $k \in K_l$, and $\mathcal{Z} = \mathrm{Diag}\{Y_l\}_{l\in L} \times \prod_{\zeta\in W}\{\zeta\}$, with $W \subseteq \mathcal{V} \cup \mathcal{V}_d \setminus \bigcup_{l\in L} Y_l$. In addition, it has to satisfy the following conditions: ...

$nt\mu f\theta/nt\mu x\theta$ format (2/2)

1. Each set Y_l should be at least countably infinite, for all $l \in L$, and the cardinality of L should be strictly smaller than that of the Y_l's.
2. All variables $\zeta_1, \ldots, \zeta_{\mathsf{rk}(f)}$ are different.
3. All variables $\mu_m^{\vec{z}}$, with $m \in M$ and $\vec{z} \in \mathcal{Z}$, are different and $\{\zeta_1, \ldots, \zeta_{\mathsf{rk}(f)}\} \cap \{\mu_m^{\vec{z}} \mid \vec{z} \in \mathcal{Z}, m \in M\} = \emptyset$.
4. For all $l \in L$, $Y_l \cap \{\zeta_1, \ldots, \zeta_{\mathsf{rk}(f)}\} = \emptyset$, and $Y_l \cap Y_{l'} = \emptyset$ for all $l' \in L$, $l \neq l'$.
5. For all $m \in M$, the set $\{\mu_m^{\vec{z}} \mid \vec{z} \in \mathcal{Z}\} \cap \left(\mathcal{V}(\theta) \cup (\bigcup_{l \in L} \mathcal{V}(\theta_l)) \cup W\right)$ is finite.
6. For all $l \in L$, the set $Y_l \cap \left(\mathcal{V}(\theta) \cup \bigcup_{l' \in L} \mathcal{V}(\theta_{l'})\right)$ is finite.

... or more complex.



Convex $nt\mu f\theta/nt\mu x\theta$ format (1/2)

A rule $r \in R$ is in convex $nt\mu f\theta$ format if has the form

$$\frac{\bigcup_{m\in M}\{t_m(\vec{z}) \xrightarrow{a_m} \mu_m^{\vec{z}} \mid \vec{z} \in \mathcal{Z}\} \qquad \bigcup_{n\in N}\{t_n(\vec{z}) \overset{b_n}{\not\longrightarrow} \mid \vec{z} \in \mathcal{Z}\} \\ \bigcup_{\tilde{m}\in\tilde{M}}\{t_{\tilde{m}}(\vec{z}_{\tilde{m}}) \xrightarrow{a_{\tilde{m}}} \mu_i^{\tilde{m}} \mid i \in \mathbb{N}\} \\ \bigcup_{\tilde{m}\in\tilde{M}}\{(\bigoplus_{i\in\mathbb{N}}[p_i^{\tilde{m}}]\mu_i^{\tilde{m}})(Y_l) \trianglerighteq_{l,k} p_{l,k} \mid l \in L_{\tilde{m}}, k \in K_l\}}{f(\zeta_1,\ldots,\zeta_{\mathrm{rk}(f)}) \xrightarrow{a} \theta}$$

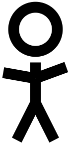
with $L = \cup_{\tilde{m}\in\tilde{M}} L_{\tilde{m}}$, $L_{\tilde{m}} \cap L_{\tilde{m}'} = \emptyset$ whenever $\tilde{m} \neq \tilde{m}'$,
$\trianglerighteq_{l,k} \in \{>, \geq\}$ for all $l \in L$ and $k \in K_l$,
$\mathcal{Z} = \mathrm{Diag}\{Y_l\}_{l\in L} \times \prod_{\zeta\in W}\{\zeta\}$, with $W \subseteq \mathcal{V} \cup \mathcal{V}_d \setminus \bigcup_{l\in L} Y_l$.
In addition, it should also satisfy conditions 1 to 6 (see above) and the following extra conditions: ...

Convex $nt\mu f\theta/nt\mu x\theta$ format (2/2)

7. For every $\tilde{m} \in \tilde{M}$, the family $\{p_i^{\tilde{m}}\}_{i\in\mathbb{N}} \subseteq [0,1] \cap \mathbb{Q}$ and $\sum_{i\in\mathbb{N}} p_i^{\tilde{m}} = 1$
8. For every $\tilde{m} \in \tilde{M}$, there is exactly one $j \in \mathbb{N}$ such that $\mu_j^{\tilde{m}} = \mu_m^{\vec{z}}$ for some $m \in M$ and $\vec{z} \in \mathcal{Z}$, in which case also $t_{\tilde{m}}(\vec{z}_{\tilde{m}}) \xrightarrow{a_{\tilde{m}}} \mu_j^{\tilde{m}} = t_m(\vec{z}) \xrightarrow{a_m} \mu_m^{\vec{z}}$. Moreover $\{\mu_i^{\tilde{m}} \mid i \in \mathbb{N}\} \cap \{\mu_i^{\tilde{m}'} \mid i \in \mathbb{N}\} = \emptyset$ for all $\tilde{m} \neq \tilde{m}'$, and $\{\mu_i^{\tilde{m}} \mid i \in \mathbb{N}\} \cap \{\zeta_1, \ldots, \zeta_{\mathrm{rk}(f)}\} = \emptyset$.
9. No variable $\mu_m^{\vec{z}}$, with $m \in M$ and $\vec{z} \in \mathcal{Z}$, appears in the source of a premise (i.e. in the set W) or in a d-sorted position of a subterm in the target of the conclusion θ.
10. θ is linear for $\{\mu_m^{\vec{z}} \mid m \in M, \vec{z} \in \mathcal{Z}\}$.

and some more conditions ... 

... or "simpler".



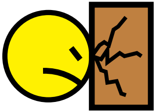
Probability abstracted $nt\mu f\theta/nt\mu x\theta$ format

Definition

A PTSS $P = \langle \Sigma, A, R \rangle$ is in probability abstracted $nt\mu f\theta/nt\mu x\theta$ format if

1. it is in $nt\mu f\theta/nt\mu x\theta$ format and
2. for every rule $r \in R$ and quantitative premise $\theta(Y) \trianglerighteq p \in \mathrm{qprem}(r)$, $p = 0$.

... or “complex”.



Probability obliterated $nt\mu f\theta$ format

A rule $r \in R$ is in probability obliterated $nt\mu f\theta$ format if it has the form

$$\frac{\bigcup_{m\in M}\{t_m \xrightarrow{a_m} \mu_m\} \quad \cup \quad \bigcup_{n\in N}\{t_n \stackrel{b_n}{\not\longrightarrow}\} \quad \cup \quad \bigcup_{l\in L}\{\theta_l(\{y_l\}) > 0\}}{f(\zeta_1,\ldots,\zeta_{\mathrm{rk}(f)}) \xrightarrow{a} \theta}$$

where all variables $\zeta_1,\ldots,\zeta_{\mathrm{rk}(f)}$, μ_m, with $m \in M$, and y_l, with $l \in L$, are different and the following restrictions are satisfied:

1. For all $m \in M$, $\mathcal{V}(t_m) \cap \{\mu_{m'} \mid m' \in M\} = \emptyset$. Similarly, for all $n \in N$, $\mathcal{V}(t_n) \cap \{\mu_{m'} \mid m' \in M\} = \emptyset$.
2. For all $l \in L$, θ_l is linear for $\{\mu_{m'} \mid m' \in M\}$ and, moreover, for all $l, l' \in L$ with $l \neq l'$, $\mathcal{V}(\theta_l) \cap \mathcal{V}(\theta_{l'}) \cap \{\mu_m \mid m \in M\} = \emptyset$.
3. θ is linear for $\{\mu_{m'} \mid m' \in M\}$, $\mathcal{V}(\theta) \cap \left(\bigcup_{l\in L} \mathcal{V}(\theta_l)\right) \cap \{\mu_m \mid m \in M\} = \emptyset$, and no variable μ_m appear in a d-sorted position of a subterm of the target of the conclusion θ.

The key to understand each format:

The understanding of the particularities of each semantic.

Outline

Future Works?

- To study other variants of bisimulation for PTS.
- To study semantics and logics for PTS with internal transitions.
- To extend these and other results to ULTras.