Proving Behavioural Apartness

DutchCATS Leiden 2024

Ruben Turkenburg[1] Harsh Beohar[2]
Clemens Kupke[3] Jurriaan Rot[1]

[1]Institute for Computing and Information Sciences (iCIS), Radboud University, NL

[2]Department of Computer Science, University of Sheffield, UK

[3]Department of Computer & Information Sciences, Strathclyde University, UK

2024-06-05

Overview

- Notions of equivalence on state-based systems
- Modelled as *coalgebras*: $\gamma : X \to BX$ for $B : \mathscr{C} \to \mathscr{C}$
  - Equivalences parametric in the functor
  - Bisimilarity, behavioural equivalence

Overview

- Notions of equivalence on state-based systems
- Modelled as *coalgebras*: $\gamma : X \to BX$ for $B : \mathscr{C} \to \mathscr{C}$
  - Equivalences parametric in the functor
  - Bisimilarity, behavioural equivalence
- Notions of inequivalence/distinguishability
  - Apartness, complement of equivalence notions
  - Finite proofs?
  - Corresponding distinguishing (modal) formulas

Outline

- Some coalgebra
- What is apartness?
- Comparing bisimilarity and apartness on transition systems
- Definitions via (canonical) relation lifting
- The problem with probabilistic systems
- A nicer proof system
- Future work

Coalgebra

- Object $X \in \mathscr{C}$ and arrow $\gamma : X \to BX$
- Functor $B : \mathscr{C} \to \mathscr{C}$ gives shape of successors

Coalgebra

- Object $X \in \mathscr{C}$ and arrow $\gamma : X \to BX$
- Functor $B : \mathscr{C} \to \mathscr{C}$ gives shape of successors
- Examples:

(Concrete) System	Base category	Coalgebra structure map
LTS	Set	$X \to \mathscr{P}(X)^A$
Markov Chain	Set/Meas	$X \to \mathscr{D}X$
DFA	Set/JSL/$\mathscr{E}\mathscr{M}(\mathscr{P})$	$X \to 2 \times X^A$
Mealy Machine	Set	$X \to \mathscr{P}(B \times X)^A$
MDP	Set/Meas	$X \to \mathscr{D}_s(X)^A$

- Often of interest: functor built from some grammar e.g.

$$B ::= A \mid \mathsf{Id} \mid B_1 \times B_2 \mid B_1 + B_2 \mid B^A \mid \mathscr{P}B \mid \mathscr{D}_s B$$

(In)Equivalences

- Equivalence/Indistinguishability: Defined coinductively
  - Bisimilarity: largest relation “closed under transitions”
  - (Coalgebraic) Behavioural equivalence: identification under coalgebra homomorphisms
- Inequivalence/Distinguishability: dual to equivalences (inductive)
  - Cobisimilarity
  - Behavioural apartness

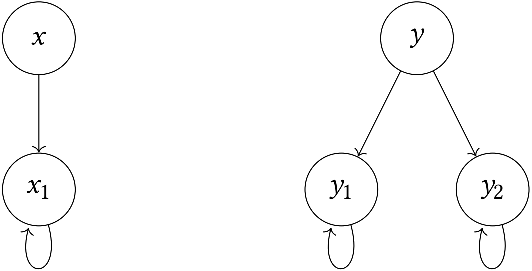
Apartness

- Goes back to Brouwer's intuitionism
- When are two real numbers equal?
- Instead:

$$r_1 \# r_2 := \exists q \in \mathbb{Q}. r_1 < q < r_2 \vee r_2 < q < r_1$$

- We can "just" give a q

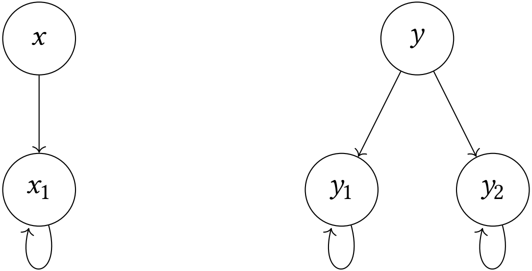
Bisimilarity on Transition Systems



$$X = \{x, y, x_1, y_1, y_2\}, \gamma : X \to \mathscr{P}_f(X) \text{ e.g. } \gamma(y) = \{y_1, y_2\}$$

$$\begin{aligned} s_1 \,\underline{\leftrightarrow}\, t_1 \iff & \forall s_1 \to s_2 .\, \exists t_1 \to t_2 .\, s_2 \,\underline{\leftrightarrow}\, t_2 \wedge \\ & \forall t_1 \to t_2 .\, \exists s_1 \to s_2 .\, s_2 \,\underline{\leftrightarrow}\, t_2 \end{aligned}$$

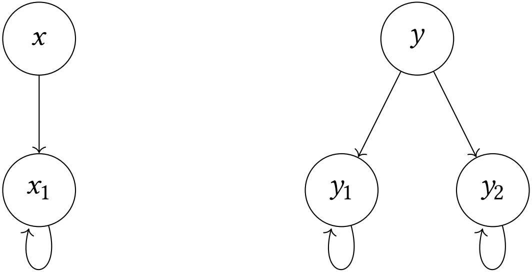
Bisimilarity on Transition Systems



$$X = \{x, y, x_1, y_1, y_2\}, \gamma : X \to \mathscr{P}_f(X) \text{ e.g. } \gamma(y) = \{y_1, y_2\}$$

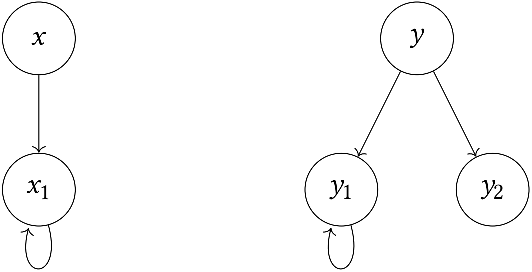
$$\begin{aligned} s_1 \mathrel{\underline{\leftrightarrow}} t_1 \iff & \forall s_1 \to s_2 .\, \exists t_1 \to t_2 .\, s_2 \mathrel{\underline{\leftrightarrow}} t_2 \wedge \\ & \forall t_1 \to t_2 .\, \exists s_1 \to s_2 .\, s_2 \mathrel{\underline{\leftrightarrow}} t_2 \end{aligned}$$

Proving Bisimilarity?



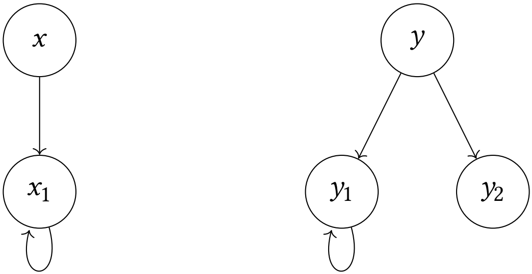
$$\dfrac{\dfrac{\dfrac{\vdots}{x_1 \underline{\leftrightarrow} y_2}}{x_1 \underline{\leftrightarrow} y_2} \qquad \dfrac{\dfrac{\vdots}{x_1 \underline{\leftrightarrow} y_1}}{x_1 \underline{\leftrightarrow} y_1}}{x \underline{\leftrightarrow} y}$$

Apartness on Transition Systems



$$
\begin{aligned}
s_1 \;\#\; t_1 \iff & \exists s_1 \to s_2.\, \forall t_1 \to t_2.\, s_2 \;\#\; t_2 \;\vee \\
& \exists t_1 \to t_2.\, \forall s_1 \to t_2.\, s_2 \;\#\; t_2
\end{aligned}
$$

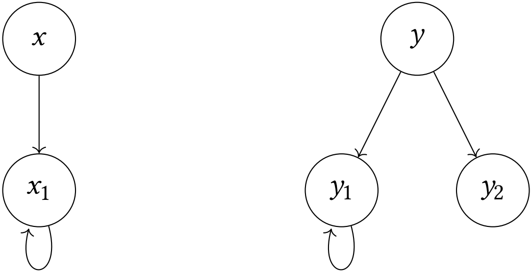
Apartness on Transition Systems



$$\begin{aligned} s_1 \# t_1 \iff & \exists s_1 \to s_2 .\, \forall t_1 \to t_2 .\, s_2 \# t_2 \lor \\ & \exists t_1 \to t_2 .\, \forall s_1 \to t_2 .\, s_2 \# t_2 \end{aligned}$$

- LFP: Inductive Proofs

Proving Apartness?



$$\cfrac{\cfrac{\forall y_2 \to y' .\, x_1 \mathrel{\#} y'}{x_1 \mathrel{\#} y_2}}{x \mathrel{\#} y}$$

Coalgebraically: Relation Lifting

- "Closure under transitions" requires application of B to relations
- Canonical relation lifting gives $\mathrm{Rel}(B)_X : \mathrm{Rel}_X \to \mathrm{Rel}_{BX}$

Coalgebraically: Relation Lifting

- "Closure under transitions" requires application of B to relations
- Canonical relation lifting gives $\mathrm{Rel}(B)_X : \mathrm{Rel}_X \to \mathrm{Rel}_{BX}$
- Example: let $R \subseteq X \times X$ and $U, V \in \mathscr{P}(X)$, then

$$\begin{aligned} U \ \mathrm{Rel}(\mathscr{P})(R)\ V \iff & \forall u \in U.\, \exists v \in V.\, (u,v) \in R \,\wedge \\ & \forall v \in V.\, \exists u \in U.\, (u,v) \in R \end{aligned}$$

- In general: requires (orthogonal) factorisation system on (finitely complete) $\mathscr{C}$

$$\begin{tikzcd} BR \arrow[r, "Br"] \arrow[dr, two heads] & B(X \times X) \arrow[r, "\langle B\pi_1, B\pi_2 \rangle"] & BX \times BX \\ & \mathrm{Rel}(B)(R) \arrow[ur, tail] & \end{tikzcd}$$

Coalgebraic Bisimilarity

- $R \subseteq X \times X$ is a bisimulation if

$$\frac{x \; R \; y}{\gamma(x) \; \mathrm{Rel}(B)(R) \; \gamma(y)}$$

- Bisimilarity: largest such relation

Coalgebraic Bisimilarity

- $R \subseteq X \times X$ is a bisimulation if

$$\frac{x \; R \; y}{\gamma(x) \; \mathsf{Rel}(B)(R) \; \gamma(y)}$$

- Bisimilarity: largest such relation
- Example: for $\gamma : X \to \mathscr{P}(X)$

$$\begin{aligned} \gamma(x) \; \mathsf{Rel}(\mathscr{P})(R) \; \gamma(y) \iff & \forall x' \in \gamma(x).\, \exists y' \in \gamma(y).\, (x', y') \in R \wedge \\ & \forall y' \in \gamma(y).\, \exists x' \in \gamma(x).\, (x', y') \in R \end{aligned}$$

Dually

- R is a cobisimulation if

$$\frac{\gamma(x)\ \overline{\mathrm{Rel}(B)(\overline{R})}\ \gamma(y)}{x\ R\ y}$$

- Cobisimilarity $\underline{\#}$ is the smallest relation closed under this rule
- Inductive $\implies$ proof system

Concretely

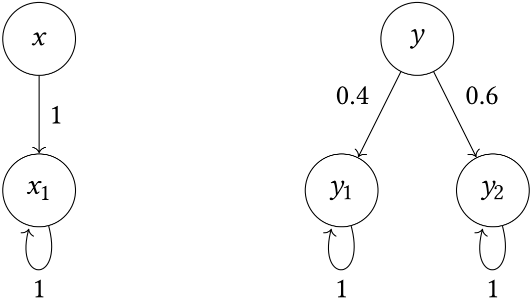
Instantiating to simple transition systems gives us exactly:

$$\frac{s_1 \to s_2 \qquad \forall t_1 \to t_2 .\, s_2 \mathrel{\underline{\#}} t_2}{s_1 \mathrel{\underline{\#}} t_1} \qquad \frac{t_1 \to t_2 \qquad \forall s_1 \to s_2 .\, s_2 \mathrel{\underline{\#}} t_2}{s_1 \mathrel{\underline{\#}} t_1}$$

Geuvers & Jacobs 2021: Proof systems for coalgebras for Kripke polynomial functors

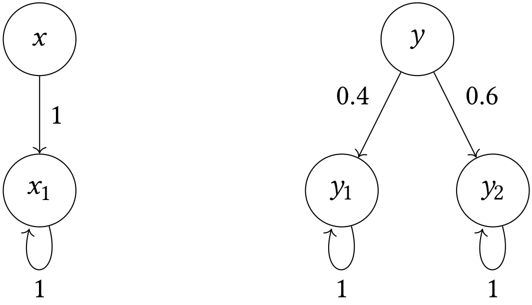
$$B \;::=\; A \mid \mathsf{Id} \mid B_1 \times B_2 \mid B_1 + B_2 \mid B^A \mid \mathscr{P}B$$

Probabilities?



$$\mu_x = 1\,|x_1\rangle \qquad \mu_y = 0.4\,|y_1\rangle + 0.6\,|y_2\rangle$$

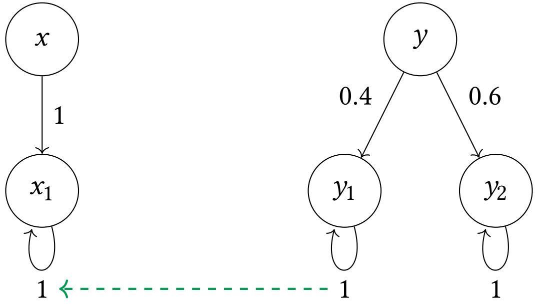
Probabilities?



$$x \underline{\leftrightarrow} y \iff \exists \text{ coupling } \omega \in \mathscr{D}(\underline{\leftrightarrow}).\, \mathscr{D}\pi_1(\omega) = \mu_x \wedge \mathscr{D}\pi_2(\omega) = \mu_y$$

Relation Lifting: (Bartels, Sokolova, de Vink 2003/4), (Sokolova 2011)

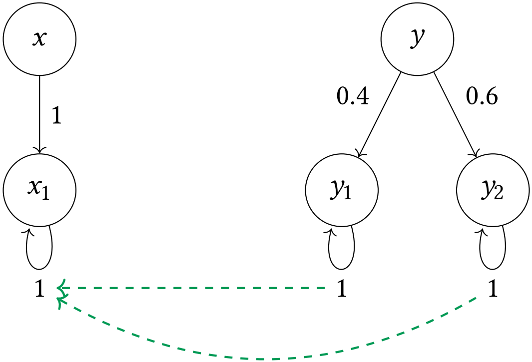
Probabilities?



$$x \mathrel{\underline{\leftrightarrow}} y \iff \exists \text{ coupling } \omega \in \mathscr{D}(\underline{\leftrightarrow}).\ \mathscr{D}\pi_1(\omega) = \mu_x \wedge \mathscr{D}\pi_2(\omega) = \mu_y$$

Relation Lifting: (Bartels, Sokolova, de Vink 2003/4), (Sokolova 2011)

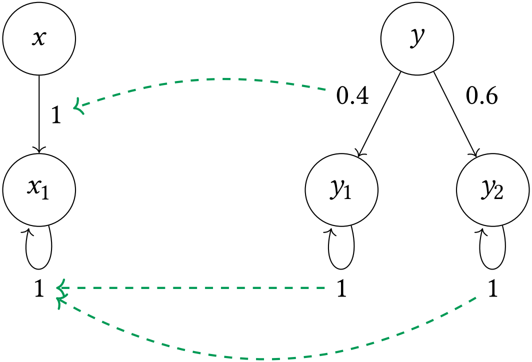
Probabilities?



$$x \mathrel{\underline{\leftrightarrow}} y \iff \exists \text{ coupling } \omega \in \mathscr{D}(\underline{\leftrightarrow}).\ \mathscr{D}\pi_1(\omega) = \mu_x \wedge \mathscr{D}\pi_2(\omega) = \mu_y$$

Relation Lifting: (Bartels, Sokolova, de Vink 2003/4), (Sokolova 2011)

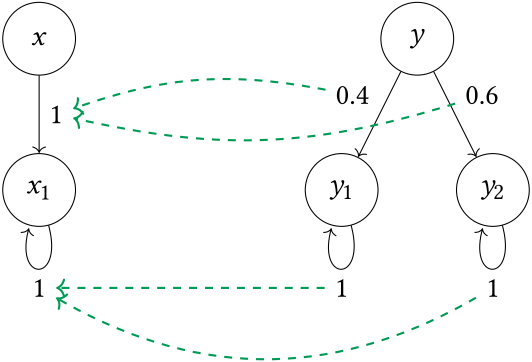
Probabilities?



$$x \underline{\leftrightarrow} y \iff \exists \text{ coupling } \omega \in \mathcal{D}(\underline{\leftrightarrow}).\, \mathcal{D}\pi_1(\omega) = \mu_x \wedge \mathcal{D}\pi_2(\omega) = \mu_y$$

Relation Lifting: (Bartels, Sokolova, de Vink 2003/4), (Sokolova 2011)

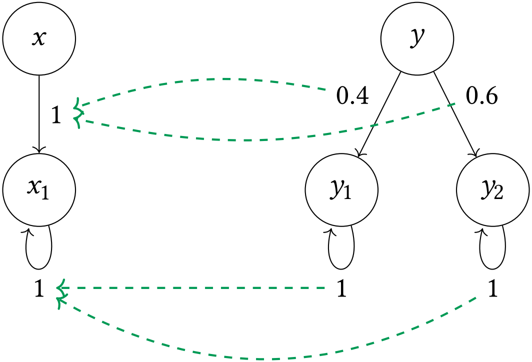
Probabilities?



$$x \underline{\leftrightarrow} y \iff \exists \text{ coupling } \omega \in \mathcal{D}(\underline{\leftrightarrow}).\, \mathcal{D}\pi_1(\omega) = \mu_x \wedge \mathcal{D}\pi_2(\omega) = \mu_y$$

Relation Lifting: (Bartels, Sokolova, de Vink 2003/4), (Sokolova 2011)

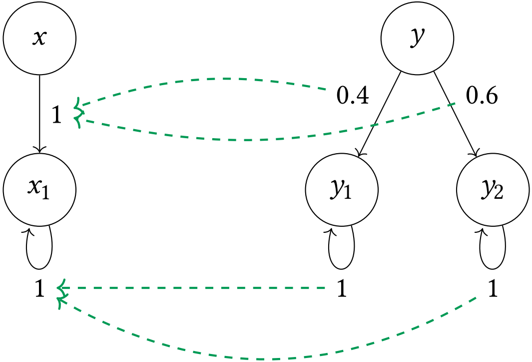
Probabilities?



$x \mathrel{\underline{\leftrightarrow}} y \iff \exists$ coupling $\omega \in \mathcal{D}(\underline{\leftrightarrow}).\ \mathcal{D}\pi_1(\omega) = \mu_x \wedge \mathcal{D}\pi_2(\omega) = \mu_y$

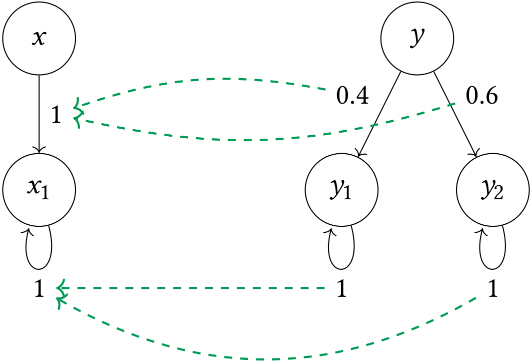
Relation Lifting: (Bartels, Sokolova, de Vink 2003/4), (Sokolova 2011)

Probabilities?



$x \# y \iff \forall$ couplings $\omega \in \mathcal{D}(\overline{\#}).\ \mathcal{D}\pi_1(\omega) \neq \mu_x \vee \mathcal{D}\pi_2(\omega) \neq \mu_y$

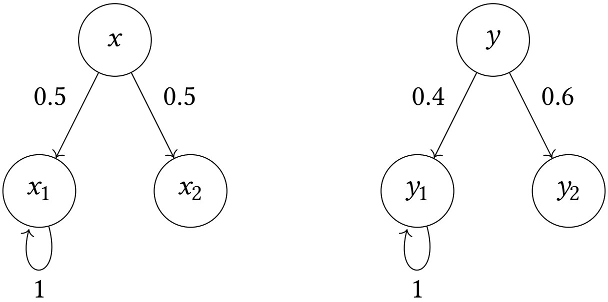
Probabilities?



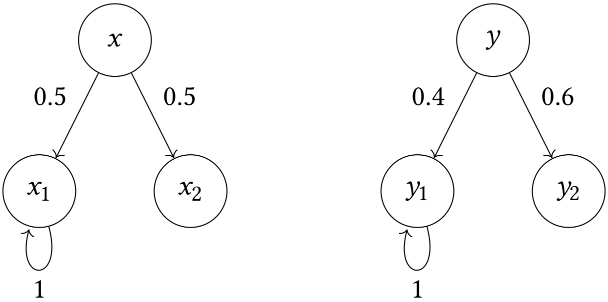
$$x \underline{\leftrightarrow} y \iff \forall z \in X.\ \sum_{z' : z \underline{\leftrightarrow} z'} \mu_x(z') = \sum_{z' : z \underline{\leftrightarrow} z'} \mu_y(z')$$

(Larsen and Skou, 1989/1991)

Apartness

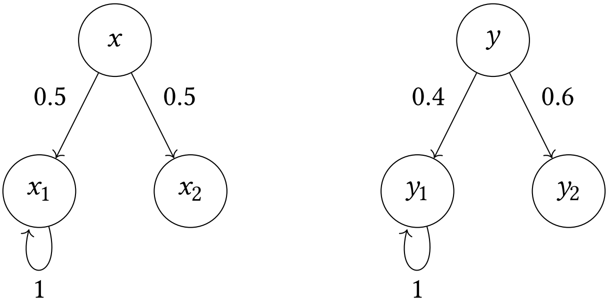


Apartness



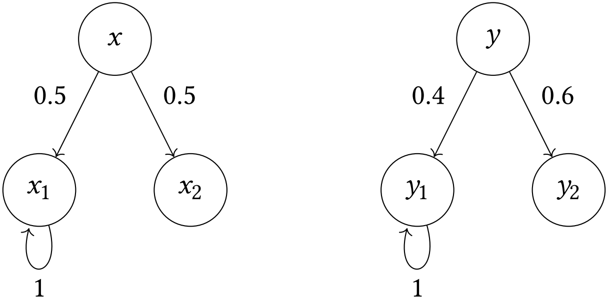
$$x \;\#\; y \iff \exists z \in X.\ \sum_{z' : \neg(z \# z')} \mu_x(z') \neq \sum_{z' : \neg(z \# z')} \mu_y(z')$$

Apartness



$$x \# y \iff \exists z \in X. \sum_{z' : \neg(z \# z')} \mu_x(z') \neq \sum_{z' : \neg(z \# z')} \mu_y(z')$$

Apartness



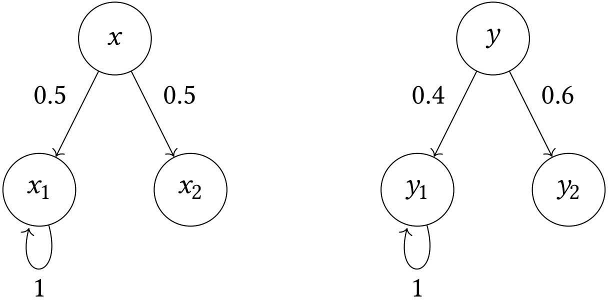
$$x \# y \iff \exists z \in X. \sum_{z' : \neg(z \# z')} \mu_x(z') \neq \sum_{z' : \neg(z \# z')} \mu_y(z')$$

- Can this be determined “step-wise”?
- Do we need the whole apartness/bisimilarity relation?

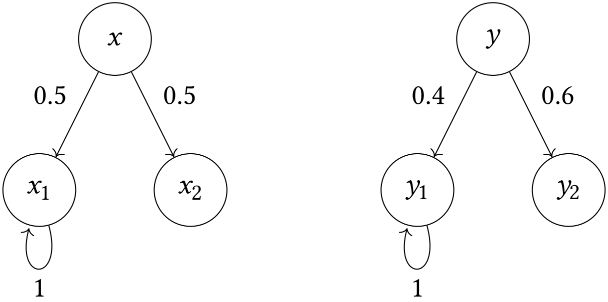
Proof Rule

$$\frac{\forall (x', y') \in R.\, x' \mathrel{\#} y' \qquad \exists z \in \mathrm{supp}(\mu_x) \cup \mathrm{supp}(\mu_y).\, \mu_x[z]_{\overline{R}} \neq \mu_y[z]_{\overline{R}}}{x \mathrel{\#} y}$$

Finite Proof



Finite Proof



$$\frac{x_1 \# x_2 \quad y_1 \# y_2 \quad x_2 \# y_1 \quad x_1 \# y_2 \qquad \mu_x[x_1]_{\overline{R}} = 0.5 \neq 0.4 = \mu_y[x_1]_{\overline{R}}}{x \# y}$$

Some generalisations

Distributions	Generally
Supports	States “reachable in one step”
$\mu_x[-]_{\overline{R}}$	$Bq_{\overline{R}}(\gamma(x))$

Reachability

Given $S \subseteq X$, a *one-step covering* of S is a set $z\colon\ Z \subseteq X$ such that transitions from S only reach states in Z

$$\begin{tikzcd} S \arrow[r, hook, "s"] \arrow[dr, "\exists g"'] & X \arrow[r, "\gamma"] & BX \\ & BZ \arrow[ur, "Bz"'] & \end{tikzcd}$$

Generalisation of *base of a functor* (Blok 2012)

Summing over equivalence classes

$$Bq_{\overline{R}}(\gamma(x)) \neq Bq_{\overline{R}}(\gamma(y))$$

- $q : X \to X/e(\overline{R})$ maps states to equivalence classes
- "Lifting relation to successors"

New Rule

$$\frac{\forall (x', y') \in R.\, x' \mathrel{\#} y' \qquad Bq_{\overline{R}}(\gamma(x)) \neq Bq_{\overline{R}}(\gamma(y))}{x \mathrel{\#} y}$$

- Comes from rule defining precongruences (Aczel & Mendler 1989)

$$\frac{x \mathrel{R} y}{Bq_R(\gamma(x)) = Bq_R(\gamma(y))}$$

- In Set: largest such (equivalence) relation coincides with *behavioural equivalence* (Aczel & Mendler, Gumm 1999):

$$x \equiv y \iff \exists f, g : (X, \gamma) \to (Z, \zeta).\ f(x) = g(y)$$

Soundness & Completeness

- Soundness follows essentially from monotonicity
- Completeness holds for finitary functors
- Relate depth of proof tree to images in *final sequence*

Final Sequence

Let $B : \mathsf{Set} \to \mathsf{Set}$

$$1 \xleftarrow{!} B1 \xleftarrow{B!} B^2 1 \longleftarrow \cdots$$

Functor $\mathsf{Ord}^{\mathrm{op}} \to \mathsf{Set}$. (cf. Kleene fixed-point theorem, Cousot & Cousout 1979)

Given $\gamma : X \to BX$:

$$\begin{aligned} \gamma_0 &= ! : X \to 1 \\ \gamma_{i+1} &= B\gamma_i \circ \gamma : X \to B^i 1 \to B^{i+1} 1 \\ \gamma_\alpha &= \lim_{\beta < \alpha} \gamma_\beta \end{aligned}$$

n-step behavioural equivalence/apartness:

$$\gamma_n(x) = \gamma_n(y)$$

Convergence and Completeness

Convergence and Injectivity

- Worrell (2005): Final sequence for finitary Set functors converges at $\omega 2$ ($B(B^{\omega 2}1) \cong B^{\omega 2}1$)
- Maps $B_{\alpha,\beta} : B^{\alpha}1 \to B^{\beta}1$ for $\omega \leq \beta \leq \alpha \leq \omega 2$ are injective

- Inductively show that for $n < \omega$ if $\gamma_n(x) \neq \gamma_n(y)$ then we have proof tree of depth n with $x \# y$ at root
- If $\gamma_\omega(x) \neq \gamma_\omega(y)$ then there is some $i < \omega$ for which $\gamma_i(x) \neq \gamma_i(y)$
- For $\gamma_{\omega+i}(x) \neq \gamma_{\omega+i}(y)$, injectivity of $B_{\omega+i,\omega}$ means $\gamma_\omega(x) \neq \gamma_\omega(y)$

Extending to more systems

- How to obtain proof system for a new type of system?

$$\frac{\forall (x', y') \in R.\, x' \mathrel{\#} y' \qquad Bq_{\overline{R}}(\gamma(x)) \neq Bq_{\overline{R}}(\gamma(y))}{x \mathrel{\#} y}$$

Example: MDPs ($\gamma : X \to \mathcal{D}_s(X)^A$)

$$\frac{\forall (x', y') \in R.\, x' \mathrel{\#} y' \qquad \exists a \in A.\, \exists z \in X.\, \mu_x^a[z]_{\overline{R}} \neq \mu_y^a[z]_{\overline{R}}}{x \mathrel{\#} y}$$

$$B ::= A \mid \mathsf{Id} \mid B_1 \times B_2 \mid B_1 + B_2 \mid B^A \mid \mathcal{P}_f B \mid \mathcal{D}_s B$$

More examples

Mealy Machines, Probabilistic Automata, POMDPs, etc.

Conclusion

- Inequivalence: Apartness rather than Bisimilarity
- Can be proved in finite steps
  - Using relation lifting
  - Via behavioural equivalence: also probabilistic systems
- Generalisations
- Restricting to "reachable" states
- Inductive characterisation of "apartness" on successors
- Proofs of soundness and completeness (for finitary behaviour functors)

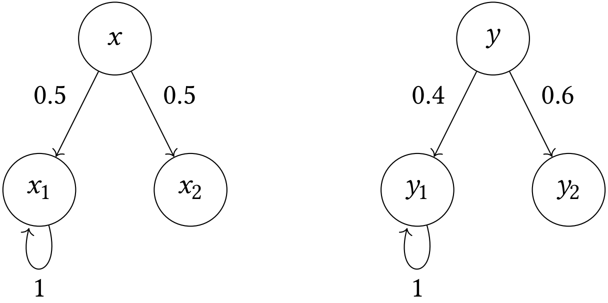
Future Work

- Connection to logics?
- Apartness $\leftrightarrow$ Distinguishing Formulas
- For MDPs: construct distinguishing formula given by

$$\varphi ::= \top \mid \varphi \wedge \varphi \mid \langle a \rangle_q \varphi$$

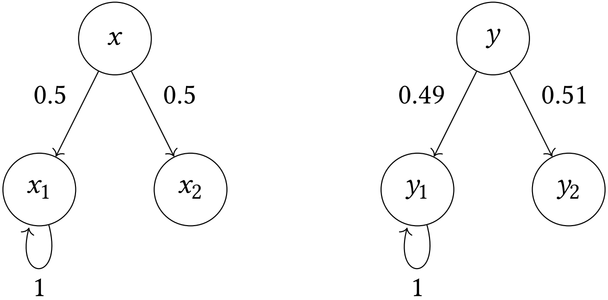
- Abstractly? Projection from proof tree to distinguishing formula(s)

Future Work



How different are x and y, really?

Future Work



How different are x and y, really?

Quantitative Apartness

- Dualising *codensity bisimilarity*

$$\frac{\forall (x', y') \in R.\, x' \#_c y' \qquad (\gamma(x), \gamma(y)) \in \bigcup_{\substack{\lambda \in \Lambda \\ h : R \supseteq h^* \underline{\Omega}}} (\tau_\lambda \circ Bh)^* \underline{\Omega}}{x \#_c y}$$

- Give some λ and h!
- No negative occurrences of $\#_c$ or R!