Helmut Veith Workshop - Turracher Höhe - 28.1.20

Presented at LICS 2019

The Theory of Traces for Systems with Probability, Nondeterminism, and Termination

Valeria Vignudelli

ENS DE LYON

Ana Sokolova

UNIVERSITY of SALZBURG

Joint work with

Filippo Bonchi

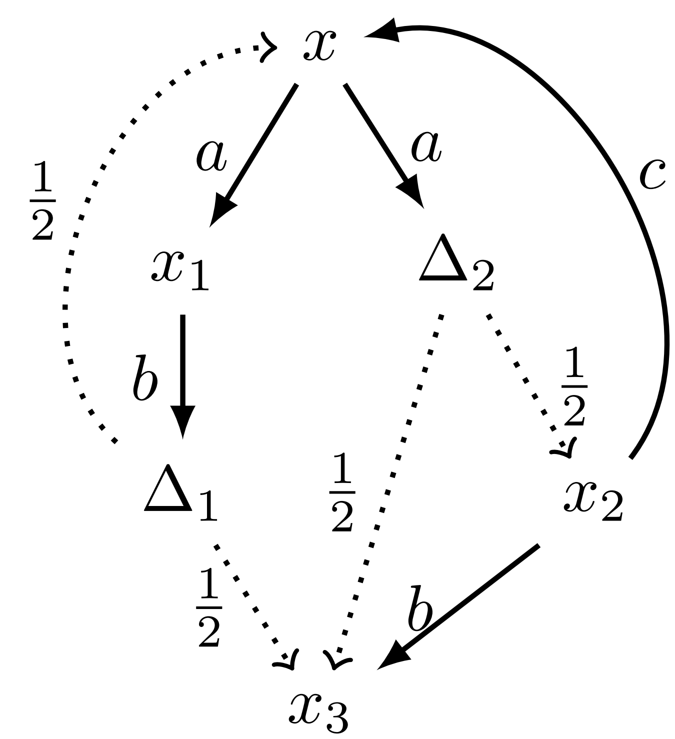
IN SUPREMÆ DIGNITATIS 1343

ENS DE LYON

Probabilistic Nondeterministic Labeled Transition Systems

$$t\colon X \to (\mathcal{P}\mathcal{D}X)^A$$

Trace Semantics for these systems is usually defined by means of schedulers and resolutions

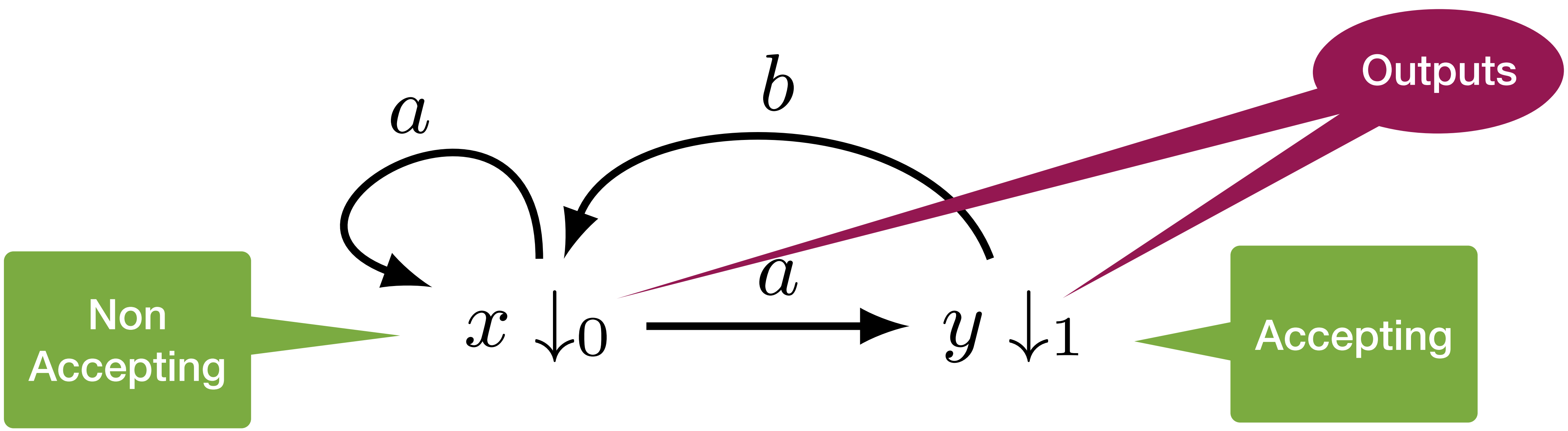


We take a totally different view: our semantics is based on automata theory, algebra and coalgebra

WARNING: In this talk, we will present our theory in its simplest possible form, throwing away all category theory

Nondeterministic Automata

$$\langle o, t\rangle \colon X \to 2 \times (\mathcal{P}X)^A$$



$$X = \{x, y\} \qquad A = \{a, b\}$$

Language Semantics

NFA = LTS + output

$X \to 2 \times (\mathcal{P}X)^A$

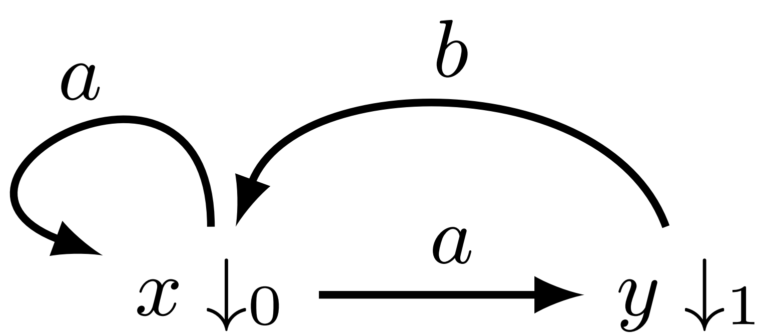
$$\begin{tikzcd} x \downarrow_0 \arrow[loop above, "{a,b}"] \arrow[r, "b"] & y \downarrow_1 \end{tikzcd}$$

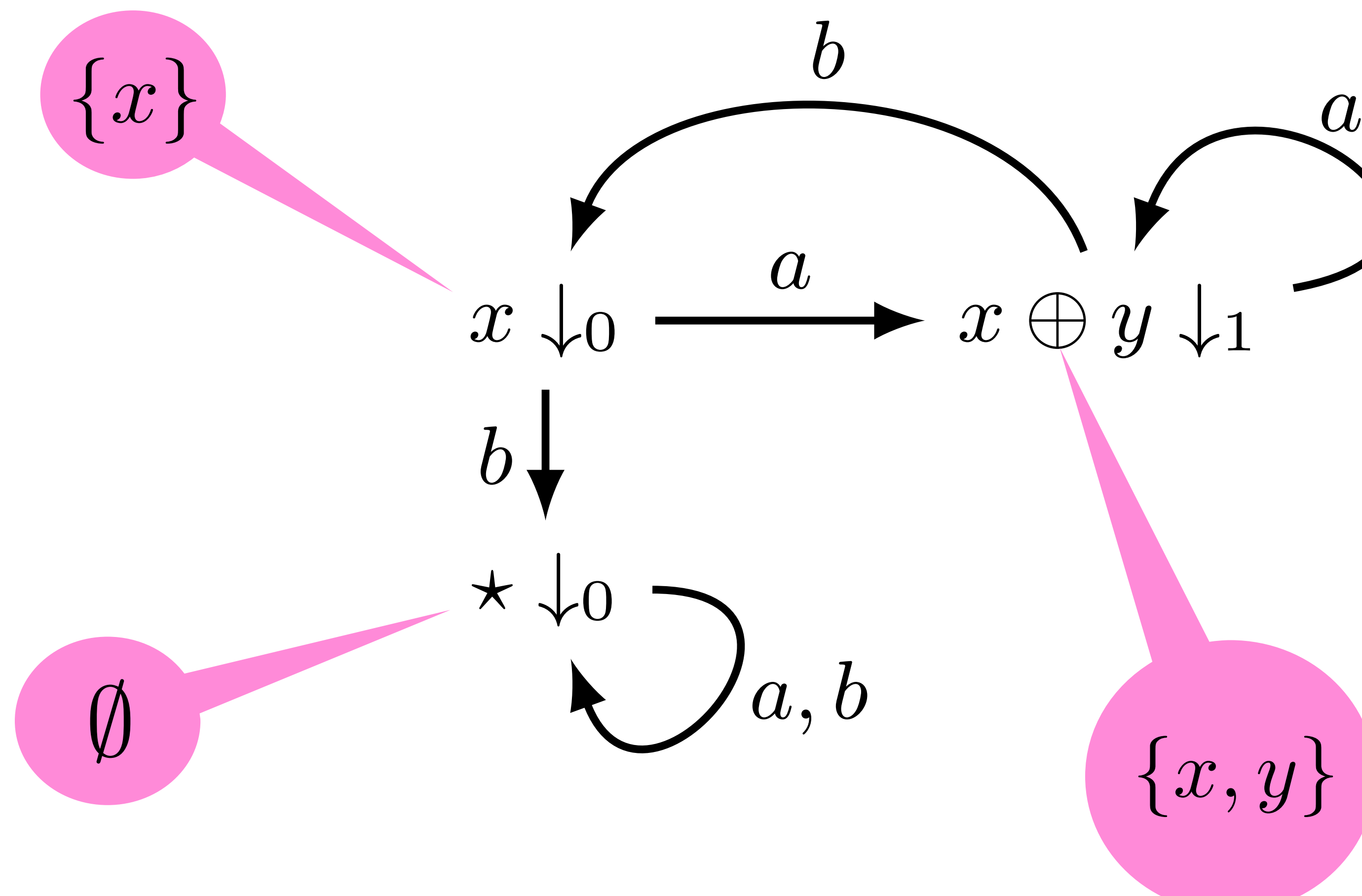
$[\![\cdot]\!] \colon X \to 2^{A^*}$

$[\![x]\!] = (a \cup b)^* b = \{w \in \{a,b\}^* \mid w \text{ ends with a } b\}$

Determinisation for Nondeterministic Automata

$$\langle o, t \rangle \colon X \to 2 \times (\mathcal{P}X)^A \quad \Longrightarrow \quad \langle o^\sharp, t^\sharp \rangle \colon \mathcal{P}X \to 2 \times (\mathcal{P}X)^A$$



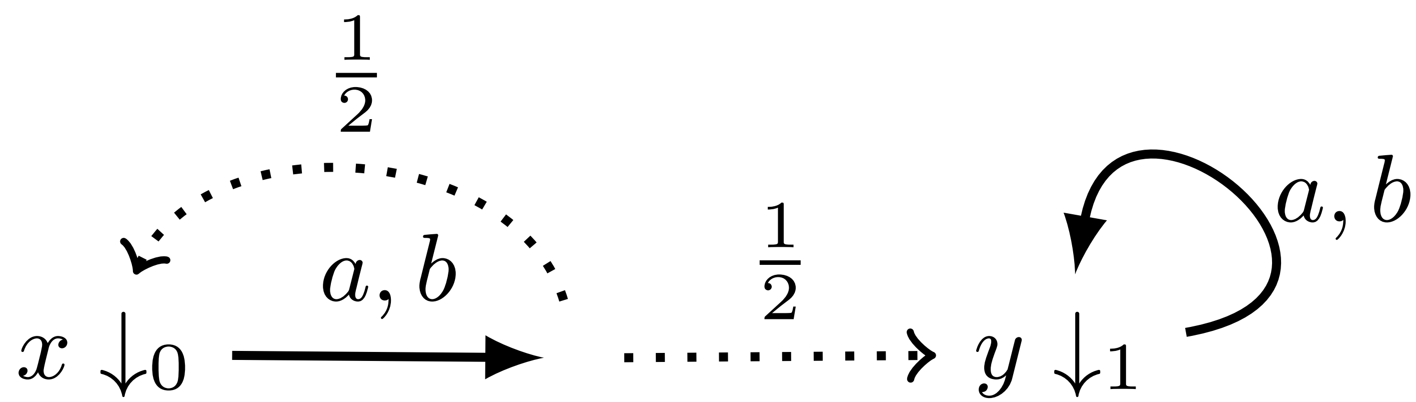


$$[\![\cdot]\!] \colon \mathcal{P}X \to 2^{A^*}$$

$$[\![S]\!](\varepsilon) = o^\sharp(S)$$
$$[\![S]\!](aw) = [\![t^\sharp(S)(a)]\!](w)$$

Probabilistic Automata

$$\langle o, t \rangle \colon X \to [0,1] \times (\mathcal{D}X)^A$$

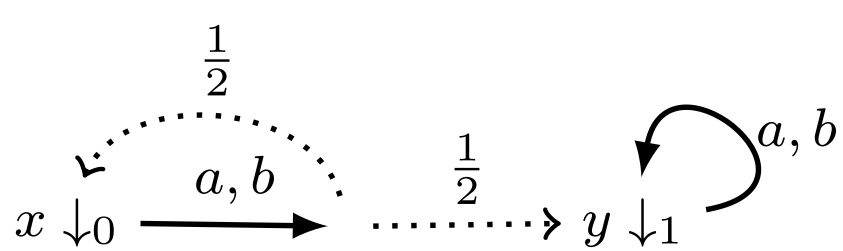


$$X = \{x, y\} \qquad A = \{a, b\}$$

Probabilistic Language Semantics

Rabin PA = PTS + output

$X \to [0,1] \times (\mathcal{D}X)^A$

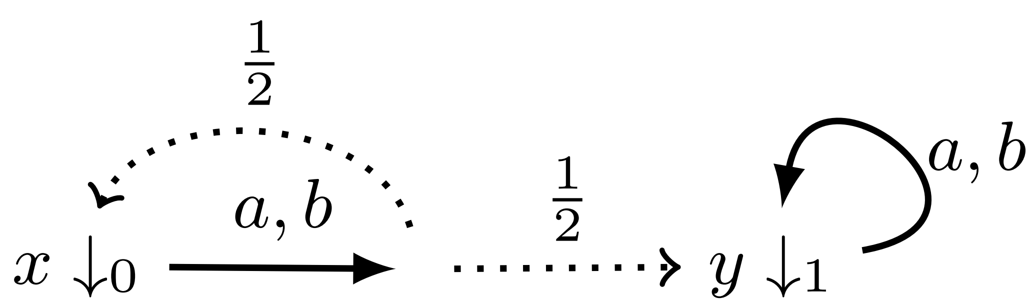


$$[\![\cdot]\!] : X \to [0,1]^{A^*}$$

$$[\![x]\!] = \left(a \mapsto \frac{1}{2}, aa \mapsto \frac{3}{4}, \dots\right)$$

Determinisation for Probabilistic Automata

$$\langle o, t\rangle \colon X \to [0,1] \times (\mathcal{D}X)^A \quad \Longrightarrow \quad \langle o^\sharp, t^\sharp\rangle \colon \mathcal{D}X \to [0,1] \times (\mathcal{D}X)^A$$



$x \downarrow_0$

δ_x

$\Big\downarrow a, b$

$x +_{\frac{1}{2}} y \downarrow_{\frac{1}{2}}$

$\Big\downarrow a, b$

$x +_{\frac{1}{4}} y \downarrow_{\frac{3}{4}}$

$x \mapsto \frac{1}{4}$
$y \mapsto \frac{3}{4}$

$\Big\downarrow a, b$

$\vdots$

$$[\![\cdot]\!] \colon \mathcal{D}X \to [0,1]^{A^*}$$

$$[\![\Delta]\!](\varepsilon) = o^\sharp(\Delta)$$
$$[\![\Delta]\!](aw) = [\![t^\sharp(\Delta)(a)]\!](w)$$

Toward a GSOS semantics

In the determinisation of **nondeterministic** automata we use terms built of the following syntax

$$s, t \ ::= \ \star, \ s \oplus t, \ x \in X$$

to represent states in $\mathcal{P}X$

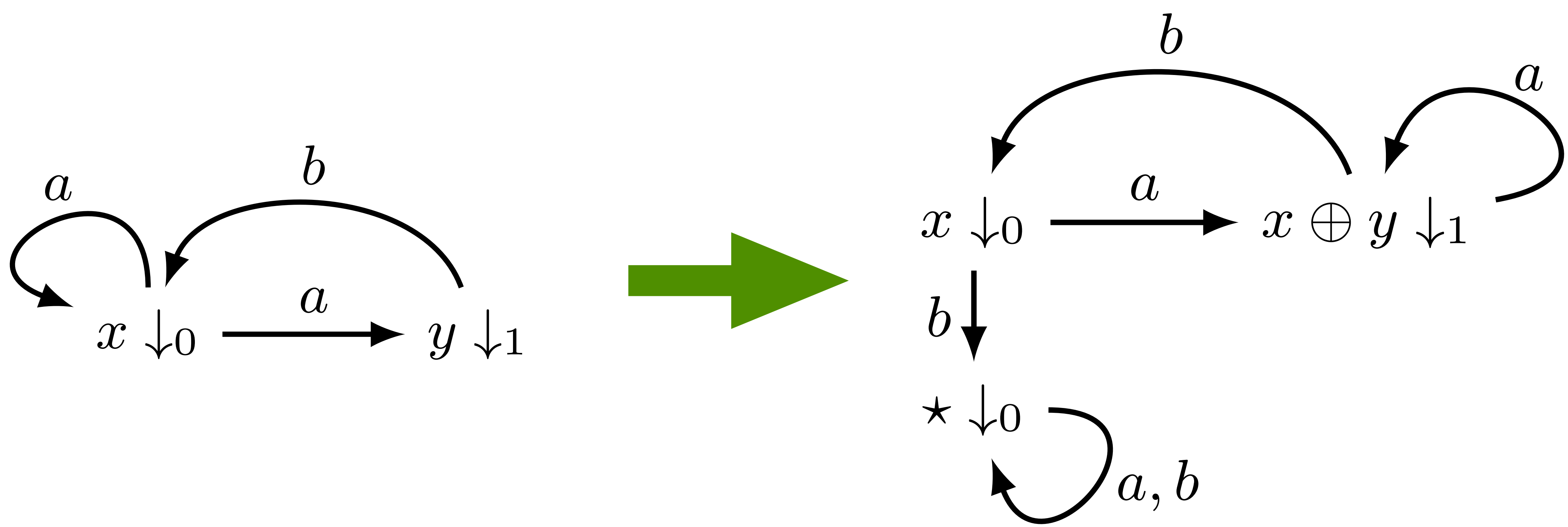
In the determinisation of **probabilistic** automata we use terms built of the following syntax

$$s, t \ ::= \ s +_p t, \ x \in X \quad \text{for all } p \in [0,1]$$

to represent elements of $\mathcal{D}X$

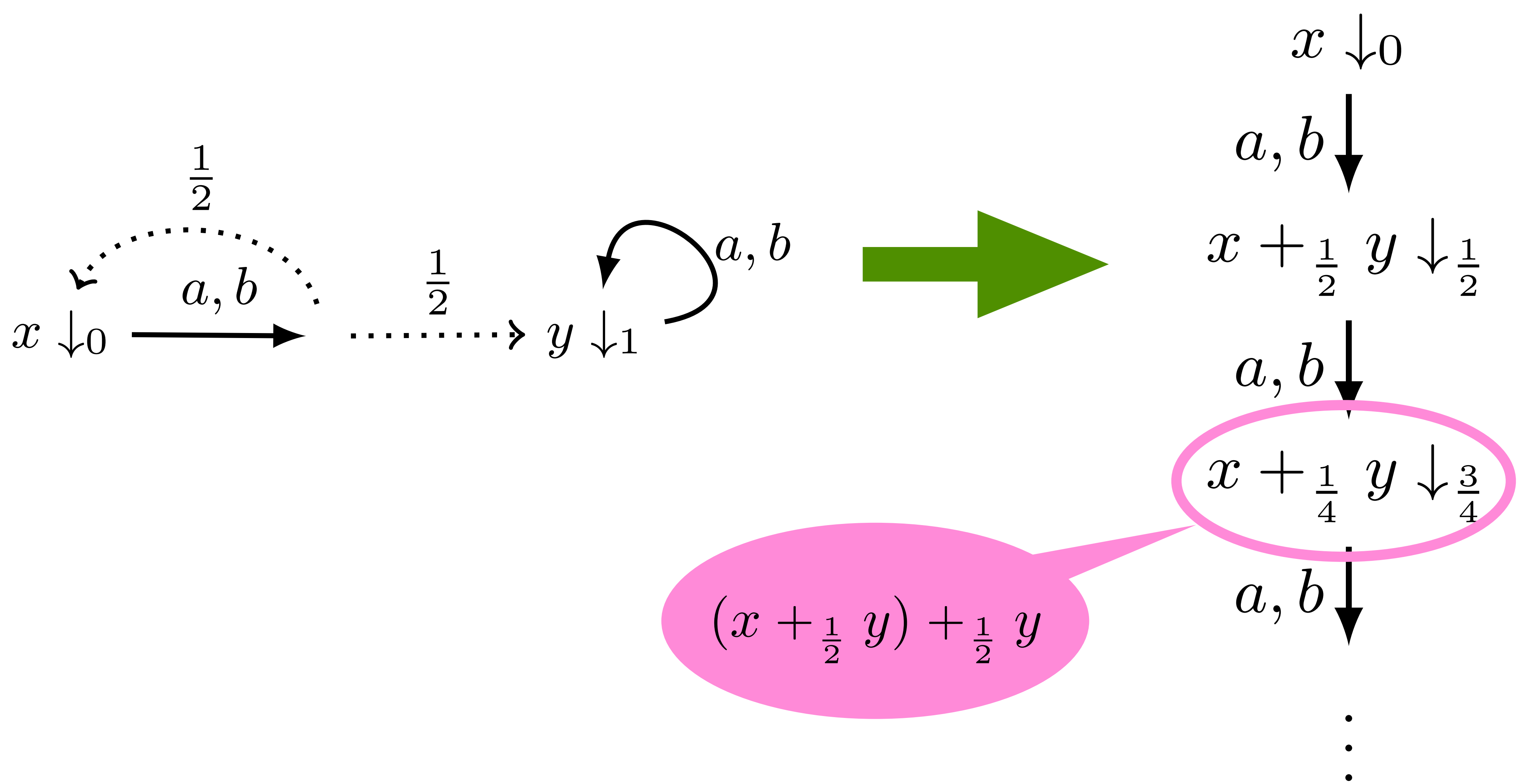
GSOS Semantics for Nondeterministic Automata

$$\frac{-}{\star \xrightarrow{a} \star} \qquad \frac{s \xrightarrow{a} s' \quad t \xrightarrow{a} t'}{s \oplus t \xrightarrow{a} s' \oplus t'} \qquad \frac{-}{\star \downarrow_0} \qquad \frac{s \downarrow_{b_1} \quad t \downarrow_{b_2}}{s \oplus t \downarrow_{b_1 \sqcup b_2}}$$



GSOS Semantics for Probabilistic Automata

$$\frac{s \xrightarrow{a} s' \quad t \xrightarrow{a} t'}{s +_p t \xrightarrow{a} s' +_p t'} \qquad \frac{s \downarrow_{q_1} \quad t \downarrow_{q_2}}{s +_p t \downarrow_{p \cdot q_1 + (1-p) \cdot q_2}}$$



The Algebraic Theory of Semilattices with Bottom

$$s, t \ ::= \ \star, \ s \oplus t, \ x \in X$$

$$\begin{array}{ccc} (x \oplus y) \oplus z & \overset{(A)}{=} & x \oplus (y \oplus z) \\ x \oplus y & \overset{(C)}{=} & y \oplus x \\ x \oplus x & \overset{(I)}{=} & x \\ x \oplus \star & \overset{(B)}{=} & x \end{array}$$

The set of terms quotiented by these axioms is isomorphic to $\mathcal{P}X$

this theory is a presentation for the powerset monad

The Algebraic Theory of Convex Algebras

$$s, t \ ::= \ s +_p t, \ x \in X \quad \text{for all } p \in [0,1]$$

$$\begin{aligned}
(x +_q y) +_p z &\overset{(A_p)}{=} x +_{pq} (y +_{\frac{p(1-q)}{1-pq}} z) \\
x +_p y &\overset{(C_p)}{=} y +_{1-p} x \\
x +_p x &\overset{(I_p)}{=} x
\end{aligned}$$

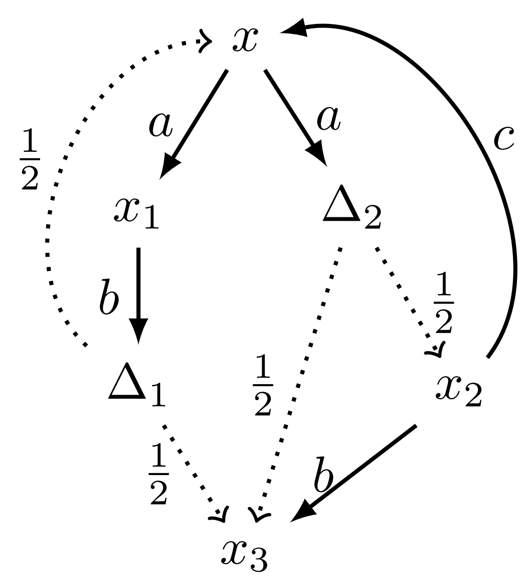
The set of terms quotiented by these axioms is isomorphic to $\mathcal{D}X$

this theory is a presentation for the distribution monad

Probabilistic Nondeterministic Language Semantics ?

NPA

$X \to ? \times (\mathcal{P}\mathcal{D}X)^A$



$[\![x]\!] = ???$

$[\![\cdot]\!]: X \to ?^{A^*}$

Algebraic Theory for Subsets of Distributions ?

For our approach it is convenient to have a theory presenting subsets of distributions

Monads can be composed by means of distributive laws, but, unfortunately, there exists no distributive law amongst powerset and distributions (Daniele Varacca Ph.D thesis)

Other general approach to compose monads/algebraic theories fail

Our first step is to decompose the powerset monad...

Three Algebraic Theories

Nondeterminism $\bigoplus$

$$(x \oplus y) \oplus z \overset{(A)}{=} x \oplus (y \oplus z)$$
$$x \oplus y \overset{(C)}{=} y \oplus x$$
$$x \oplus x \overset{(I)}{=} x$$

Monad: $\mathcal{P}_{ne}$

Algebras: **Semilattices**

Probability $+_p$

$$(x +_q y) +_p z \overset{(A_p)}{=} x +_{pq} (y +_{\frac{p(1-q)}{1-pq}} z)$$
$$x +_p y \overset{(C_p)}{=} y +_{1-p} x$$
$$x +_p x \overset{(I_p)}{=} x$$

Monad: $\mathcal{D}$

Algebras: **Convex Algebras**

Termination $\star$

no axioms

Monad: $\cdot + 1$

Algebras: **Pointed Sets**

The Algebraic Theory of Convex Semilattices

$$\oplus \quad +_p$$

$$(x \oplus y) \oplus z \stackrel{(A)}{=} x \oplus (y \oplus z) \qquad (x +_q y) +_p z \stackrel{(A_p)}{=} x +_{pq} (y +_{\frac{p(1-q)}{1-pq}} z)$$

$$x \oplus y \stackrel{(C)}{=} y \oplus x \qquad x +_p y \stackrel{(C_p)}{=} y +_{1-p} x$$

$$x \oplus x \stackrel{(I)}{=} x \qquad x +_p x \stackrel{(I_p)}{=} x$$

$$(x \oplus y) +_p z \stackrel{(D)}{=} (x +_p z) \oplus (y +_p z)$$

Monad C: non-empty convex subsets of distributions

One proof is more semantic: the strategy is rather standard but the full proof is tough

convexity comes from the following derived law

$$s \oplus t \stackrel{(C)}{=} s \oplus t \oplus s +_p t$$

One proof is more syntactic: based on normal form and a unique base theorem. Hope to be generalised by more abstract categorical machinery

Adding Termination

$$\oplus \quad +_p \quad \star$$

$$(x \oplus y) \oplus z \stackrel{(A)}{=} x \oplus (y \oplus z) \qquad (x +_q y) +_p z \stackrel{(A_p)}{=} x +_{pq} (y +_{\frac{p(1-q)}{1-pq}} z)$$

$$x \oplus y \stackrel{(C)}{=} y \oplus x \qquad x +_p y \stackrel{(C_p)}{=} y +_{1-p} x$$

$$x \oplus x \stackrel{(I)}{=} x \qquad x +_p x \stackrel{(I_p)}{=} x$$

$$(x \oplus y) +_p z \stackrel{(D)}{=} (x +_p z) \oplus (y +_p z)$$

The Algebraic Theory of Pointed Convex Semilattices

$$x \oplus \star \stackrel{(B)}{=} x$$

The Algebraic Theory of Convex Semilattices with Bottom

$$x \oplus \star \stackrel{(T)}{=} \star$$

The Algebraic Theory of Convex Semilattices with Top

These three algebras are those freely generated by the singleton set 1

They give rise to three different semantics: may, must, and may-must

$$\mathbb{M}_{\mathcal{I}} = (\mathcal{I}, \text{min-max}, +_p^{\mathcal{I}}, [0,0])$$

$$\mathcal{I} = \{[x,y] \mid x, y \in [0,1] \text{ and } x \leq y\}$$

$$\text{min-max}([x_1, y_1], [x_2, y_2]) = [\min(x_1, x_2), \max(y_1, y_2)]$$

$$[x_1, y_1] +_p^{\mathcal{I}} [x_2, y_2] = [x_1 +_p x_2,\ y_1 +_p y_2]$$

The Theory of Pointed Convex Semilattices

$$\mathbb{M}\text{ax} = ([0,1], \max, +_p, 0)$$

The Algebraic Theory of Convex Semilattices with bottom

$$\mathbb{M}\text{in} = ([0,1], \min, +_p, 0)$$

The Algebraic Theory of Convex Semilattices with Top

Syntax and Transitions

For the three semantics, we use the same syntax

$$s, t \ ::= \ \star, \ s \oplus t, \ s +_p t, \ x \in X \quad \text{for all } p \in [0,1]$$

and transitions

$$\frac{-}{\star \xrightarrow{a} \star} \qquad \frac{s \xrightarrow{a} s' \quad t \xrightarrow{a} t'}{s \oplus t \xrightarrow{a} s' \oplus t'} \qquad \frac{s \xrightarrow{a} s' \quad t \xrightarrow{a} t'}{s +_p t \xrightarrow{a} s' +_p t'}$$

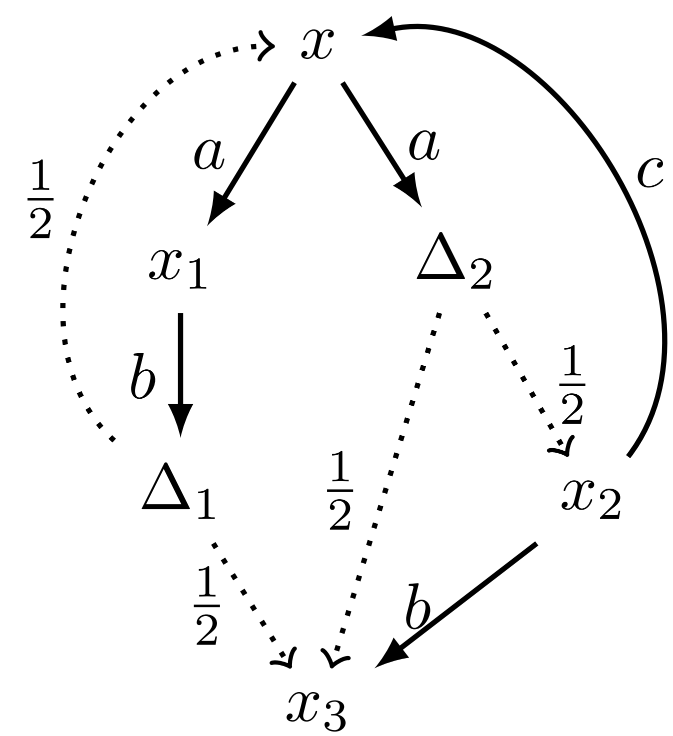
but different output functions...

Example without outputs

$$x \xrightarrow{a} x_1 \oplus (x_3 +_{\frac{1}{2}} x_2)$$

$$x_1 \xrightarrow{b} x +_{\frac{1}{2}} x_3$$

$$x_2 \xrightarrow{b} x_3 \qquad x_2 \xrightarrow{c} x$$



$$x \xrightarrow{b,c} \star$$

$$x_1 \xrightarrow{a,c} \star$$

$$x_2 \xrightarrow{a} \star$$

$$x_3 \xrightarrow{a,b,c} \star$$

$$x \xrightarrow{a} x_1 \oplus (x_3 +_{\frac{1}{2}} x_2) \xrightarrow{b} (x +_{\frac{1}{2}} x_3) \oplus (\star +_{\frac{1}{2}} x_3)$$

Outputs for May

We take as algebra of outputs

$$\mathbb{M}\mathrm{ax} = \quad ([0,1], \max, +_p, 0)$$

that gives rise to the following three rules

$$\frac{-}{\star \downarrow_0} \qquad \frac{s \downarrow_{q_1} \qquad t \downarrow_{q_2}}{s \oplus t \downarrow_{\mathtt{max}(q_1, q_2)}} \qquad \frac{s \downarrow_{q_1} \qquad t \downarrow_{q_2}}{s +_p t \downarrow_{q_1 +_p q_2}}$$

Outputs for Must

We take as algebra of outputs

$$\mathbb{M}\mathrm{in} = ([0,1], \min, +_p, 0)$$

that gives rise to the following three rules

$$\frac{-}{\star \downarrow_0} \qquad \frac{s \downarrow_{q_1} \quad t \downarrow_{q_2}}{s \oplus t \downarrow_{\mathtt{min}(q_1, q_2)}} \qquad \frac{s \downarrow_{q_1} \quad t \downarrow_{q_2}}{s +_p t \downarrow_{q_1 +_p q_2}}$$

Outputs for May-Must

We take as algebra of outputs

$$\mathbb{M}_{\mathcal{I}} = (\mathcal{I}, \text{min-max}, +_p^{\mathcal{I}}, [0,0])$$

that gives rise to the following three rules

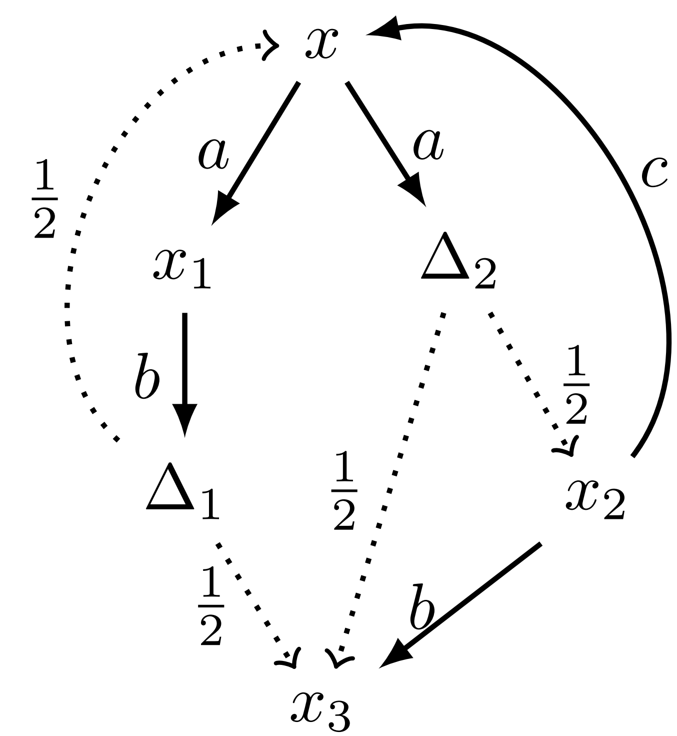
$$\frac{-}{\star \downarrow_{[0,0]}} \qquad \frac{s \downarrow_I \quad t \downarrow_J}{s \oplus t \downarrow_{\texttt{min-max}(I,J)}} \qquad \frac{s \downarrow_I \quad t \downarrow_J}{s +_p t \downarrow_{I +_p^{\mathcal{I}} J}}$$

Example with outputs

$$x \xrightarrow{a} x_1 \oplus (x_3 +_{\frac{1}{2}} x_2)$$

$$x_1 \xrightarrow{b} x +_{\frac{1}{2}} x_3$$

$$x_2 \xrightarrow{b} x_3 \qquad x_2 \xrightarrow{c} x$$



$$x \xrightarrow{b,c} \star$$

$$x_1 \xrightarrow{a,c} \star$$

$$x_2 \xrightarrow{a} \star$$

$$x_3 \xrightarrow{a,b,c} \star$$

All states output 1

$x \downarrow_1$ $\quad x_1 \downarrow_1$ $\quad x_2 \downarrow_1$ $\quad x_3 \downarrow_1$

May $\quad x \downarrow_1 \xrightarrow{a} x_1 \oplus (x_3 +_{\frac{1}{2}} x_2) \downarrow_1 \xrightarrow{b} (x +_{\frac{1}{2}} x_3) \oplus (\star +_{\frac{1}{2}} x_3) \downarrow_1$

Must $\quad x \downarrow_1 \xrightarrow{a} x_1 \oplus (x_3 +_{\frac{1}{2}} x_2) \downarrow_1 \xrightarrow{b} (x +_{\frac{1}{2}} x_3) \oplus (\star +_{\frac{1}{2}} x_3) \downarrow_{\frac{1}{2}}$

Conclusions

Traces carry a convex semilattice
The three trace semantics are convex semilattice homomorphisms
Trace equivalences are congruence w.r.t. convex semilattice operations
Coinduction up-to these operation is sound

Both probabilistic and convex bisimilarity
implies the three trace equivalences

The equivalences are "backward compatible" with standard trace equivalences
for non deterministic and probabilistic systems

The may-equivalence coincides with one in
Bernardo, De Nicola, Loreti TCS 2014


Thank You

Part II

More Semantics for Probability and Nondeterminism via Coalgebra

Probabilistic Nondeterministic LTS

Can be given different semantics:

1. Bisimilarity
2. Convex bisimilarity
3. Distribution bisimilarity
4. Trace semantics

strong bisimilarity

probabilistic/ combined bisimilarity

belief-state bisimilarity

[Bonchi,Silva, S. CONCUR'17]

trace and testing theory

[Bonchi, S., Vignudelli LICS'19]

Behavioural Equivalences

LTS

$X \to (\mathcal{P}X)^A$

Two states are equivalent iff they admit the same traces (words).

trace equivalence

An equivalence relation $R \subseteq X \times X$ is a bisimulation of the LTS $X \to (\mathcal{P}X)^A$ iff whenever $(x, y) \in R$ for all $a \in A$

$$x \xrightarrow{a} x' \quad \Rightarrow \quad \exists y'. y \xrightarrow{a} y' \wedge (x', y') \in R.$$

Bisimilarity, denoted by $\sim$, is the largest bisimulation.

bisimilarity

Behavioural Equivalences

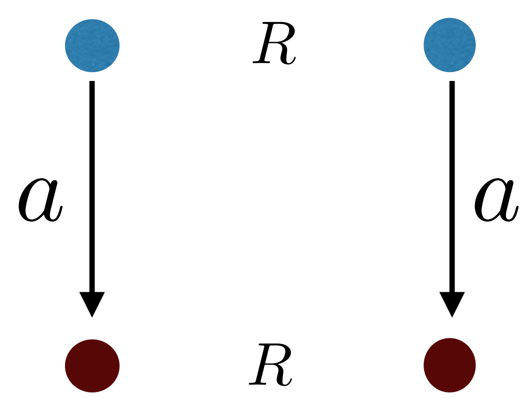
LTS

$X \to (\mathcal{P}X)^A$

Two states are equivalent iff they admit the same traces (words).

trace equivalence

bisimulation



largest bisimulation

bisimilarity

Probabilistic Nondeterministic LTS

Can be given different semantics:

1. Bisimilarity
2. Convex bisimilarity
3. Distribution bisimilarity
4. Trace semantics

strong bisimilarity

probabilistic/ combined bisimilarity

belief-state bisimilarity

[Bonchi,Silva, S. CONCUR'17]

trace and testing theory

[Bonchi, S., Vignudelli LICS'19]

Bisimilarity

An equivalence relation R on the PA $c\colon X \to (\mathcal{P}\mathcal{D}X)^A$ is a bisimulation iff whenever $(s,t) \in R$ for all $a \in A$ and $\mu \in \mathcal{D}X$

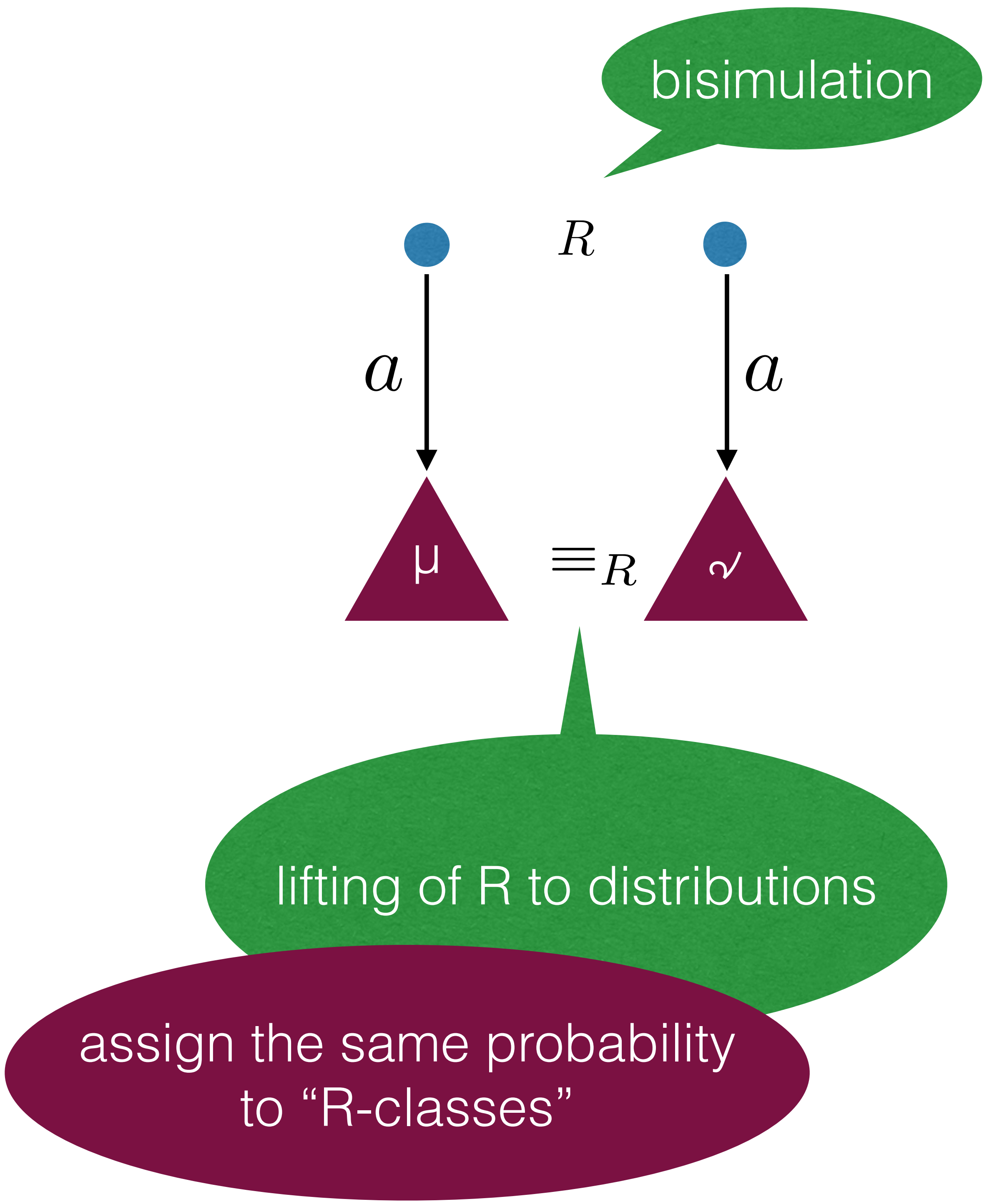
$$s \xrightarrow{a} \mu \Longrightarrow \exists \nu \in \mathcal{D}X.\ t \xrightarrow{a} \nu \wedge \mu \equiv_R \nu$$

where $\mu \equiv_R \nu$ iff $\mu[C] = \nu[C]$ for all R-equivalence classes C, with $\mu[C] = \sum_{x \in C} \mu(x)$.

Bisimilarity on $c\colon X \to (\mathcal{P}\mathcal{D}X)^A$, denoted by $\sim$, is the largest bisimulation.

Bisimilarity

$\sim$ largest bisimulation



Convex bisimilarity

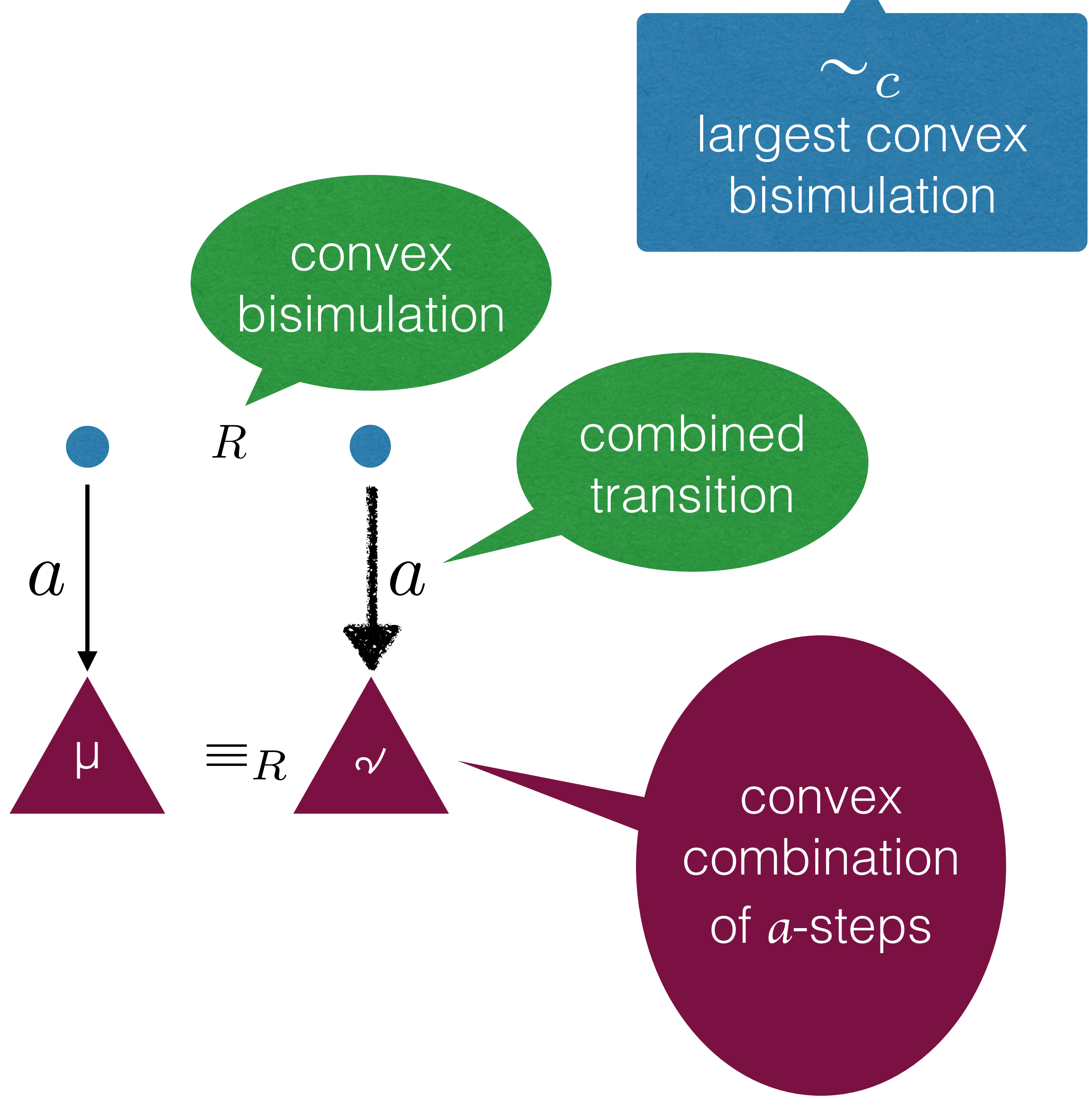
An equivalence relation $R \subseteq X \times X$ is a convex bisimulation of the PA $c\colon X \to (\mathcal{P}\mathcal{D}X)^A$ iff whenever $(x, y) \in R$, for all $a \in A$ and $\mu \in \mathcal{D}X$

convex combination

$$x \xrightarrow{a} \mu \quad \Rightarrow \quad \exists \nu.\, \mu \equiv_R \nu \wedge \nu = \sum_{i=1}^{n} p_i \nu_i \wedge y \xrightarrow{a} \nu_i.$$

Convex bisimilarity on $c\colon X \to (\mathcal{P}\mathcal{D}X)^A$, denoted by $\sim_c$, is the largest bisimulation.

Convex bisimilarity



Distribution bisimilarity

An equivalence relation R on the carrier of the belief-state transformer $c\colon \mathcal{D}X \to (\mathcal{P}\mathcal{D}X)^A$ is a distribution bisimulation iff whenever $(\mu,\nu) \in R$ for all $a \in A$

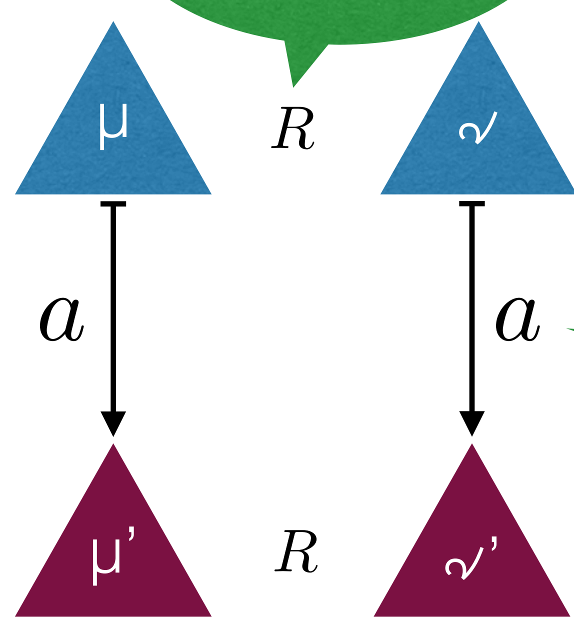
$$\mu \xrightarrow{a} \mu' \implies \exists \nu' \in \mathcal{D}X.\ \nu \xrightarrow{a} \nu' \wedge (\mu',\nu') \in R.$$

Distribution bisimilarity on $c\colon \mathcal{D}X \to (\mathcal{P}\mathcal{D}X)^A$, denoted by $\sim_d$, is the largest distribution bisimulation.

Distribution bisimilarity

$\sim_d$
largest distribution bisimulation

distribution bisimulation



transition in the belief-state transformer

$\sim_d$
is LTS bisimilarity on the belief-state transformer

Coalgebras

Uniform framework for dynamic transition systems, based on category theory.

$$X \xrightarrow{c} FX$$

generic notion of behavioural equivalence

$\approx$

states

object in the base category ***C***

behaviour type

functor on the base category ***C***

form a category too

$\mathbf{CoAlg_C}(F)$

The category of F-coalgebras

$\mathbf{CoAlg_C}(F)$

behaviour-preserving maps

Objects = coalgebras

$X \xrightarrow{c} FX$

Arrows = coalgebra homomorphisms

$h\colon X \to Y$

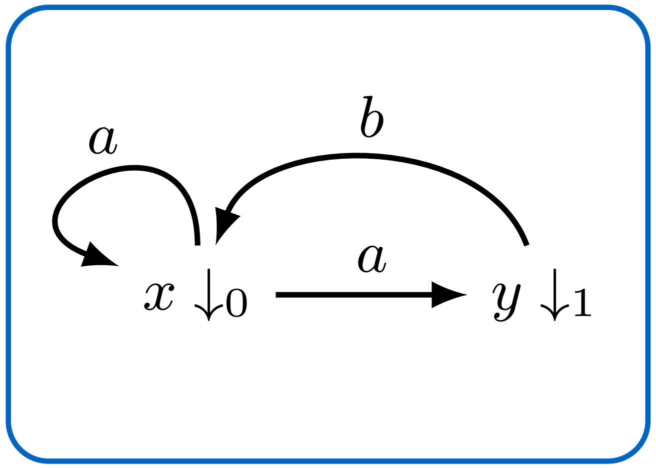
$$\begin{tikzcd} X \arrow[r, "h"] \arrow[d, "c_X"'] & Y \arrow[d, "c_Y"] \\ FX \arrow[r, "Fh"'] & FY \end{tikzcd}$$

Two states $x, y \in X$ are behaviourally equivalent, notation $x \approx y$ iff there exists a coalgebra homomorphism $h\colon X \to Y$ from $c\colon X \to FX$ to some coalgebra $d\colon Y \to FY$ such that $h(x) = h(y)$.

Examples

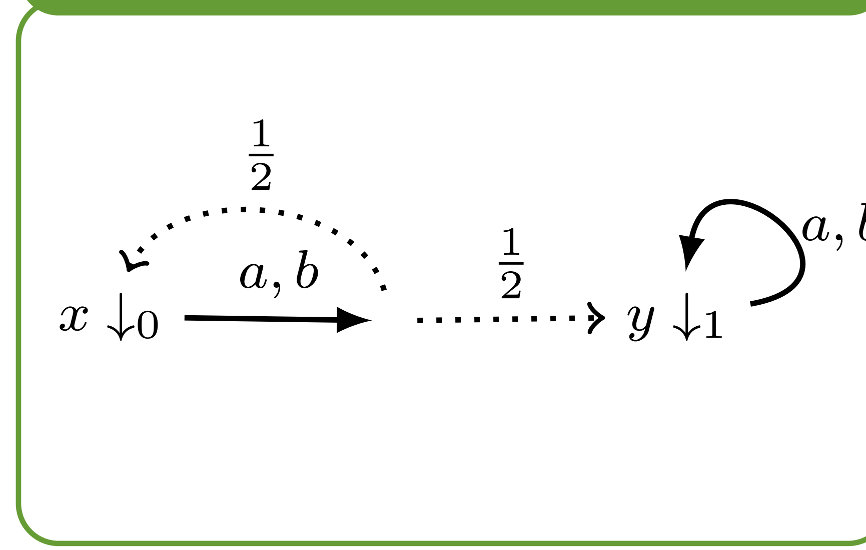
NFA

$X \to 2 \times (\mathcal{P}X)^A$



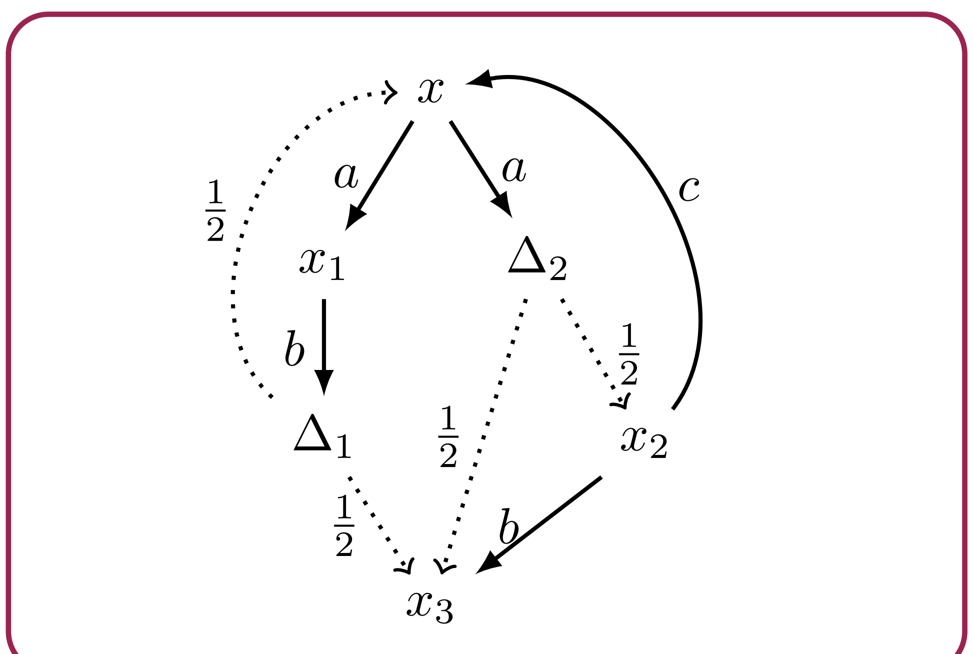
Rabin PA

$\mathcal{D}X \to [0,1] \times (\mathcal{D}X)^A$



PNLTS

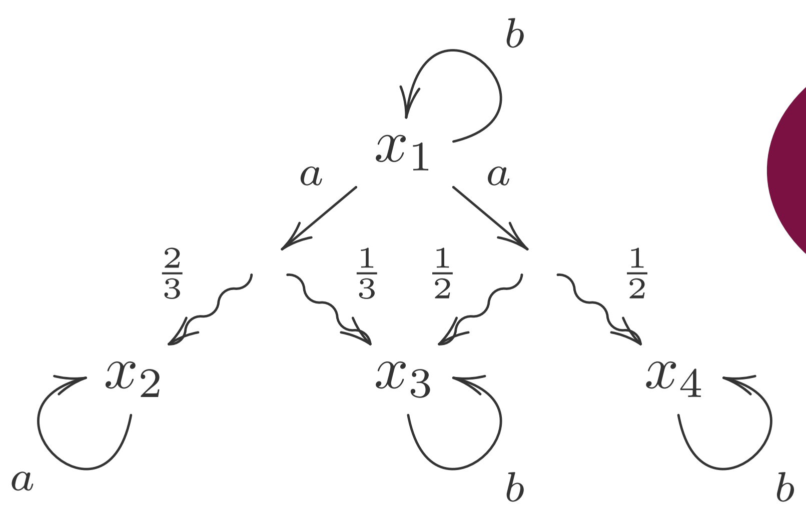
$X \to (\mathcal{P}\mathcal{D}X)^A$



all on
Sets

PA coalgebraically

$X \to (\mathcal{P}\mathcal{D}X)^A$



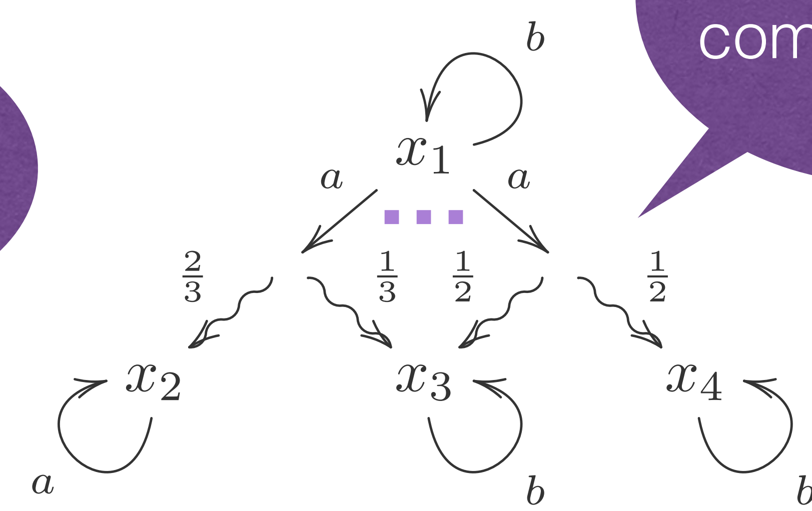
on **Sets**

$\sim \; = \; \approx$

$\sim_c \; = \; \approx$

$X \to (\mathcal{C}X)^A$

and all convex combinations



$X \to (\mathcal{P}_c X+1)^A$

$$\begin{tikzcd} & \frac{1}{3}x_1 + \frac{2}{3}x_2 \arrow[dl, mapsto, "a"'] \arrow[dr, mapsto, "a"] & & \dots \\ \frac{8}{9}x_2 + \frac{1}{9}x_3 & \dots & \frac{2}{3}x_2 + \frac{1}{6}x_3 + \frac{1}{6}x_4 & \end{tikzcd}$$

on convex algebras

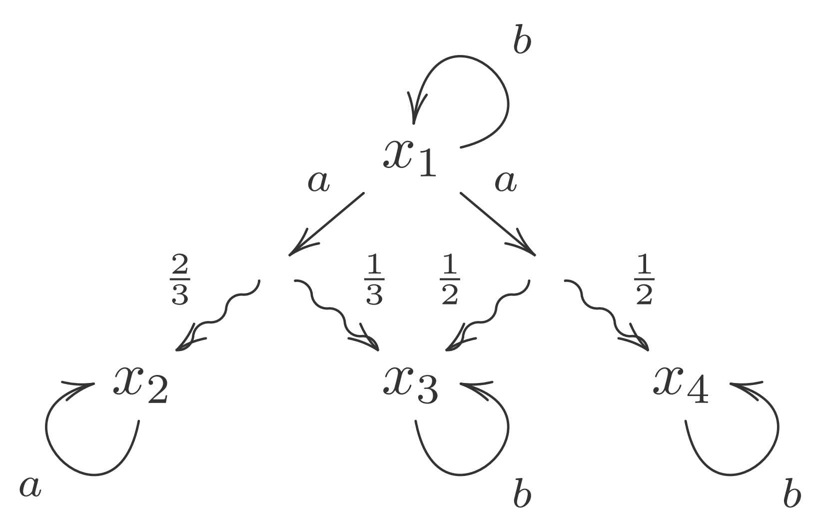
$\sim_d \; = \; \approx$

$\mathcal{EM}(\mathcal{D})$

Determinisations

PA

$X \to (\mathcal{PD}X)^A$



belief-state transformer

LTS on a convex algebra

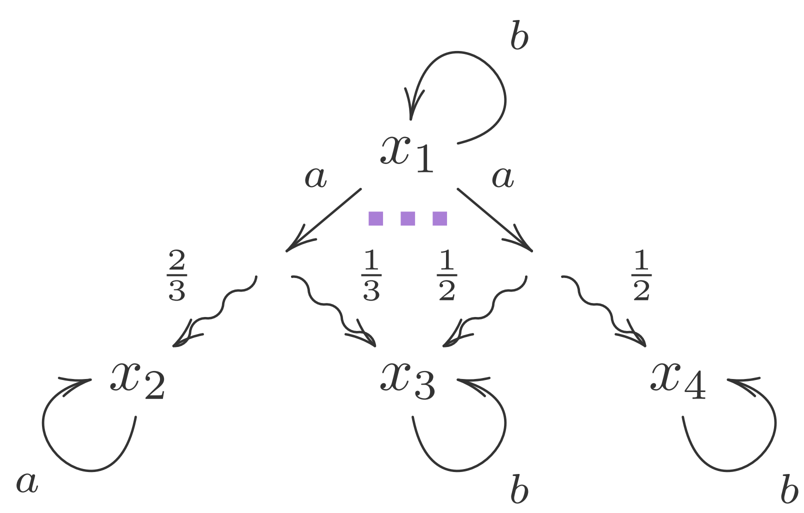
$$\frac{1}{3}x_1 + \frac{2}{3}x_2 \qquad \cdots$$

$$\frac{2}{3}x_2 + \frac{1}{6}x_3 + \frac{1}{6}x_4 \xleftarrow{\;a\;} \frac{1}{3}x_1 + \frac{2}{3}x_2 \xrightarrow{\;a\;} \frac{8}{9}x_2 + \frac{1}{9}x_3$$

$$\cdots$$

Determinisations

$X \to (\mathcal{C}X)^A$



$$x_1 \xrightarrow{a} \left(\tfrac{2}{3}x_2 + \tfrac{1}{3}x_3\right) \oplus \left(\tfrac{1}{2}x_3 + \tfrac{1}{2}x_4\right)$$

LTS on a convex semilattice

Theory of traces for probability, nondeterminism, and termination
…

Thank You !


Thank You,
Helmut !