

Measuring Confinement via Weak Bisimulation

Herbert Wiklicky

joint work with
Alessandra Di Pierro and Chris Hankin

Imperial College London

Università di Pisa

Overview

- Motivation

Overview

- Motivation
- Probabilistic Transition Systems

Overview

- Motivation
- Probabilistic Transition Systems
- Strong Bisimulation

Overview

- Motivation
- Probabilistic Transition Systems
- Strong Bisimulation
- Weak Bisimulation

Overview

- Motivation
- Probabilistic Transition Systems
- Strong Bisimulation
- Weak Bisimulation
- Further Work

Non-Interference

Non-Interference = Indistinguishability
[Goguen, Meseguer 82]

Non-Interference

Non-Interference = Indistinguishability

[Goguen, Meseguer 82]

Generalisation:

Approximate Non-Interference = Similarity

[Di Pierro, Hankin, Wiklicky 02/04]

Non-Interference

Non-Interference = Indistinguishability

[Goguen, Meseguer 82]

Generalisation:

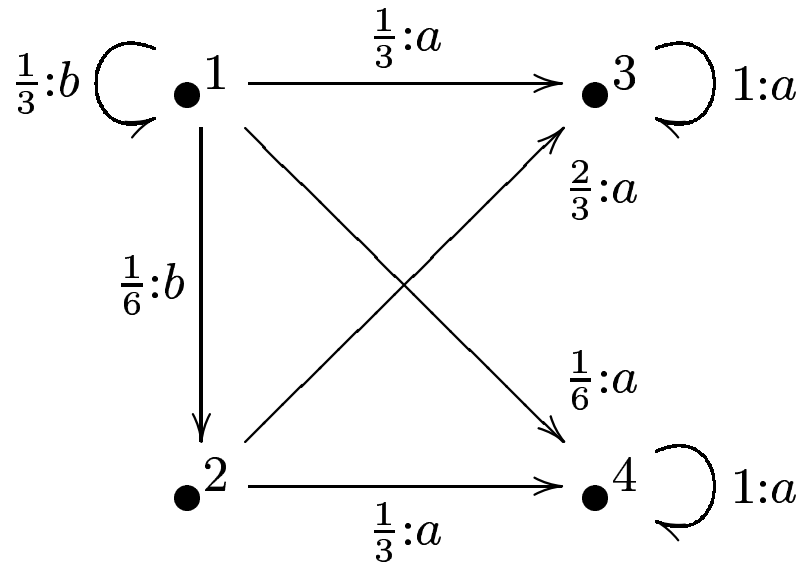
Approximate Non-Interference = Similarity

[Di Pierro, Hankin, Wiklicky 02/04]

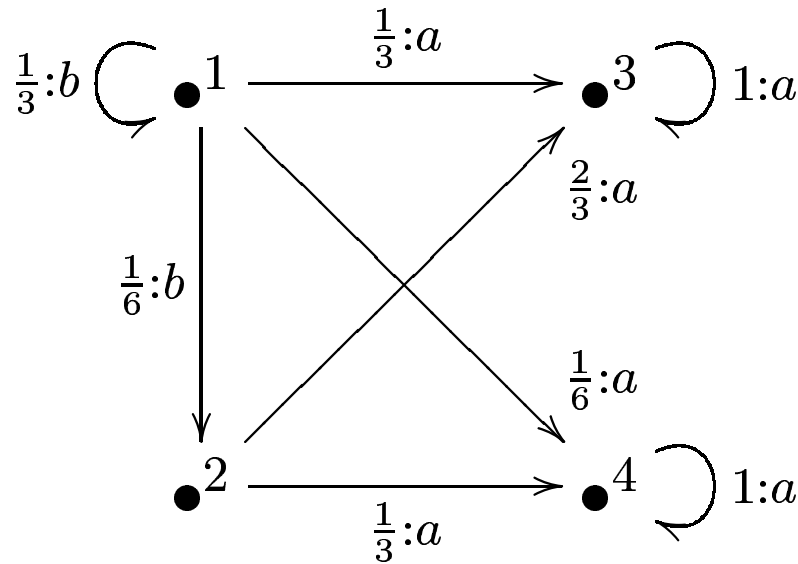
Depending on Notion of Observability

Introduce/Allow: Non-observable, silent, high-level τ actions
e.g. [Smith 03], [Aldini, Bravetti, Gorrieri 03], [Aldini, Di
Pierro 04]

Transition Graphs and Matrices



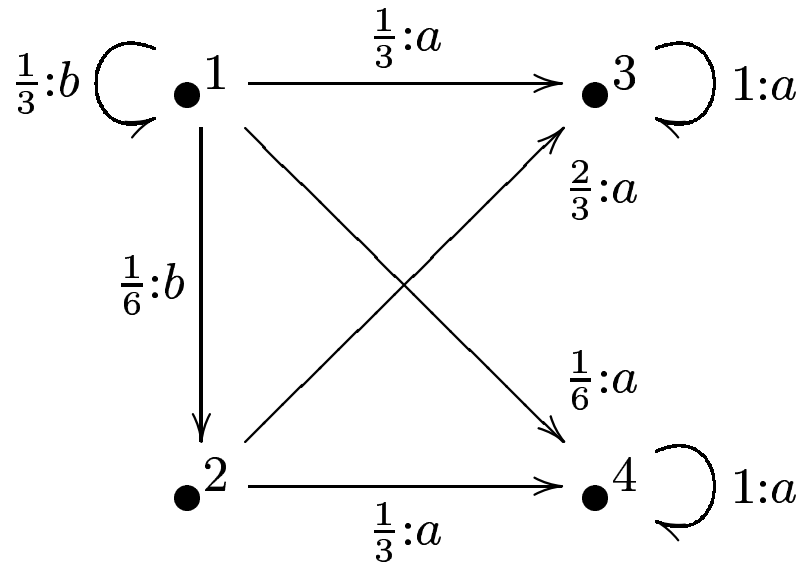
Transition Graphs and Matrices



$$\mathbf{M}_a(p) = \begin{pmatrix} 0 & 0 & \frac{1}{3} & \frac{1}{6} \\ 0 & 0 & \frac{2}{3} & \frac{1}{3} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\mathbf{M}_b(p) = \begin{pmatrix} \frac{1}{3} & \frac{1}{6} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Transition Graphs and Matrices



$$\mathbf{M}(p) = \begin{pmatrix} 0 & 0 & \frac{1}{3} & \frac{1}{6} \\ 0 & 0 & \frac{2}{3} & \frac{1}{3} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \oplus \begin{pmatrix} \frac{1}{3} & \frac{1}{6} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Probabilistic Transition System

A **probabilistic transition system** (PTS) is a tuple $(S, A, \longrightarrow, \pi_0)$, where:

- S is a non-empty, finite set of *states*,
- A is a non-empty, finite set of *actions*,
- $\longrightarrow \subseteq S \times \text{Dist}(A \times S)$ is a (*generative*) *transition relation*, and
- $\pi_0 \in \text{Dist}(S)$ is an *initial distribution* on S .

Matrix Representation

For quantitative/probabilistic relations $R \subseteq X \times \mathbb{W} \times X$ define:

$$(\mathbf{M}_R)_{xy} = \begin{cases} w & \text{iff } (x, w, y) \in R \\ 0 & \text{otherwise} \end{cases}$$

Matrix Representation

For quantitative/probabilistic relations $R \subseteq X \times \mathbb{W} \times X$
define:

$$(\mathbf{M}_R)_{xy} = \begin{cases} \sum w & \text{iff } (x, w, y) \in R \\ 0 & \text{otherwise} \end{cases}$$

Matrix Representation

For quantitative/probabilistic relations $R \subseteq X \times \mathbb{W} \times X$ define:

$$(\mathbf{M}_R)_{xy} = \begin{cases} w & \text{iff } (x, w, y) \in R \\ 0 & \text{otherwise} \end{cases}$$

For labelled relations $L \subseteq X \times A \times \mathbb{W} \times X$ define:

$$L|_a = \{(x, w, y) \mid (x, a, w, y) \in L\}$$

and then:

$$\mathbf{M}_L = \bigoplus_{a \in A} \mathbf{M}_{L|_a}$$

Strong Bisimulation

A **bisimulation** is a binary relation \sim_b on states of a labelled transition system satisfying for all $\alpha \in A$:

$$\begin{aligned} p \sim_b q \text{ and } p \xrightarrow{\alpha} p' &\Rightarrow \exists q' : q \xrightarrow{\alpha} q' \text{ and } p' \sim_b q', \\ p \sim_b q \text{ and } q \xrightarrow{\alpha} q' &\Rightarrow \exists p' : p \xrightarrow{\alpha} p' \text{ and } q' \sim_b p'. \end{aligned}$$

Strong Bisimulation

A **bisimulation** is a binary relation \sim_b on states of a labelled transition system satisfying for all $\alpha \in A$:

$$\begin{aligned} p \sim_b q \text{ and } p \xrightarrow{\alpha} p' &\Rightarrow \exists q' : q \xrightarrow{\alpha} q' \text{ and } p' \sim_b q', \\ p \sim_b q \text{ and } q \xrightarrow{\alpha} q' &\Rightarrow \exists p' : p \xrightarrow{\alpha} p' \text{ and } q' \sim_b p'. \end{aligned}$$

A **probabilistic bisimulation** is an equivalence relation \sim_b on states of a probabilistic transition system satisfying for all $\alpha \in A$:

$$p \sim_b q \text{ and } p \xrightarrow{\alpha} \pi \Rightarrow q \xrightarrow{\alpha} \varrho \text{ and } \pi \sim_b \varrho.$$

[Larsen Skou 91]

Strong Bisimulation (Linear)

Given the operator representations $\mathbf{M}(p)$ and $\mathbf{M}(q)$ of two probabilistic transition systems $p = (S, A, \longrightarrow, s_0)$ and $q = (S', A, \longrightarrow', s'_0)$ then p and q are probabilistic bisimilar iff there exists classification matrices \mathbf{K}_p and \mathbf{K}_q of dimension $(|S| \times n)$ and $(|S'| \times n)$ for some n such that

$$\mathbf{K}_p^\dagger \cdot \mathbf{M}(p) \cdot \mathbf{K}_p = \mathbf{K}_q^\dagger \cdot \mathbf{M}(q) \cdot \mathbf{K}_q,$$

i.e. for all $\alpha \in A$ we have

$$\mathbf{K}_p^\dagger \cdot \mathbf{M}(\overset{\alpha}{\longrightarrow}) \cdot \mathbf{K}_p = \mathbf{K}_q^\dagger \cdot \mathbf{M}(\overset{\alpha}{\longrightarrow}') \cdot \mathbf{K}_q.$$

Probabilistic Abstract Interpretation

Let \mathcal{C} and \mathcal{D} be two probabilistic domains (Hilbert spaces). A **probabilistic abstract interpretation** is a pair of bounded linear operators $A : \mathcal{C} \rightarrow \mathcal{D}$ and $G : \mathcal{D} \rightarrow \mathcal{C}$, between (the concrete domain) \mathcal{C} and (the abstract domain) \mathcal{D} , such that G is the Moore-Penrose pseudo-inverse of A .

Probabilistic Abstract Interpretation

Let \mathcal{C} and \mathcal{D} be two probabilistic domains (Hilbert spaces). A **probabilistic abstract interpretation** is a pair of bounded linear operators $\mathbf{A} : \mathcal{C} \rightarrow \mathcal{D}$ and $\mathbf{G} : \mathcal{D} \rightarrow \mathcal{C}$, between (the concrete domain) \mathcal{C} and (the abstract domain) \mathcal{D} , such that \mathbf{G} is the Moore-Penrose pseudo-inverse of \mathbf{A} .

Given the concrete semantical function via an operator Φ on a Hilbert space \mathcal{C} and a linear abstraction function $\mathbf{A} : \mathcal{C} \mapsto \mathcal{D}$. Utilising its Moore-Penrose pseudo-inverse $\mathbf{G} = \mathbf{A}^\dagger$ of \mathbf{A} we define the abstract (induced) semantics as

$$\Psi = \mathbf{A} \circ \Phi \circ \mathbf{G}.$$

Moore-Penrose Pseudoinverse

Let \mathcal{C} and \mathcal{D} be two Hilbert spaces and $A : \mathcal{C} \mapsto \mathcal{D}$ a linear map between them. A linear map $A^\dagger = G : \mathcal{D} \mapsto \mathcal{C}$ is the **Moore-Penrose pseudo-inverse** of A iff

$$A \circ G = P_A \quad \text{and} \quad G \circ A = P_G$$

where P_A and P_G denote orthogonal projections onto the ranges of A and G .

Moore-Penrose Pseudoinverse

Let \mathcal{C} and \mathcal{D} be two Hilbert spaces and $A : \mathcal{C} \mapsto \mathcal{D}$ a linear map between them. A linear map $A^\dagger = G : \mathcal{D} \mapsto \mathcal{C}$ is the **Moore-Penrose pseudo-inverse** of A iff

$$A \circ G = P_A \quad \text{and} \quad G \circ A = P_G$$

where P_A and P_G denote orthogonal projections onto the ranges of A and G .

Let $\mathcal{C} = (\mathcal{C}, \leq_{\mathcal{C}})$ and $\mathcal{D} = (\mathcal{D}, \leq_{\mathcal{D}})$ be two partially ordered sets. If there are two monotone functions $\alpha : \mathcal{C} \mapsto \mathcal{D}$ and $\gamma : \mathcal{D} \mapsto \mathcal{C}$ such that for all $c \in \mathcal{C}$ and $d \in \mathcal{D}$:

$$c \leq_{\mathcal{C}} \gamma(d) \quad \text{iff} \quad \alpha(c) \leq_{\mathcal{D}} d,$$

then $(\mathcal{C}, \alpha, \gamma, \mathcal{D})$ form a **Galois connection**.

Moore-Penrose Pseudoinverse

Let \mathcal{C} and \mathcal{D} be two Hilbert spaces and $A : \mathcal{C} \mapsto \mathcal{D}$ a linear map between them. A linear map $A^\dagger = G : \mathcal{D} \mapsto \mathcal{C}$ is the **Moore-Penrose pseudo-inverse** of A iff

$$A \circ G = P_A \quad \text{and} \quad G \circ A = P_G$$

where P_A and P_G denote orthogonal projections onto the ranges of A and G .

An operator $A \in \mathcal{B}(\mathcal{H})$ is Moore-Penrose invertible if and only if it is **normally solvable**, i.e. the range $\{Ax \mid x \in \mathcal{H}\}$ is closed.

Weak Bisimulation

A **probabilistic weak bisimulation** is an equivalence relation \sim_w on states of a PTS satisfying for all $\alpha \in A$:

$$p \sim_w q \text{ and } p \xrightarrow{\tau^*} \xrightarrow{\alpha} \xrightarrow{\tau^*} \pi$$
$$\Rightarrow$$
$$q \xrightarrow{\tau^*} \xrightarrow{\alpha} \xrightarrow{\tau^*} \rho \text{ and } \pi \sim_w \rho.$$

Trace Probabilities

The probability of reaching a state or a certain class of states by sequences of actions or **traces** is defined in for strings in a generic language $\Lambda \subset A^*$ recursively as follows:

$$\mathcal{P}(s, \Lambda, C) = 1 \quad \text{if } s \in C \text{ and } \varepsilon \in \Lambda$$

$$\mathcal{P}(s, \Lambda, C) = \sum_{(a,t) \in A \times S} P(s, a, t) \cdot \mathcal{P}(t, \Lambda/a, C) \quad \text{otherwise}$$

where Λ/a denotes the set of all strings λ such that $a\lambda \in \Lambda$, and ε denotes the empty string.

Exact Reachability

Given the operator representation $\mathbf{M}(p)$ of a probabilistic process p with $A = \{\alpha, \beta, \dots, \tau\}$, then we define, for $\alpha \in A$

$$\mathbf{E}_\alpha(p)(n, m) = \mathbf{M}_\tau(p)^n \mathbf{M}_\alpha(p) \mathbf{M}_\tau(p)^m.$$

We denote by $\mathbf{E}(p)(n, m)$ the direct sum $\bigoplus_{\alpha \in A} \mathbf{E}_\alpha(p)(n, m)$

Exact Reachability

Given the operator representation $\mathbf{M}(p)$ of a probabilistic process p with $A = \{\alpha, \beta, \dots, \tau\}$, then we define, for $\alpha \in A$

$$\mathbf{E}_\alpha(p)(n, m) = \mathbf{M}_\tau(p)^n \mathbf{M}_\alpha(p) \mathbf{M}_\tau(p)^m.$$

We denote by $\mathbf{E}(p)(n, m)$ the direct sum $\bigoplus_{\alpha \in A} \mathbf{E}_\alpha(p)(n, m)$

It is easy to show the following result:

Given the operator representation $\mathbf{M}(p)$ of a probabilistic process p , then for all states $s, s' \in S$,

$$(\mathbf{E}_\alpha(p)(n, m))_{s, s'} = \mathcal{P}(s, \tau^n \alpha \tau^m, s').$$

Naive Approach

Combine probabilities reaching s' from s with trace $\tau^n a \tau^m$:

$$\bar{\mathbf{E}}_{\alpha}(p) = \sum_{n,m=0}^{\infty} \mathbf{E}_{\alpha}(p)(n, m),$$

Naive Approach

Combine probabilities reaching s' from s with trace $\tau^n a \tau^m$:

$$\bar{\mathbf{E}}_{\alpha}(p) = \sum_{n,m=0}^{\infty} \mathbf{E}_{\alpha}(p)(n, m),$$

Naive Idea:

Given the operator representations $\mathbf{M}(p)$ and $\mathbf{M}(q)$ of two probabilistic transition systems $p = (S, A, \longrightarrow, s_0)$ and $q = (S', A, \longrightarrow', s'_0)$ then p and q are probabilistic bisimilar iff there exists classification matrices \mathbf{K}_p and \mathbf{K}_q of dimension $(|S| \times n)$ and $(|S'| \times n)$ for some n such that

$$\mathbf{K}_p^{\dagger} \cdot \mathbf{E}(p) \cdot \mathbf{K}_p = \mathbf{K}_q^{\dagger} \cdot \mathbf{E}(q) \cdot \mathbf{K}_q.$$

Naive Approach

Combine probabilities reaching s' from s with trace $\tau^n a \tau^m$:

$$\bar{\mathbf{E}}_{\alpha}(p) = \sum_{n,m=0}^{\infty} \mathbf{E}_{\alpha}(p)(n, m),$$

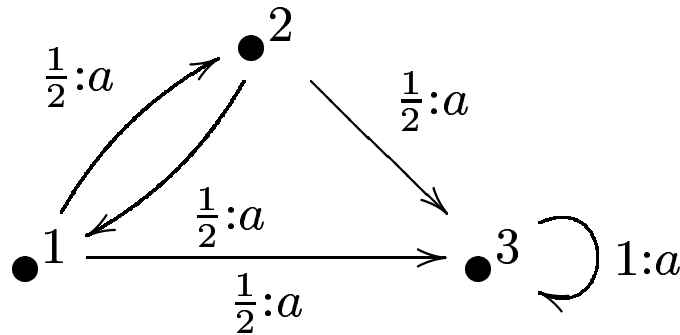
WRONG

Given the operator representations $\mathbf{M}(p)$ and $\mathbf{M}(q)$ of two probabilistic transition systems $p = (S, A, \longrightarrow, s_0)$ and $q = (S', A, \longrightarrow', s'_0)$ then p and q are probabilistic bisimilar iff there exists classification matrices \mathbf{K}_p and \mathbf{K}_q of dimension $(|S| \times n)$ and $(|S'| \times n)$ for some n such that

$$\mathbf{K}_p^{\dagger} \cdot \mathbf{E}(p) \cdot \mathbf{K}_p = \mathbf{K}_q^{\dagger} \cdot \mathbf{E}(q) \cdot \mathbf{K}_q.$$

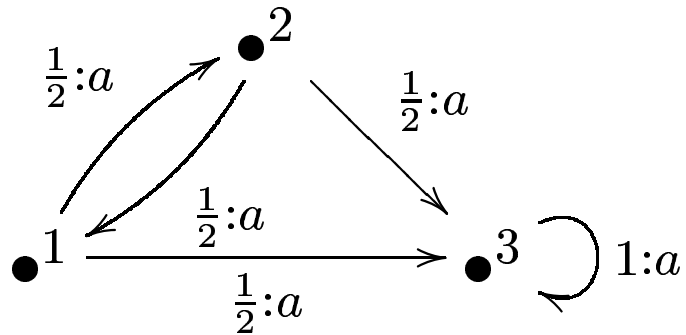
Naive Approach: Problem

Consider the following simple PTS with only one action a :



Naive Approach: Problem

Consider the following simple PTS with only one action a :

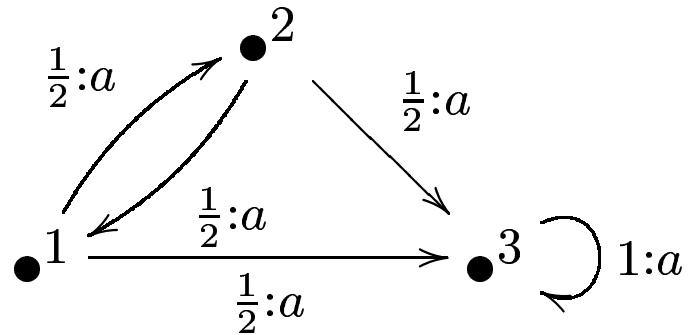


In order to calculate the probabilities $\mathcal{P}(s, a^*, \{t\})$, we construct the operators:

$$\mathbf{M}_a = \begin{pmatrix} 0 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & 1 \end{pmatrix}$$

Naive Approach: Problem

Consider the following simple PTS with only one action a :

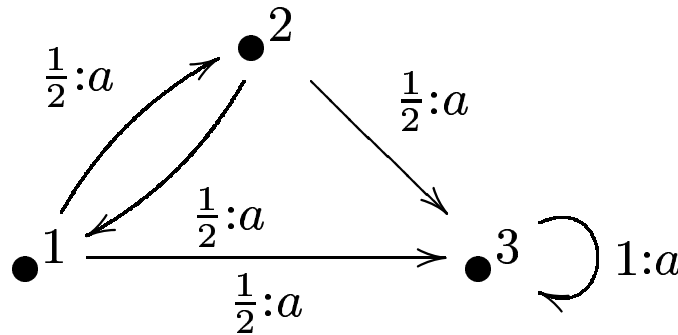


In order to calculate the probabilities $\mathcal{P}(s, a^*, \{t\})$, we construct the operators:

$$\lim_{n \rightarrow \infty} \mathbf{M}_a^n = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Naive Approach: Problem

Consider the following simple PTS with only one action a :



In order to calculate the probabilities $\mathcal{P}(s, a^*, \{t\})$, we construct the operators:

$$\bar{\mathbf{E}}_a(p) = \sum_{i=0}^{\infty} \mathbf{M}_a^i = \begin{pmatrix} \frac{4}{3} & \frac{2}{3} & \infty \\ \frac{2}{3} & \frac{4}{3} & \infty \\ 0 & 0 & \infty \end{pmatrix}$$

Weak Bisimulation

A **weak bisimulation** is an equivalence relation \sim_w on S such that for all $s \sim_w s'$ and all $\alpha \in A \setminus \{\tau\} \cup \varepsilon$ and all equivalence classes $C \in S / \sim_w$ we have:

$$\mathcal{P}(s, \tau^* \alpha \tau^*, C) = \mathcal{P}(s', \tau^* \alpha \tau^*, C)$$

[Baier, Hermanns 97]

Projection Operators as Filter

We define a “projection into t ” as a diagonal matrix which contains a single entry 1 at the position (t, t) , and its “negation”, i.e.

$$(\mathbf{P}_t)_{ij} = \begin{cases} 1 & \text{for } i = j = t \\ 0 & \text{otherwise} \end{cases} \quad (\mathbf{P}_t^\perp)_{ij} = \begin{cases} 1 & \text{for } i = j \neq t \\ 0 & \text{otherwise} \end{cases}$$

Projection Operators as Filter

We define a “projection into t ” as a diagonal matrix which contains a single entry 1 at the position (t, t) , and its “negation”, i.e.

$$(\mathbf{P}_t)_{ij} = \begin{cases} 1 & \text{for } i = j = t \\ 0 & \text{otherwise} \end{cases} \quad (\mathbf{P}_t^\perp)_{ij} = \begin{cases} 1 & \text{for } i = j \neq t \\ 0 & \text{otherwise} \end{cases}$$

We consider the modified transition operator

$$\mathbf{M}_{\alpha, \neg t}(p) = \mathbf{P}_t^\perp \mathbf{M}_\alpha(p)$$

we get the same transitions as in $\mathbf{M}_\alpha(p)$ except that all transitions from t are cancelled out.

First Passages

Consider column t in $\mathbf{M}_{\alpha, \neg t}^n(p)$ we obtain for each state s the probability of reaching t in exactly n steps without passing through t .

We can extract this t column by multiplying with \mathbf{P}_t , i.e.

$$(\mathbf{P}_t^\perp \mathbf{M}_\alpha(p))^n \cdot \mathbf{P}_t = \mathbf{M}_{\alpha, \neg t}(p) \cdot \mathbf{P}_t.$$

First Passages

The probability of getting from state s to t via the minimal trace in at most n steps is then given by:

$$\sum_{i=0}^n (\mathbf{P}_t^\perp \mathbf{M}_\alpha(p))^i \cdot \mathbf{P}_t = \sum_{i=0}^n (\mathbf{M}_{\alpha, \neg t}(p))^i \cdot \mathbf{P}_t$$

First Passages

The probability of getting from state s to t via the minimal trace in at most n steps is then given by:

$$\sum_{i=0}^n (\mathbf{P}_t^\perp \mathbf{M}_\alpha(p))^{i-1} \cdot \mathbf{P}_t = \sum_{i=0}^n (\mathbf{M}_{\alpha, -t}(p))^{i-1} \cdot \mathbf{P}_t$$

Combining this information for all states t we obtain for all $\alpha \in A$ the matrix:

$$\sum_{t \in S} \left(\sum_{i=0}^n (\mathbf{P}_t^\perp \mathbf{M}_\alpha(p))^{i-1} \cdot \mathbf{P}_t \right) = \sum_{t \in S} \left(\sum_{i=0}^n (\mathbf{M}_{\alpha, -t}(p))^{i-1} \cdot \mathbf{P}_t \right)$$

Example

In the previous example, the projection operators for $t = 2$ are:

$$\mathbf{P}_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \mathbf{P}_2^\perp = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and the corresponding modified a -transition operator is

$$\mathbf{M}_{a, \neg 2} = \mathbf{P}_2^\perp \mathbf{M}_a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Example

$$\mathbf{M}_{a,-2}^0 \mathbf{P}_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\mathbf{M}_{a,-2}^1 \mathbf{P}_2 = \begin{pmatrix} 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\mathbf{M}_{a,-2}^2 \mathbf{P}_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

...

Example

We can combine the information on the probability of reaching all states in i steps in the operator $\sum_{t \in S} \mathbf{M}_{a, \neg t}^i \mathbf{P}_t$.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \frac{1}{4} \\ 0 & 0 & \frac{1}{4} \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \frac{1}{8} \\ 0 & 0 & \frac{1}{8} \\ 0 & 0 & 0 \end{pmatrix}, \dots$$

Finally, we can compute the probability of reaching a state from any other by any string in the language a^* by

$$\sum_{t \in S} \left(\sum_{i=0}^{\infty} \mathbf{M}_{a, \neg t}^i \mathbf{P}_t \right) = \sum_{i=0}^{\infty} \left(\sum_{t \in S} \mathbf{M}_{a, \neg t}^i \mathbf{P}_t \right) = \begin{pmatrix} 1 & \frac{1}{2} & 1 \\ \frac{1}{2} & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Reachability

Given the operator representations $\mathbf{M}(p)$ of a probabilistic transition system $p = (S, A, \longrightarrow, s_0)$ then for all $\alpha \in A$:

$$\mathcal{P}(s, \alpha^*, \{t\}) = \left(\sum_{i=0}^{\infty} \left(\sum_{t \in S} \mathbf{M}_{\alpha, \neg t}^i(p) \mathbf{P}_t \right) \right)_{st} .$$

Reachability

Given the operator representation $\mathbf{M}(p)$ of a PTS p with $A = \{a, b, \dots, \tau\}$, then we define for all $\alpha \in A$:

$$\mathbf{F}_\alpha(p)(n, m) = \sum_{t \in S} \mathbf{M}_\tau(p)^n \cdot \mathbf{M}_\alpha(p) \cdot (\mathbf{P}_t^\perp \mathbf{M}_\tau(p))^m \cdot \mathbf{P}_t.$$

We denote by $\mathbf{F}(p)(n, m)$ the direct sum $\bigoplus_{\alpha \in A} \mathbf{F}_\alpha(p)(n, m)$.

The operator $\mathbf{F}_\alpha(p)(n, m)$ encodes the probabilities of reaching a state by the trace $\tau^n \alpha \tau^m$, for some fixed $n, m \in \mathbb{N}$. The extension to the language $\tau^* \alpha \tau^*$ is via:

$$\bar{\mathbf{F}}_\alpha(p) = \sum_{n, m=0}^{\infty} \mathbf{F}_\alpha(p)(n, m)$$

Reachability

Given the operator representation $\mathbf{M}(p)$ of a probabilistic transition system $p = (S, A, \longrightarrow, s_0)$ then for all $\alpha \in A$:

$$\mathcal{P}(s, \tau^* \alpha \tau^*, \{t\}) = (\overline{\mathbf{F}}_\alpha(p))_{st}$$

Reachability

Given the operator representation $\mathbf{M}(p)$ of a process $p = (S, A, \longrightarrow, s_0)$ with $A = \{a, b, \dots, \tau\}$, and a partition $\mathcal{C} = \{C_i\}_i$ of S represented by a classification matrix \mathbf{K} '

$$\mathbf{F}_\alpha(p, \mathbf{K})(n, m) = \sum_{C_i \in \mathcal{C}} \mathbf{M}_\tau(p)^n \cdot \mathbf{M}_\alpha(p) \cdot (\mathbf{P}_{C_i}^\perp \mathbf{M}_\tau(p))^m \cdot \mathbf{P}_{C_i}.$$

We denote by $\mathbf{F}(p, \mathbf{K})(n, m)$ the direct sum $\bigoplus_{\alpha \in A}$.

Furthermore, we define:

$$\bar{\mathbf{F}}_\alpha(p, \mathbf{K}) = \sum_{n, m=0}^{\infty} \mathbf{F}_\alpha(p, \mathbf{K})(n, m).$$

Reachability

Given the operator representations $\mathbf{M}(p)$ of a probabilistic transition systems $p = (S, A, \longrightarrow, s_0)$ and a partition $\mathcal{C} = \{C_i\}_i$ of S represented by a classification matrix \mathbf{K} then for all $\alpha \in A$:

$$\mathcal{P}(s, \tau^* \alpha \tau^*, C) = (\overline{\mathbf{F}}_\alpha(p, \mathbf{K}) \cdot \mathbf{K})_{sC}.$$

Weak Bisimulation (Linear)

Given the operator representations $\mathbf{M}(p)$ and $\mathbf{M}(q)$ of two probabilistic transition systems $p = (S, A, \longrightarrow, s_0)$ and $q = (S', A, \longrightarrow', s'_0)$ then p and q are probabilistic weak bisimilar iff there exist classification matrices $\mathbf{K}_p \in \mathcal{C}(|S|, n)$ and $\mathbf{K}_q \in \mathcal{C}(|S'|, n)$ for some $n \geq 1$ such that

$$\mathbf{K}_p^\dagger \cdot \bar{\mathbf{F}}(p, \mathbf{K}_p) \cdot \mathbf{K}_p = \mathbf{K}_q^\dagger \cdot \bar{\mathbf{F}}(q, \mathbf{K}_q) \cdot \mathbf{K}_q,$$

i.e. for all $\alpha \in A$ we have

$$\mathbf{K}_p^\dagger \cdot \bar{\mathbf{F}}_\alpha(p, \mathbf{K}_p) \cdot \mathbf{K}_p = \mathbf{K}_q^\dagger \cdot \bar{\mathbf{F}}_\alpha(q, \mathbf{K}_q) \cdot \mathbf{K}_q.$$

Approximate Weak Bisimulation

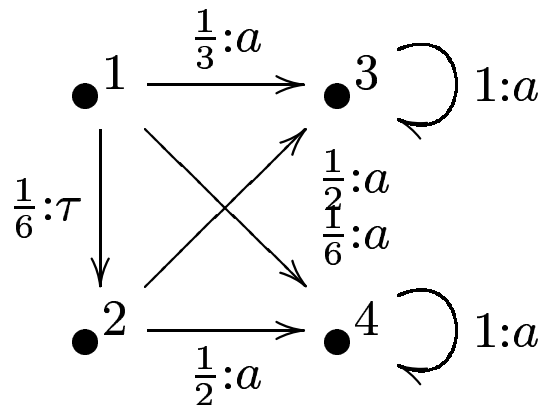
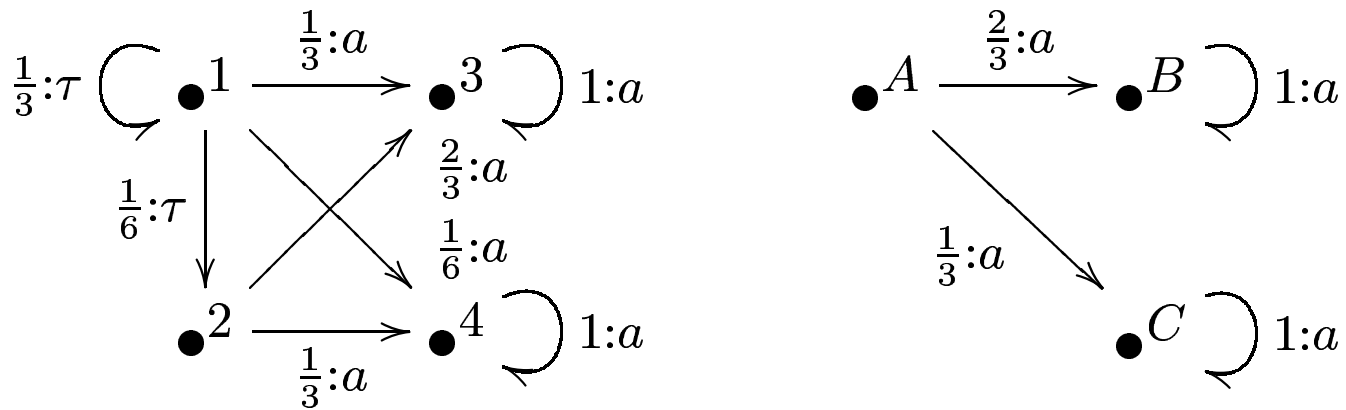
Given the operator representations $M(p)$ and $M(q)$ of two probabilistic transition systems $p = (S, A, \longrightarrow, s_0)$ and $q = (S', A, \longrightarrow', s'_0)$, we say that p and q are **probabilistic ε -weak bisimilar**, denoted by $p \sim_w^\varepsilon q$, if

$$\inf_{\mathbf{K}_p, \mathbf{K}_q \in \mathcal{C}} \|\mathbf{K}_p^\dagger \cdot \bar{\mathbf{F}}(p, \mathbf{K}_p) \cdot \mathbf{K}_p - \mathbf{K}_q^\dagger \cdot \bar{\mathbf{F}}(q, \mathbf{K}_q) \cdot \mathbf{K}_q\| = \varepsilon$$

where $\|\cdot\|$ denotes an appropriate norm.

Example [Smith 03]

The processes p , q and r are described by the following transition graphs:



Example [Smith 03]

Their matrix representations are given by:

$$\mathbf{M}_a(p) = \begin{pmatrix} 0 & 0 & \frac{1}{3} & \frac{1}{6} \\ 0 & 0 & \frac{2}{3} & \frac{1}{3} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \mathbf{M}_\tau(p) = \begin{pmatrix} \frac{1}{3} & \frac{1}{6} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Example [Smith 03]

Their matrix representations are given by:

$$\mathbf{M}_a(q) = \begin{pmatrix} 0 & \frac{2}{3} & \frac{1}{3} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Example [Smith 03]

Their matrix representations are given by:

$$\mathbf{M}_a(r) = \begin{pmatrix} 0 & 0 & \frac{1}{3} & \frac{1}{6} \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \mathbf{M}_\tau(r) = \begin{pmatrix} 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Example [Smith 03]

Partitioning states in three classes and using \mathbf{K}_p and \mathbf{K}_p^\dagger :

$$\begin{aligned} C_1 &= \{s_1, s_2\} \\ C_2 &= \{s_3\} \\ C_3 &= \{s_4\} \end{aligned} \quad \mathbf{K}_p = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \mathbf{K}_p^\dagger = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Compute $\mathcal{P}(s_i, \tau^* a \tau^*, C_j)$ and the abstracted system:

$$\overline{\mathbf{F}}_a(p, \mathbf{K}_p) \cdot \mathbf{K}_p = \begin{pmatrix} 0 & \frac{2}{3} & \frac{1}{3} \\ 0 & \frac{2}{3} & \frac{1}{3} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \mathbf{K}_p^\dagger \cdot \overline{\mathbf{F}}_a(p, \mathbf{K}_p) \cdot \mathbf{K}_p = \begin{pmatrix} 0 & \frac{2}{3} & \frac{1}{3} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Example [Smith 03]

Processes p and q probabilistic weak bisimilar as we have

$$\mathbf{K}_p^\dagger \cdot \bar{\mathbf{F}}_a(p) \cdot \mathbf{K} = \mathbf{M}_a(q)$$

Note in this example the “naive” approach based on $\bar{\mathbf{E}}$ is sufficient $\bar{\mathbf{E}}(p) \cdot \mathbf{K}_p = \bar{\mathbf{F}}(p, \mathbf{K}_p) \cdot \mathbf{K}_p$ and:

$$\mathbf{K}_p^\dagger \cdot \bar{\mathbf{E}}_a(p) \cdot \mathbf{K}_p = \mathbf{K}_p^\dagger \cdot \bar{\mathbf{F}}_a(p, \mathbf{K}_p) \cdot \mathbf{K}_p$$

Example [Smith 03]

Processes r and q are only probabilistic weak ε - bisimilar:

$$\begin{aligned} & \| \mathbf{K}_r^\dagger \cdot \bar{\mathbf{F}}_a(r, \mathbf{K}_r) \cdot \mathbf{K}_r - \mathbf{M}_a(q) \| = \\ & = \left\| \begin{pmatrix} 0 & \frac{13}{24} & \frac{11}{24} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & \frac{2}{3} & \frac{1}{3} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\| = \frac{1}{4} \end{aligned}$$

This measures the **statistical** dissimilarity of r and q .

Conclusion & Further Work

- PTS & Linear Operator Semantics

Conclusion & Further Work

- PTS & Linear Operator Semantics
- Probabilistic Abstract Interpretation

Conclusion & Further Work

- PTS & Linear Operator Semantics
- Probabilistic Abstract Interpretation
- Projections as Filters/Guards

Conclusion & Further Work

- PTS & Linear Operator Semantics
- Probabilistic Abstract Interpretation
- Projections as Filters/Guards
- Computational Efficiency

Conclusion & Further Work

- PTS & Linear Operator Semantics
- Probabilistic Abstract Interpretation
- Projections as Filters/Guards
- Computational Efficiency
- Continuous Optimisation