Category Theory for Compositional Verification

Kazuki Watanabe [1,2]
Clovis Eberhart [2,3]
Kazuyuki Asada [4]
Ichiro Hasuo [1,2]

Category Theory for Compositional Verification Models

Kazuki Watanabe [1,2]
Clovis Eberhart [2,3]
Kazuyuki Asada [4]
Ichiro Hasuo [1,2]

Category Theory for Compositional ~~Verification~~ Models

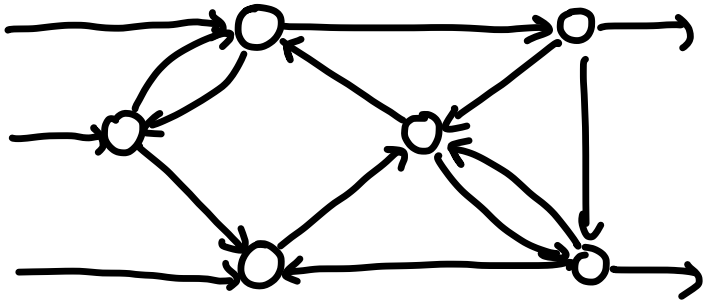
Markov Decision Processes

Kazuki Watanabe [1,2]
Clovis Eberhart [2,3]
Kazuyuki Asada [4]
Ichiro Hasuo [1,2]

Plan

categorical side

syntax



semantics

$\rightsquigarrow$ morphism $3 \to 2$ in $\mathbb{S}$

(+ bidirectional setting)

---

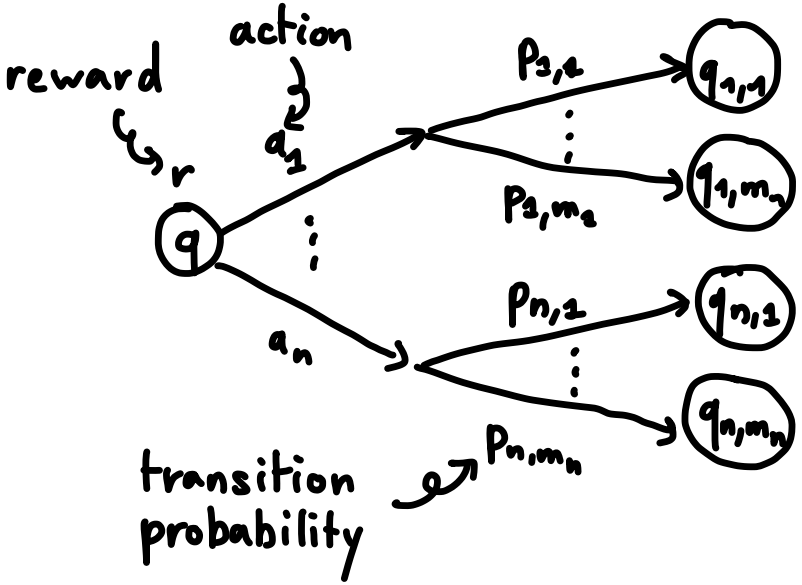
algorithmic side

We get a nice algorithm from a categorical approach.

(+ free syntax)

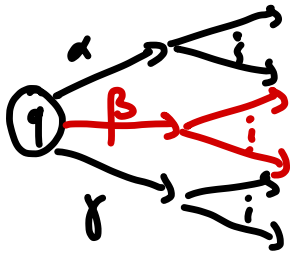
Markov Decision Processes

Definition: "graph-like" structure with actions, probabilities, and rewards.



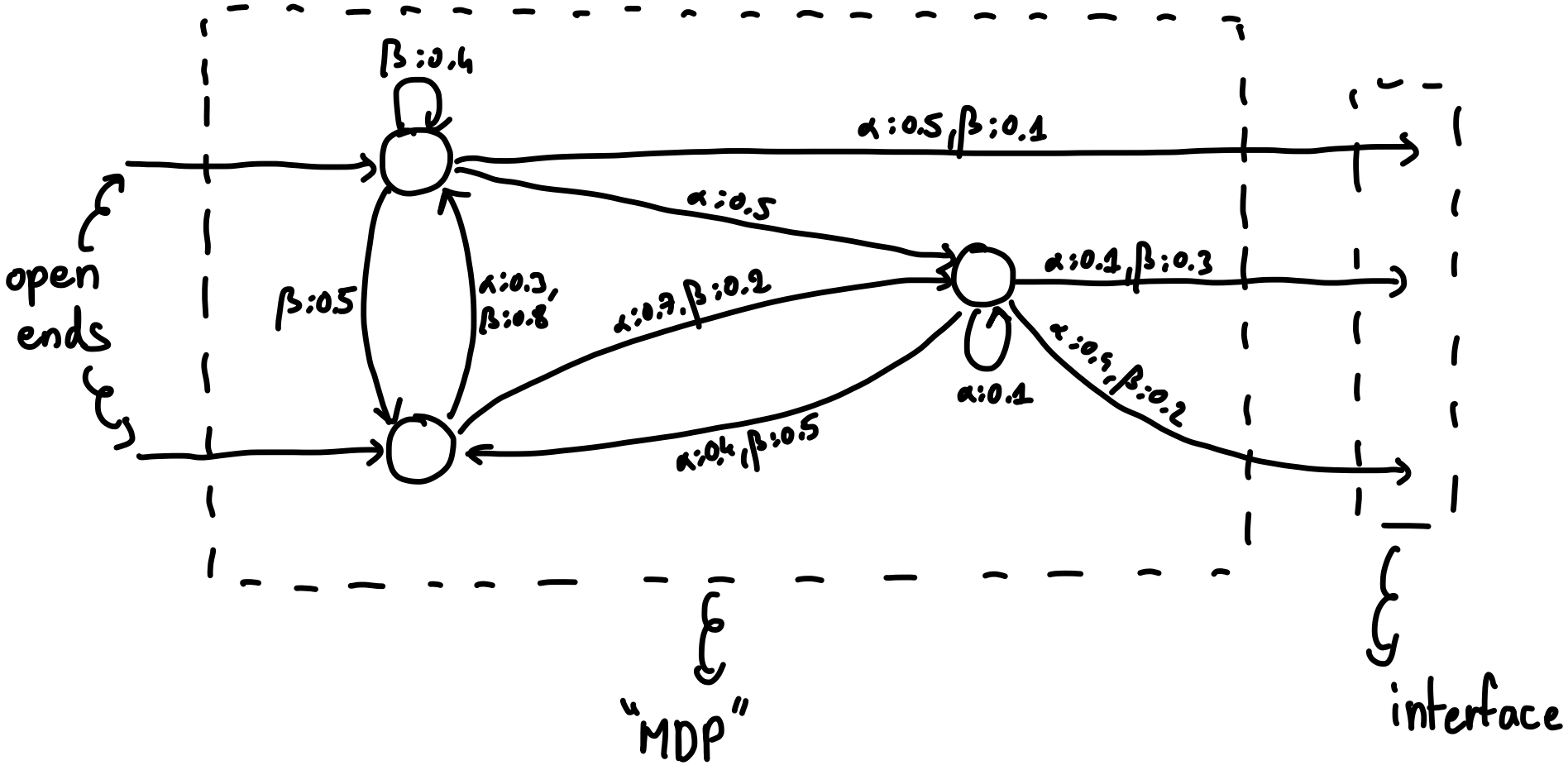
$$\left(\begin{array}{l}\text{coalgebras} \\ X \to (\mathcal{D}_{\leq 1} X)^{\Sigma} \times \mathbb{Q} \\ (\text{where } \Sigma = \{a_1, \ldots, a_n\})\end{array}\right)$$

scheduler: choice of action for each state
↳ expected reward from q_i to q_f



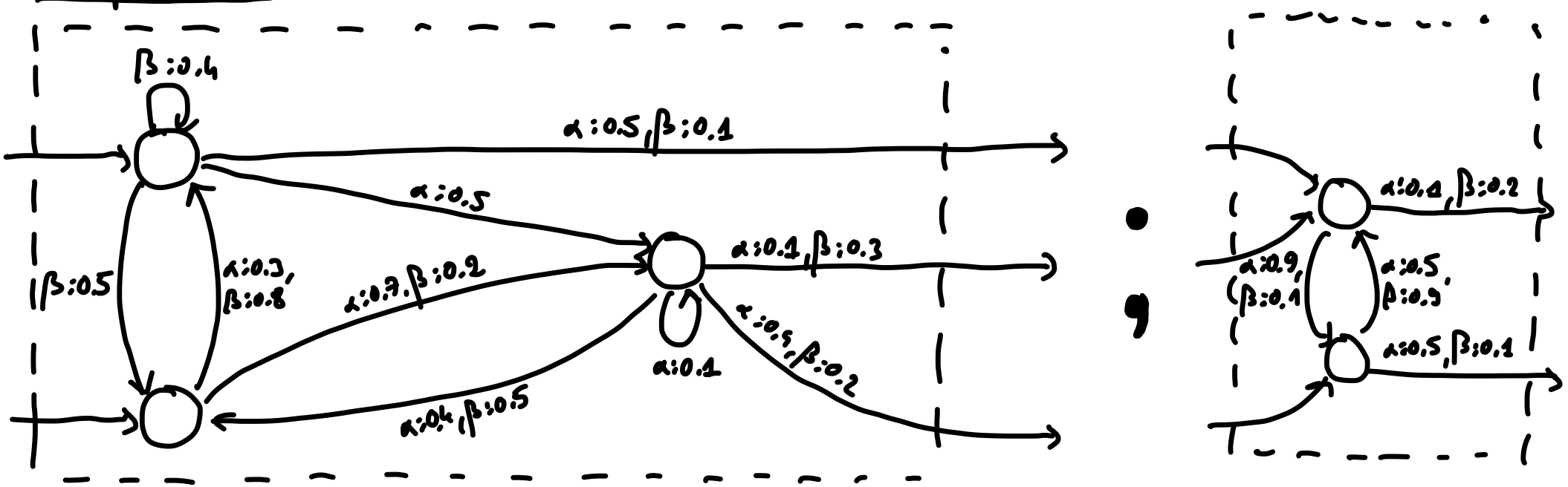
Problem: given $\mathcal{A}, q_i, q_f$, find the maximum expected reward from q_i to q_f.

Open MDPs

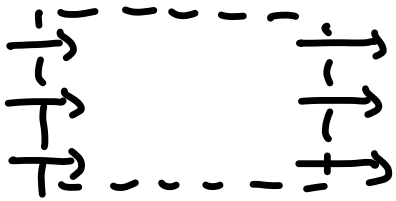


Composition of OMDPs

composition:



identities:



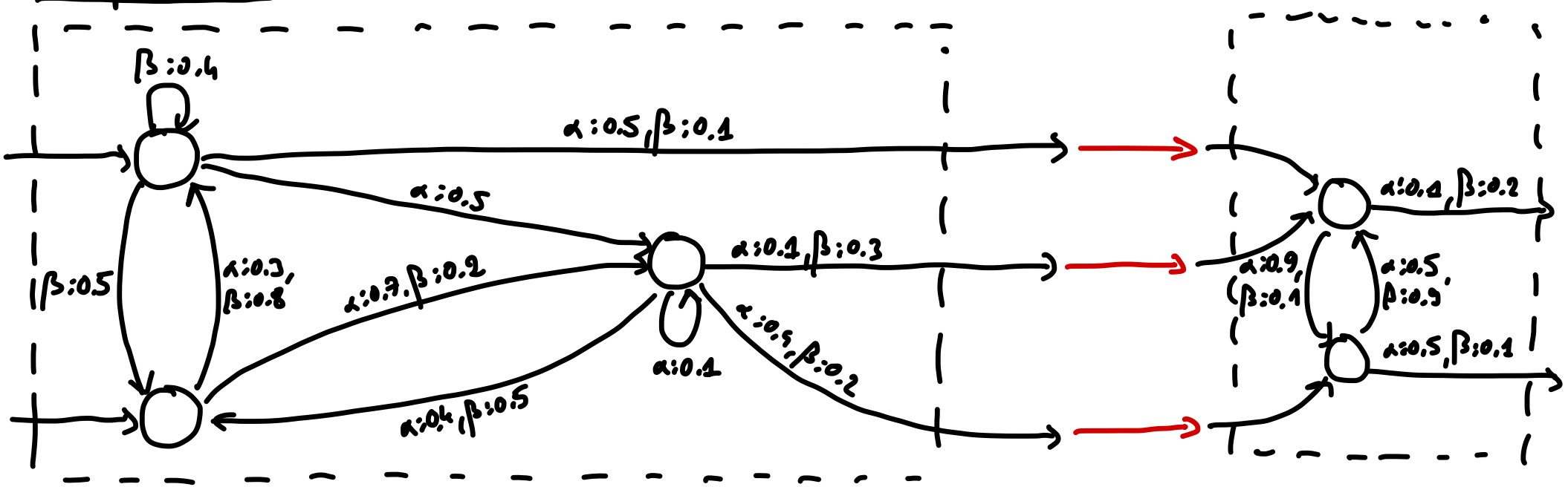
Lemma: OMDP ; _ objects : natural numbers

_ morphisms $m \to n$: OMDPs with m (n) open ends on the left (right)

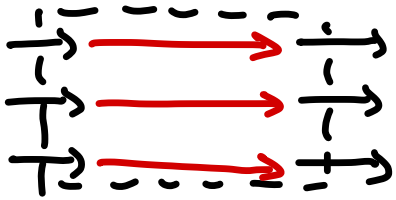
forms a category.

Composition of OMDPs

composition:



identities:

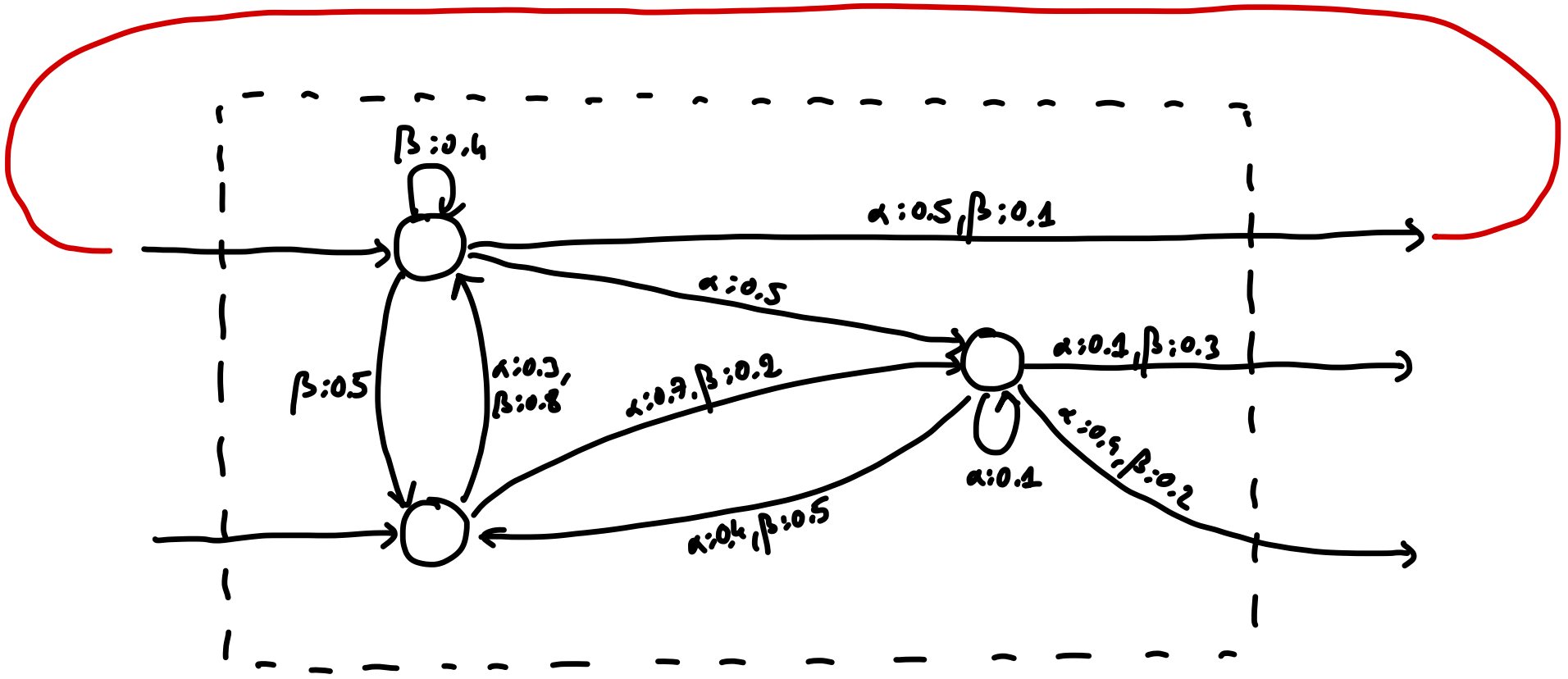


Lemma: OMDP ; _ objects : natural numbers

_ morphisms $m \to n$: OMDPs with m (n) open ends on the left (right)

forms a category.

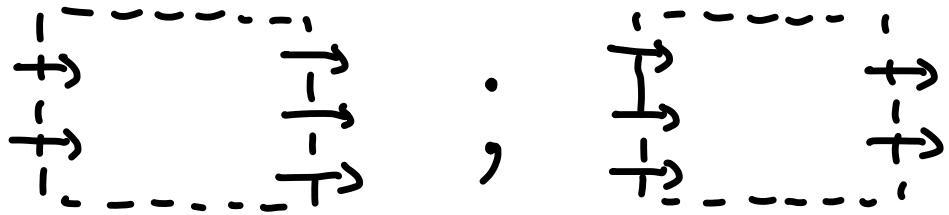
Trace of OMDPs



Lemma: OMDP forms a traced symmetric monoidal category (TSMC).

Semantics of OMDPs

To compute maximum expected reward compositionally, we need to know all possible expected rewards from entries to exits.



Probabilities: $RP_{\alpha;\beta}(i,k) = \sum_{j=1}^{n} RP_{\alpha}(i,j)\, RP_{\beta}(j,k)$

Expected reward: $ER_{\alpha;\beta}(i,k) = \sum_{j=1}^{n} ER_{\alpha}(i,j)\, RP_{\beta}(j,k) + RP_{\alpha}(i,j)\, ER_{\beta}(j,k)$

To compute expected rewards compositionally, we need to know:
- expected rewards
- reachability probabilities

Semantic Category for OMDPs

Definition of $\mathbb{S}$:

- objects : natural numbers
- morphisms $m \to n$: (sets of) mappings $[n] \to T^{PR}[m]$

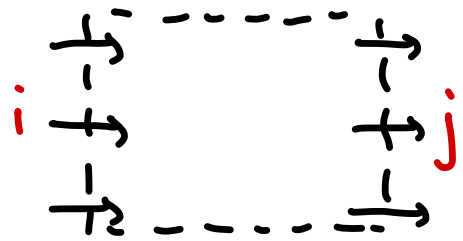
  where $T^{PR} X = \{ (p_x, r_x)_{x \in X} \mid \sum_{x \in X} p_x \leq 1, \forall x \in X.\ p_x \geq 0,\ p_x = 0 \Rightarrow r_x = 0 \}$

  - T^{PR}: probabilistic reward monad
  - p_x: probability
  - r_x: reward

Composition: $f : m \to n$, $g : n \to p$

- $p_{f;g}(i,k) = \sum_{j=1}^{m} p_f(i,j)\, p_g(j,k)$
- $r_{f;g}(i,k) = \sum_{j=1}^{m} r_f(i,j)\, p_g(j,k) + p_f(i,j)\, r_g(j,k)$

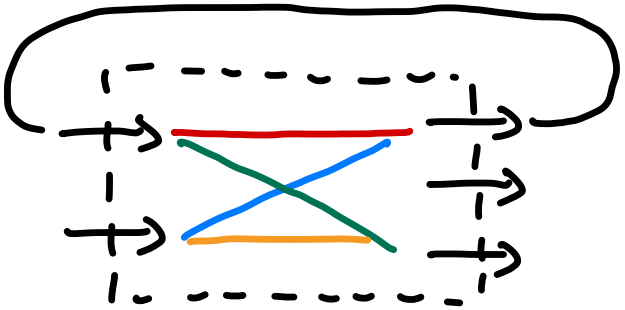
Trace in semantics



$$RP_f = \begin{bmatrix} p_f(1,1) & \cdots & p_f(1,m) \\ \vdots & p_f(i,j) & \vdots \\ p_f(n,1) & \cdots & p_f(n,m) \end{bmatrix}$$

(same for ER_f with $r_f(i,j)$)

$$\text{Trace} : (f : [p+n] \to [p+m]) \longmapsto (tr_p(f) : [n] \to [m])$$



$$RP_f = \left[\begin{array}{c|c} RP_{loop} & RP_{out} \\ \hline RP_{in} & RP_{through} \end{array}\right]$$

(same for ER_f)

$$RP_{tr_p(f)} = RP_{through} + \sum_{d \in \mathbb{N}} RP_{in}\, RP_{loop}^{\,d}\, RP_{out}$$

$$ER_{tr_p(f)} = ER_{through} + \sum_{d \in \mathbb{N}} \begin{bmatrix} RP_{in} & ER_{in} \end{bmatrix} \begin{bmatrix} RP_{loop} & ER_{loop} \\ 0 & RP_{loop} \end{bmatrix}^d \begin{bmatrix} ER_{out} \\ RP_{out} \end{bmatrix}$$

Lemma: $\mathbb{S}$ is a TSMC.

Trace in semantics

(observations by P.-A. Melliès and T. Seiller)

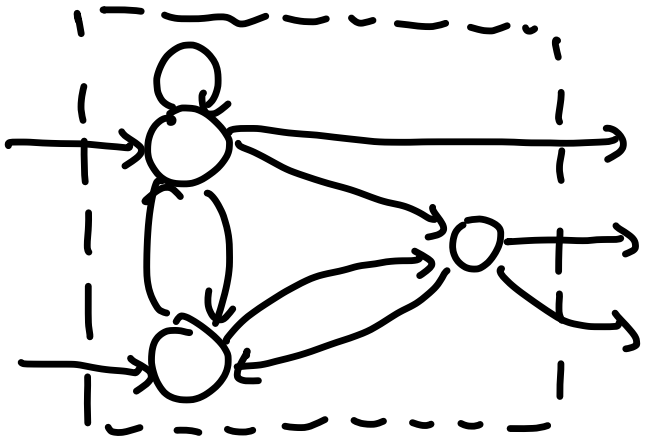
We can think of RP_f and ER_f as a single matrix of elements of $\mathbb{R}^2$.

$$\begin{pmatrix} t \\ n \end{pmatrix} + \begin{pmatrix} t' \\ n' \end{pmatrix} = \begin{pmatrix} t+t' \\ n+n' \end{pmatrix} \qquad \begin{pmatrix} t \\ n \end{pmatrix} \cdot \begin{pmatrix} t' \\ n' \end{pmatrix} = \begin{pmatrix} tt' \\ tn' + t'n \end{pmatrix}$$

$$R_f = \begin{bmatrix} \begin{pmatrix} p_f(1,1) \\ r_f(1,1) \end{pmatrix} & \cdots & \begin{pmatrix} p_f(1,m) \\ r_f(1,m) \end{pmatrix} \\ \vdots & & \vdots \\ \begin{pmatrix} p_f(n,1) \\ r_f(n,1) \end{pmatrix} & \cdots & \begin{pmatrix} p_f(n,m) \\ r_f(n,m) \end{pmatrix} \end{bmatrix} \qquad R_f = \left[\begin{array}{c|c} R_{loop} & R_{out} \\ \hline R_{in} & R_{through} \end{array}\right]$$

$$R_{tr(f)} = R_{through} + \sum_{d \in \mathbb{N}} R_{in}\, R_{loop}^{\,d}\, R_{out}$$

Interpretation of OMDPs



$\rightsquigarrow$ morphism $2 \to 3$ in $\$$

(i.e. a set of mappings $2 \to T^{PR} 3$)

$$[\![\mathcal{M}]\!](i,j) = \{(RP_\sigma(i,j), ER_\sigma(i,j)) \mid \sigma \text{ scheduler}\}$$

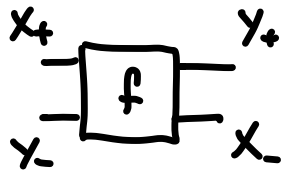
Lemma: $[\![-]\!]$ is a traced symmetric monoidal functor.

↳ We can compute expected rewards compositionally!

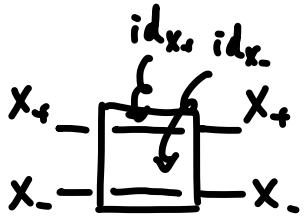
Bidirectionality and Int-construction

$\mathrm{Int}(\mathbb{C})$: - objects : (X_+, X_-) where X_+, X_- objects of $\mathbb{C}$

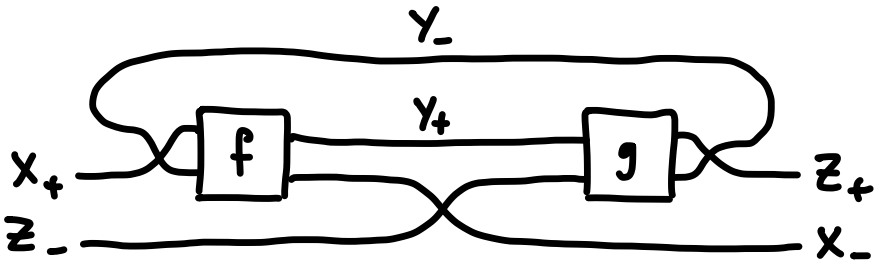
- morphisms $(X_+, X_-) \to (Y_+, Y_-) : f \in \mathbb{C}(X_+ \otimes Y_-, Y_+ \otimes X_-)$



identity on (X_+, X_-) : $id_{(X_+,X_-)} \triangleq id_{X_+ \otimes X_-}$



composition :



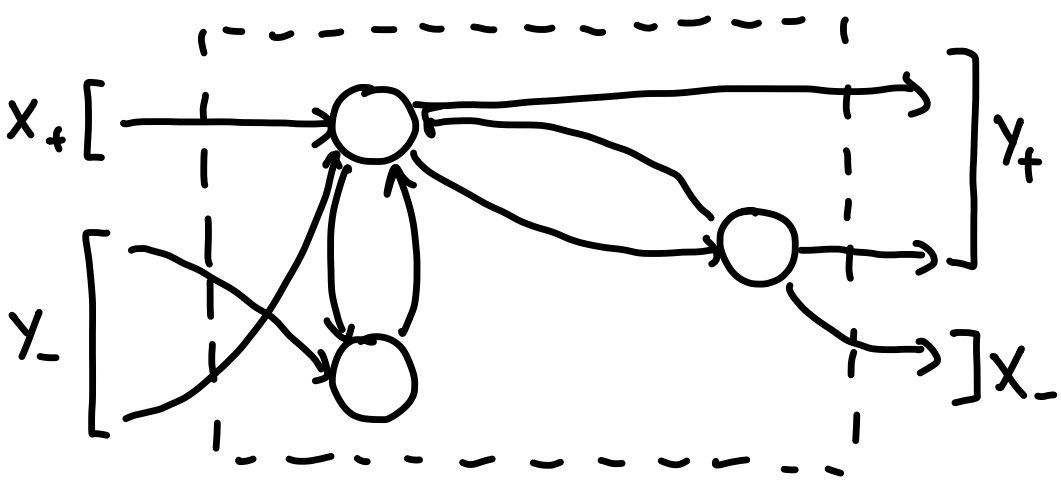
Lemma : $\mathrm{Int}(\mathbb{C})$ is compact closed.

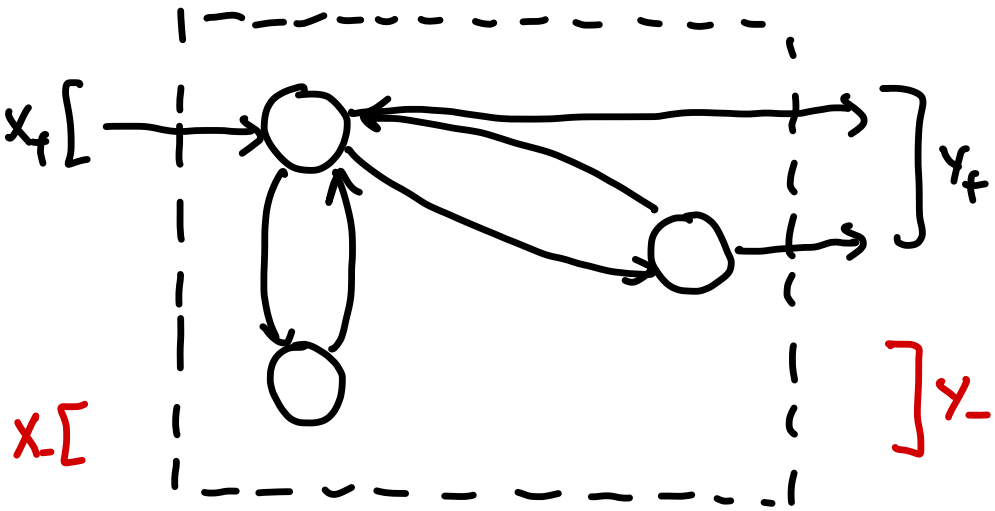
unit : $\eta_X : \mathrm{Int}(\mathbb{C})((I,I), (X_+, X_-) \otimes (X_-, X_+)) = \mathrm{Int}(\mathbb{C})((I,I), (X_+ \otimes X_-, X_+ \otimes X_-))$

$= \mathbb{C}(X_+ \otimes X_-, X_+ \otimes X_-)$

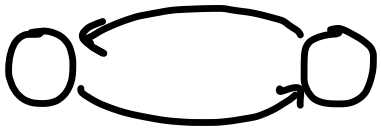
$\eta_X = id_{X_+ \otimes X_-}$

Int-construction : example

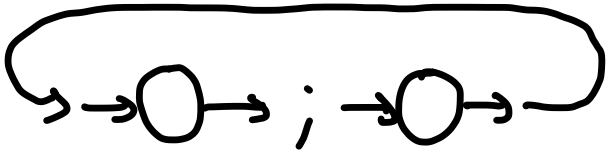




usefulness : ease of modelling



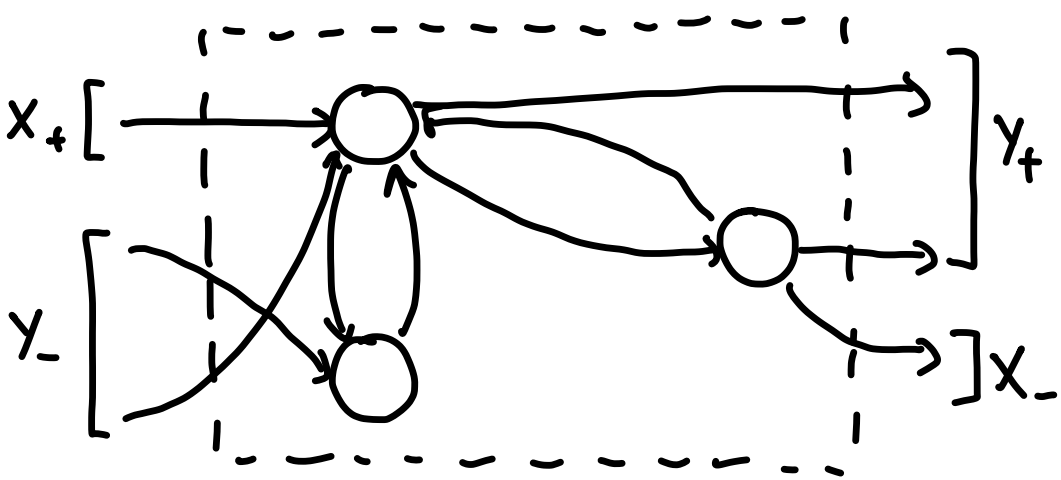
graph

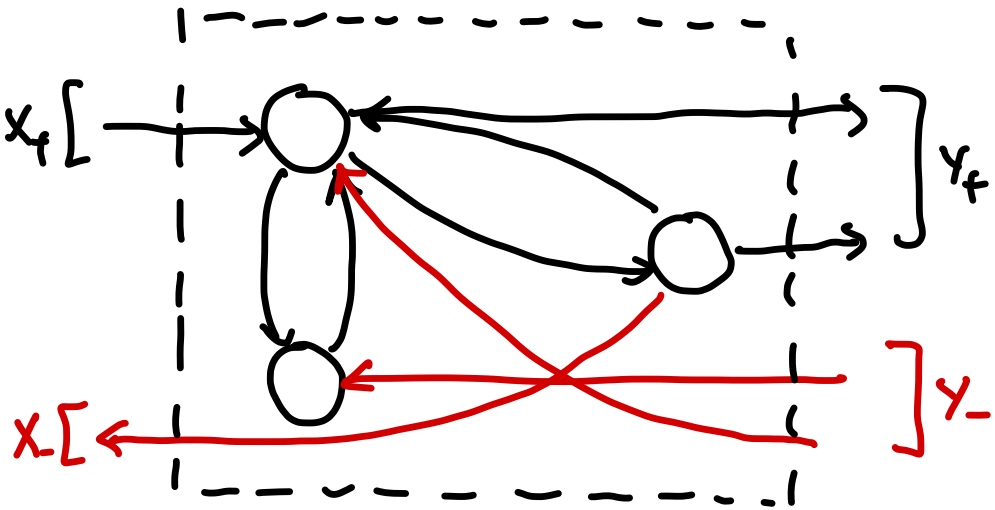


in TSMC

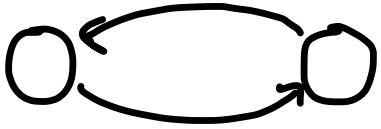
in CompCC

Int-construction : example

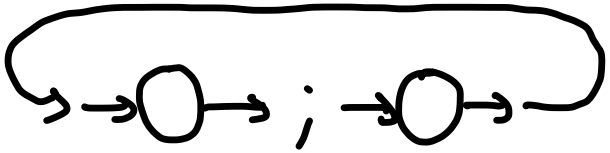




usefulness : ease of modelling



graph



in TSMC

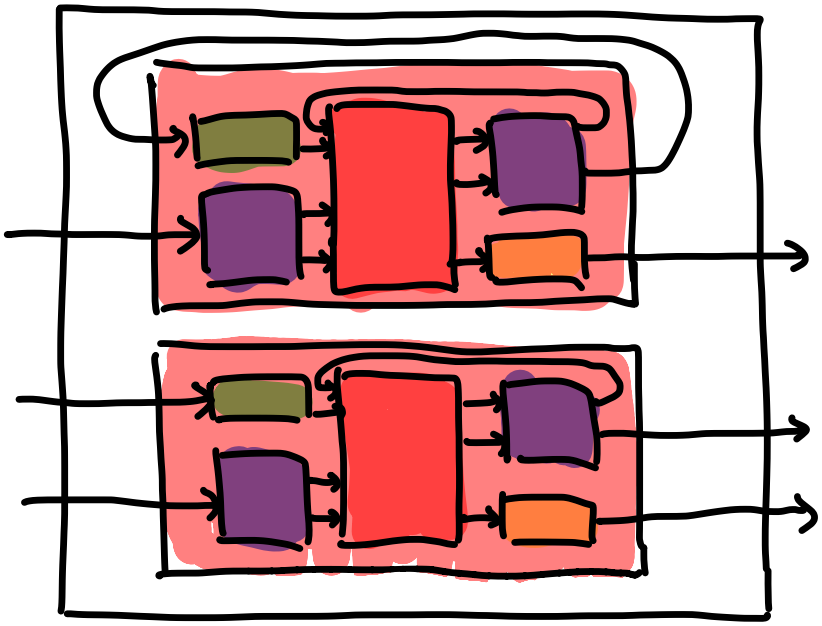
in CompCC

Algorithm

This work is published in CAV !

Algorithm to compute $[\![\mathcal{M}]\!]$:

- if $\mathcal{M} = \mathcal{M}_1 ; \mathcal{M}_2$ then $[\![\mathcal{M}]\!] = [\![\mathcal{M}_1]\!] ; [\![\mathcal{M}_2]\!]$
  (idem if $\mathcal{M} = tr_p(\mathcal{M}') \ldots$)
- if $\mathcal{M}$ is a single state, computing $[\![\mathcal{M}]\!]$ is trivial



Our algorithm:

- beats state of the art when there is repetition
- performance increases with degree of repetition
- cannot handle large interfaces in practice

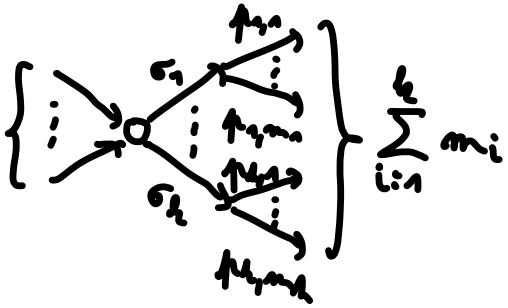
Free Syntax

Formally, open MDPs are <u>equivalence classes</u> of (n, m, Q, E, P, R)

↳ not so nice to reason about or program on.

Also, would be nice to reason with universal properties.

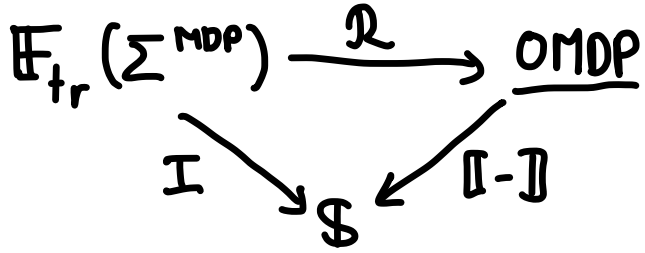
Free syntax : $\mathbb{F}_{tr}(\Sigma^{MDP})$ with $\Sigma^{MDP} = \{(n, n, ((\mu_{\sigma_{1,1}}, \dots, \mu_{\sigma_{1,m_1}}), \dots (\mu_{\sigma_{k,1}}, \dots, \mu_{\sigma_{k,m_k}})) : n \to \sum_{i=1}^{k} m_i\}$

$(n, n, ((\mu_{\sigma_{1,1}}, \dots), \dots, (\mu_{\sigma_{k,1}}, \dots))) \hookrightarrow$ 

Realisation functor : $\mathcal{R} : \mathbb{F}_{tr}(\Sigma^{MDP}) \to$ <u>OMDP</u>

<u>Lemma</u> : $\mathcal{R}$ is full.

Algorithm (in depth)



$\mathcal{I}, \mathcal{R}$: defined inductively (by universal property)

Lemma. $[\![-]\!] \circ \mathcal{R} = \mathcal{I}$.

Algo :

Data : a morphism $f : m \to n$ in $\mathbb{F}_{tr}(\Sigma^{MDP})$ (actually not exact)

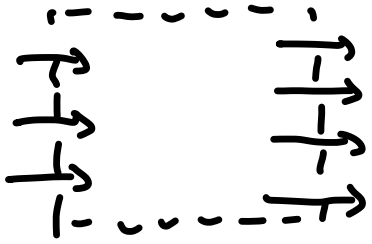
Returns : $\mathcal{I}(f)$

if $(f = f_1 ; f_2)$ { return $\mathcal{I}(f_1) ; \mathcal{I}(f_2)$ }
elif $(f = f_1 \otimes f_2)$ { return $\mathcal{I}(f_1) \otimes \mathcal{I}(f_2)$ }
elif $(f = Tr(f'))$ { return $Tr(\mathcal{I}(f'))$ }
elif (f generator) {enumerate all schedulers}

- inductive on structure of f
- can be done while remembering $\mathcal{I}(g)$ for sob-MDPs

New heuristics from compositionality

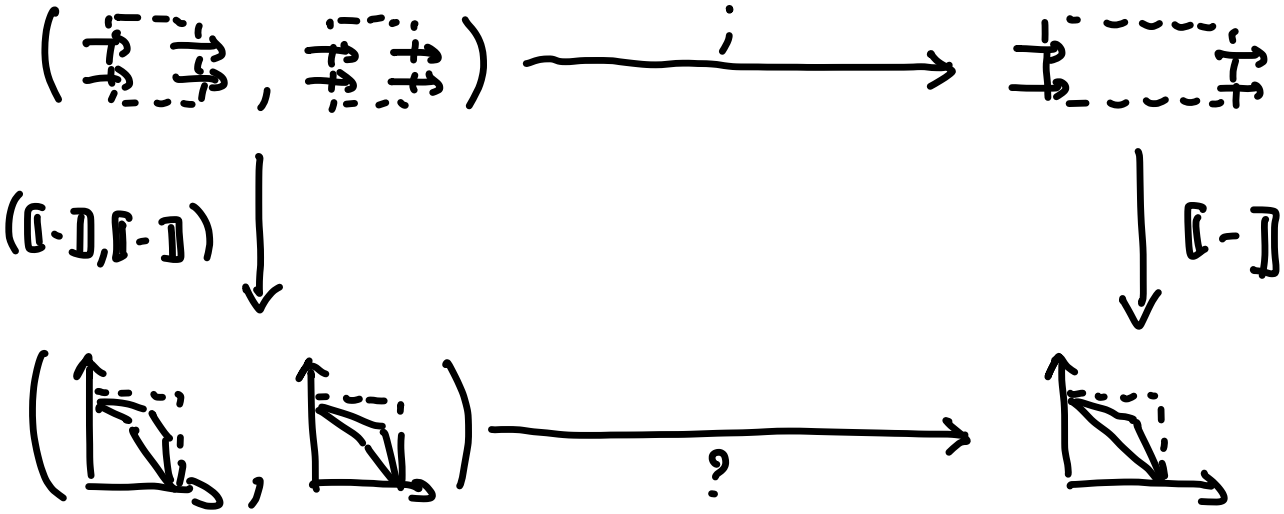
Our algorithm is inefficient on large interfaces.



Why: scheduler potentially optimal if for all other schedulers, it reaches at least one exit with higher probability / reward.
⇒ number increases exponentially with number of exits.

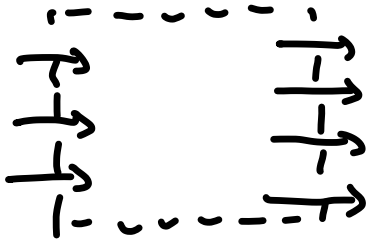
Watanabe, van der Vegt, Hasuo, Rot, Junges. Pareto Curves for Compositionally Model Checking String Diagrams of MDPs.

↳ give a sound heuristic to approximate maximal reachability probability.



New heuristics from compositionality

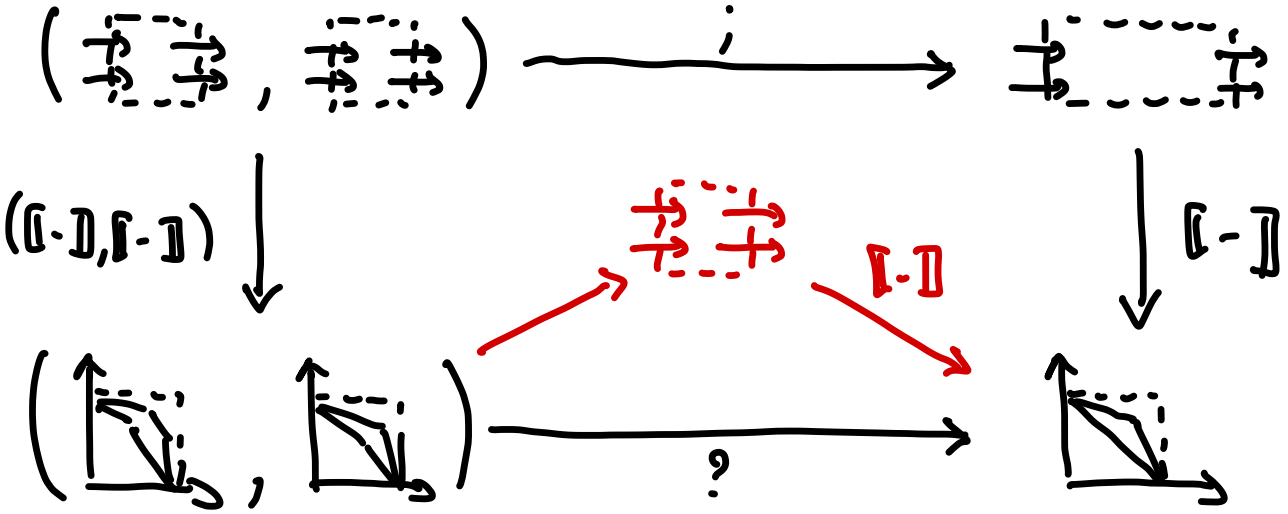
Our algorithm is inefficient on large interfaces.



Why: scheduler potentially optimal if for all other schedulers, it reaches at least one exit with higher probability / reward.
⇒ number increases exponentially with number of exits.

Watanabe, van der Vegt, Hasuo, Rot, Junges. Pareto Curves for Compositionally Model Checking String Diagrams of MDPs.

↳ give a sound heuristic to approximate maximal reachability probability.



If you're interested

- Watanabe, E., Asada, Hasuo. A Compositional Approach to Parity Games. MFPS '21.
  ↳ best account of the categorical techniques used in our approach (arXiv version has appendices)

- Watanabe, E., Asada, Hasuo. Compositional Probabilistic Model Checking with String Diagrams of MDPs. CAV '23.
  ↳ gives algorithm and experimental results
- Watanabe, E., Asada, Hasuo. Compositional Solution of Mean Payoff Games by String Diagrams.
  ↳ develops a "meager semantics"
- Watanabe, van der Vegt, Hasuo, Rot, Junges. Pareto Curves for Compositionally Model Checking String Diagrams of MDPs. TACAS '24.
  ↳ develops a sound heuristic based on compositionality
- Lechenne, E., Hasuo. A Compositional Approach to Petri Nets. CMCS '24
  ↳ interesting case of Petri nets

Conclusion

categorical side

$\rightsquigarrow$ morphism $2 \to 3$ in $\mathbb{S}$

semantics

algorithmic side

We get a nice algorithm from a categorical approach.

Future work

- general framework for compositional syntax
- general framework for semantics of compositional systems (based on open coalgebras)