Proving Behavioural Apartness

CMCS 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

2024-04-07

Overview

- Notions of equivalence
  - Bisimilarity (relation lifting), behavioural equivalence

Overview

- Notions of equivalence
  - Bisimilarity (relation lifting), behavioural equivalence
- Notions of inequivalence/distinguishability
  - Apartness, complement of equivalence notions
  - Finite proofs? Corresponding distinguishing (modal) formulas
  - (Opposite) Relation lifting (Geuvers and Jacobs: Relating Apartness and Bisimulation): not for distributions
  - Complement of Behavioural Equivalence: Behavioural Apartness ✓

Outline

- What is apartness?
- Comparing bisimilarity and apartness on transition systems
- The problem with probabilistic systems
- A nicer proof system
- Future work

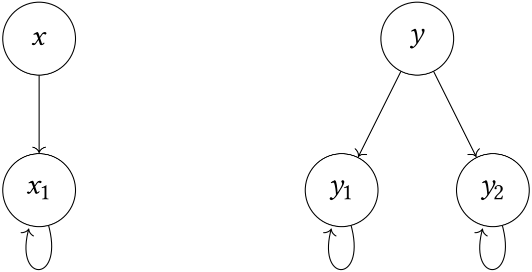
Apartness

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

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

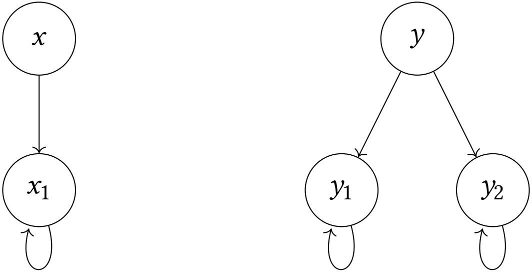
- We can "just" give a q

Bisimilarity on Transition Systems



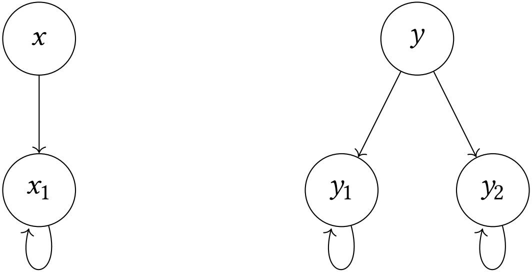
$$
\begin{aligned}
s_1 \mathrel{\underline{\leftrightarrow}} t_1 \iff & \forall s_1 \to s_2 .\, \exists t_1 \to t_2 .\, s_2 \mathrel{\underline{\leftrightarrow}} t_2 \wedge \\
& \forall t_1 \to t_2 .\, \exists s_1 \to s_2 .\, s_2 \mathrel{\underline{\leftrightarrow}} t_2
\end{aligned}
$$

Bisimilarity on Transition Systems



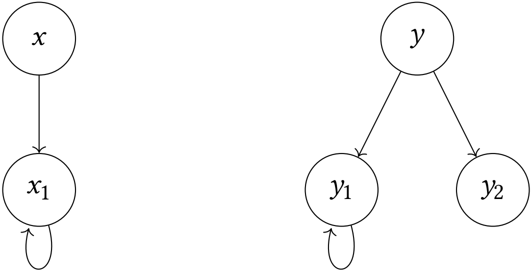
$$s_1 \mathrel{\underline{\leftrightarrow}} t_1 \iff \forall s_1 \to s_2 .\, \exists t_1 \to t_2 .\, s_2 \mathrel{\underline{\leftrightarrow}} t_2 \wedge$$
$$\forall t_1 \to t_2 .\, \exists s_1 \to s_2 .\, s_2 \mathrel{\underline{\leftrightarrow}} t_2$$

Proving Bisimilarity?



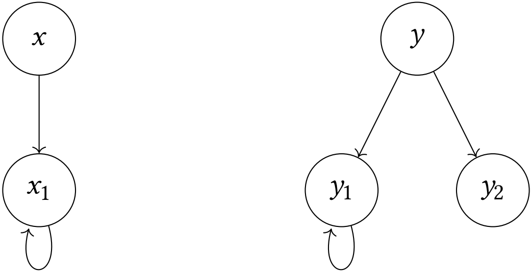
$$\dfrac{\dfrac{\dfrac{\vdots}{x_1 \underline{\leftrightarrow} y_2}}{x_1 \underline{\leftrightarrow} y_2} \qquad \dfrac{\dfrac{\vdots}{x_1 \underline{\leftrightarrow} y_1}}{x_1 \underline{\leftrightarrow} y_1}}{x \underline{\leftrightarrow} y}$$

Apartness on Transition Systems



$$s_1 \# t_1 \iff \exists s_1 \to s_2 .\, \forall t_1 \to t_2 .\, s_2 \# t_2 \lor$$
$$\exists t_1 \to t_2 .\, \forall s_1 \to t_2 .\, s_2 \# t_2$$

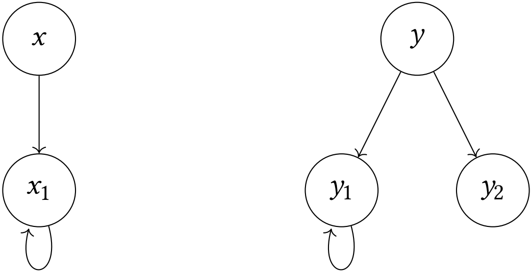
Apartness on Transition Systems



$$s_1 \;\#\; t_1 \iff \exists s_1 \to s_2 .\, \forall t_1 \to t_2 .\, s_2 \;\#\; t_2 \;\vee$$
$$\exists t_1 \to t_2 .\, \forall s_1 \to t_2 .\, s_2 \;\#\; t_2$$

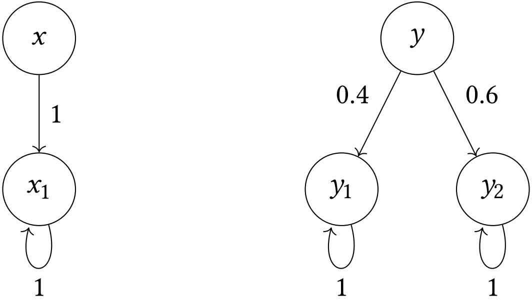
- LFP: Inductive Proofs

Proving Apartness?



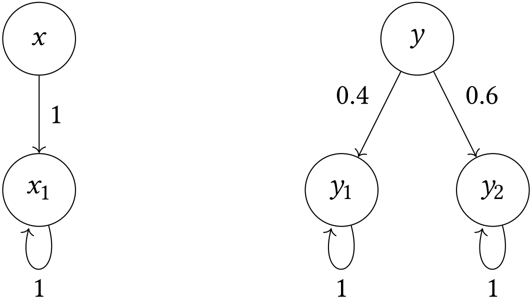
$$\frac{\dfrac{\forall y_2 \to y' .\, x_1 \# y'}{x_1 \# y_2}}{x \# y}$$

Probabilities?



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

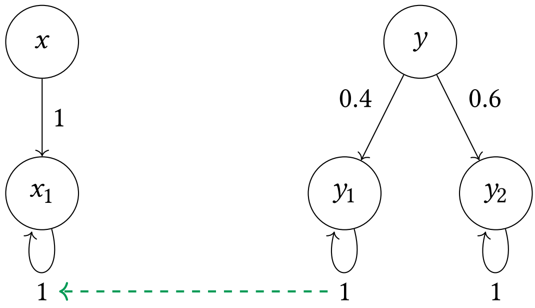
Probabilities?



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

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

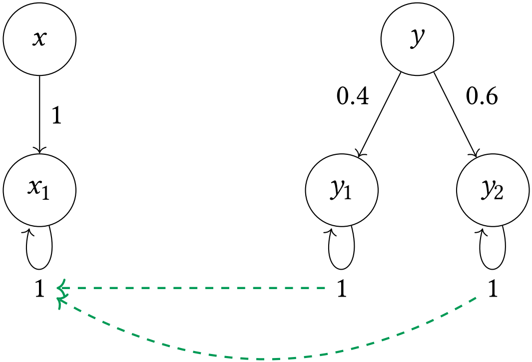
Probabilities?



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

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

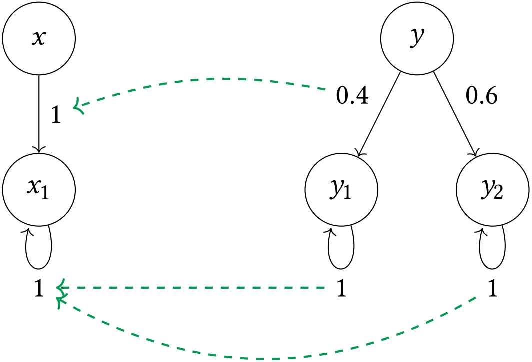
Probabilities?



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

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

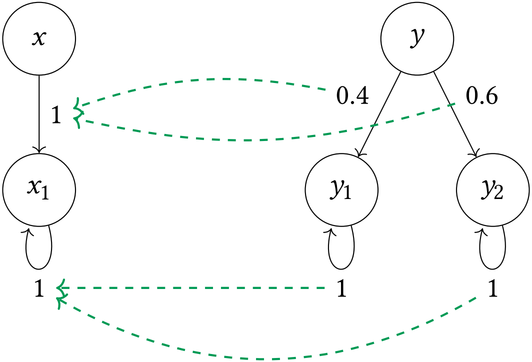
Probabilities?



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

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

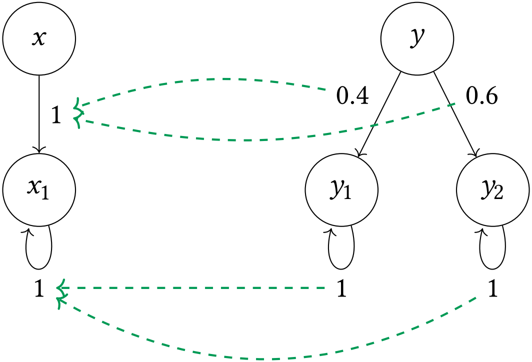
Probabilities?



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

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

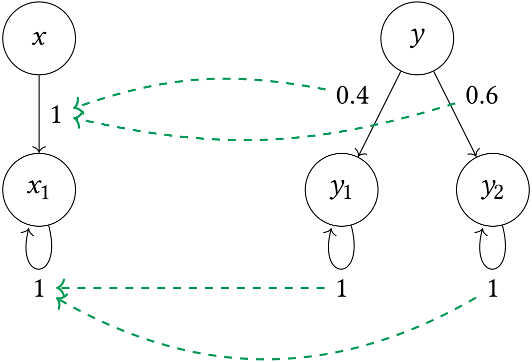
Probabilities?



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

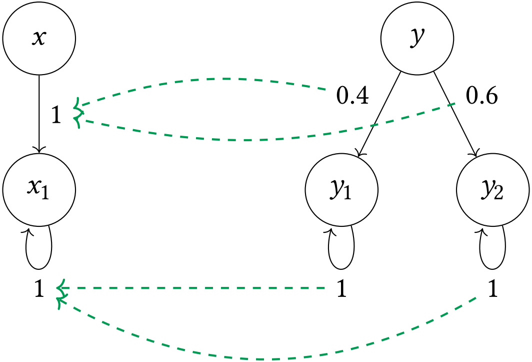
Relation Lifting: (Bartels, Sokolova, de Vink 2003/4), (Sokolova 2011)

Probabilities?



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

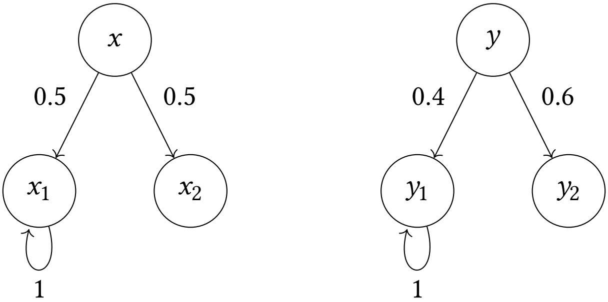
Probabilities?



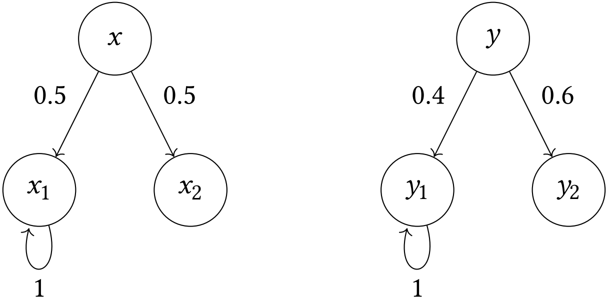
$$x \underline{\leftrightarrow} y \iff \forall z \in X.\ \sum_{z' : z \underline{\leftrightarrow} z'} \mu_x(z') = \sum_{z' : z \underline{\leftrightarrow} z'} \mu_y(z')$$

(Larsen and Skou, 1989/1991)

Apartness

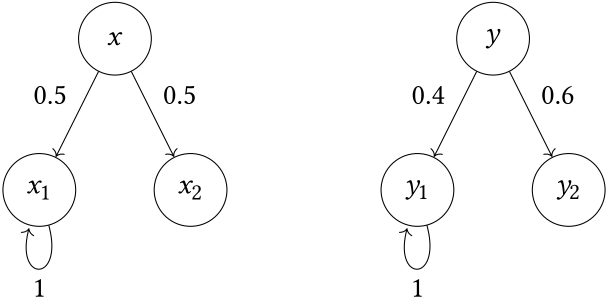


Apartness



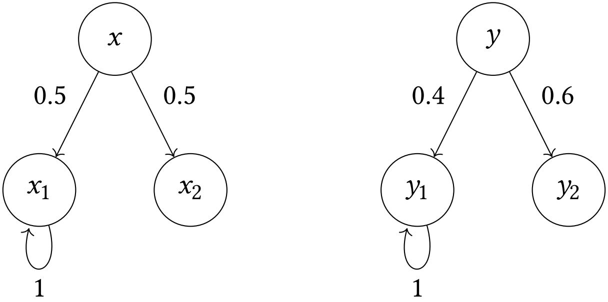
$$x \# y \iff \exists z \in X.\ \sum_{z' : \neg(z \# z')} \mu_x(z') \neq \sum_{z' : \neg(z \# z')} \mu_y(z')$$

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



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

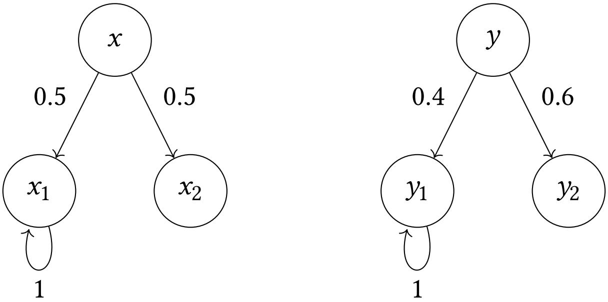
- Can this be determined “step-wise”?
- Do we need the whole apartness/bisimilarity relation?

Proof Rule

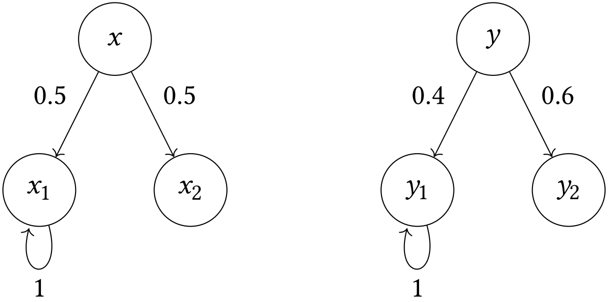
$$\frac{\forall (x', y') \in R.\, x' \# y' \qquad \exists z \in \mathrm{supp}(\mu_x) \cup \mathrm{supp}(\mu_y).\, \mu_x[z]_{\overline{R}} \neq \mu_y[z]_{\overline{R}}}{x \# y}$$

- Monotonicity of operator defining precongruences of Aczel & Mendler allows such a rule

Finite Proof



Finite Proof



$$\frac{\begin{array}{ll} x_1 \# x_2 & \\ y_1 \# y_2 & \\ x_2 \# y_1 & \\ x_1 \# y_2 & \mu_x[x_1]_{\overline{R}} = 0.5 \neq 0.4 = \mu_y[x_1]_{\overline{R}} \end{array}}{x \# y}$$

Some generalisations

State-based systems as coalgebras $\gamma : X \to BX$ for a (finitary) functor $B : \mathsf{Set} \to \mathsf{Set}$

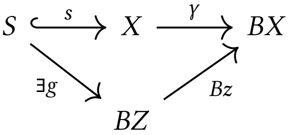
Examples

DFAs: $\gamma : X \to 2 \times X^A$, Mealy Machines: $\gamma : X \to \mathscr{P}(B \times X)^A$, MDPs: $\gamma : X \to \mathscr{D}_s(X)^A$

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 $z : Z \subseteq X$ such that transitions from S only reach states in Z



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"

Extending to more systems

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

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

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

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

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

More examples

Mealy Machines, Probabilistic Automata, POMDPs, etc.

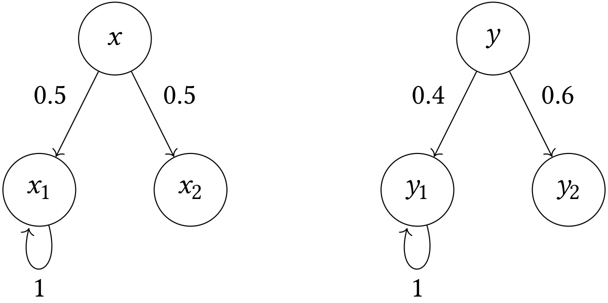
Conclusion

- 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
- In the paper: proofs of soundness and completeness (for finitary behaviour functors)

Future Work

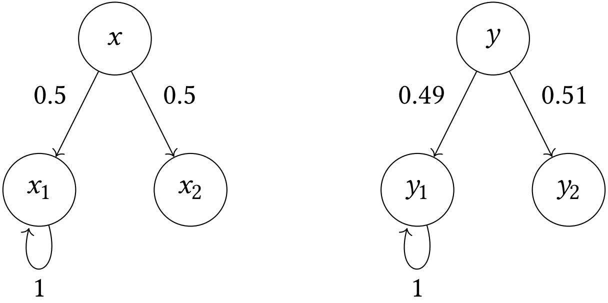
- Connection to logics?
- Apartness $\leftrightarrow$ Distinguishing Formulas

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!