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]

SOKENDAI NII ERATO MMSD JFLI Japanese-French Laboratory for Informatics

Category Theory for Compositional ~~Verification~~ ~~Models~~ Markov Decision Processes

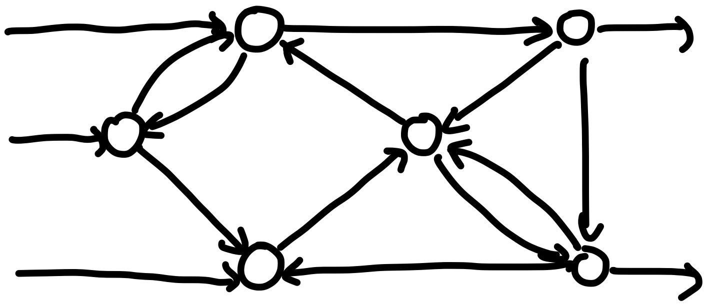
Kazuki Watanabe[1,2]
Clovis Eberhart[2,3]
Kazuyuki Asada[4]
Ichiro Hasuo[1,2]

SOKENDAI NII ERATO MMSD JFLI Japanese-French Laboratory for Informatics

Plan

categorical side

syntax



semantics

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

(+ bidirectional setting)

---

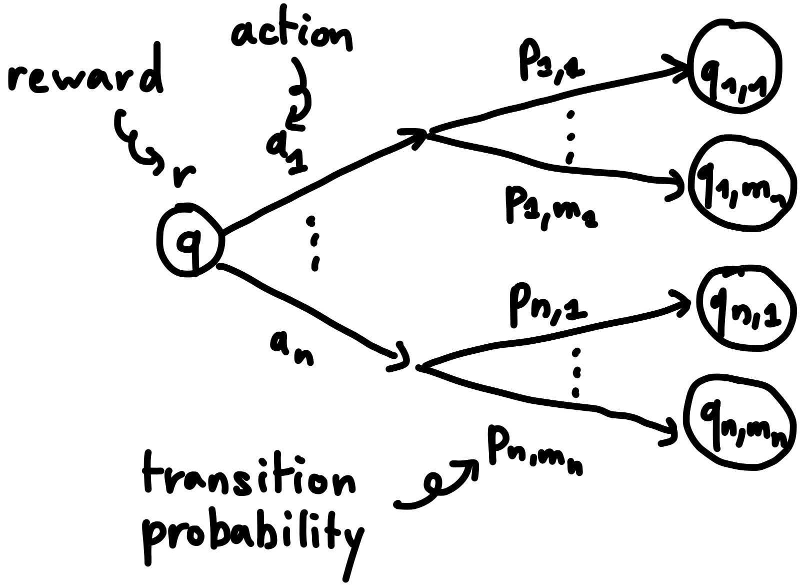
algorithmic side

We get a nice algorithm from a categorical approach.

(+ free syntax)

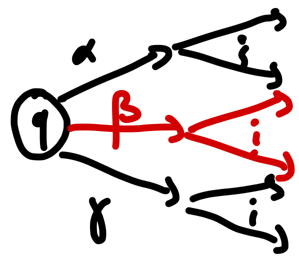
Markov Decision Processes

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



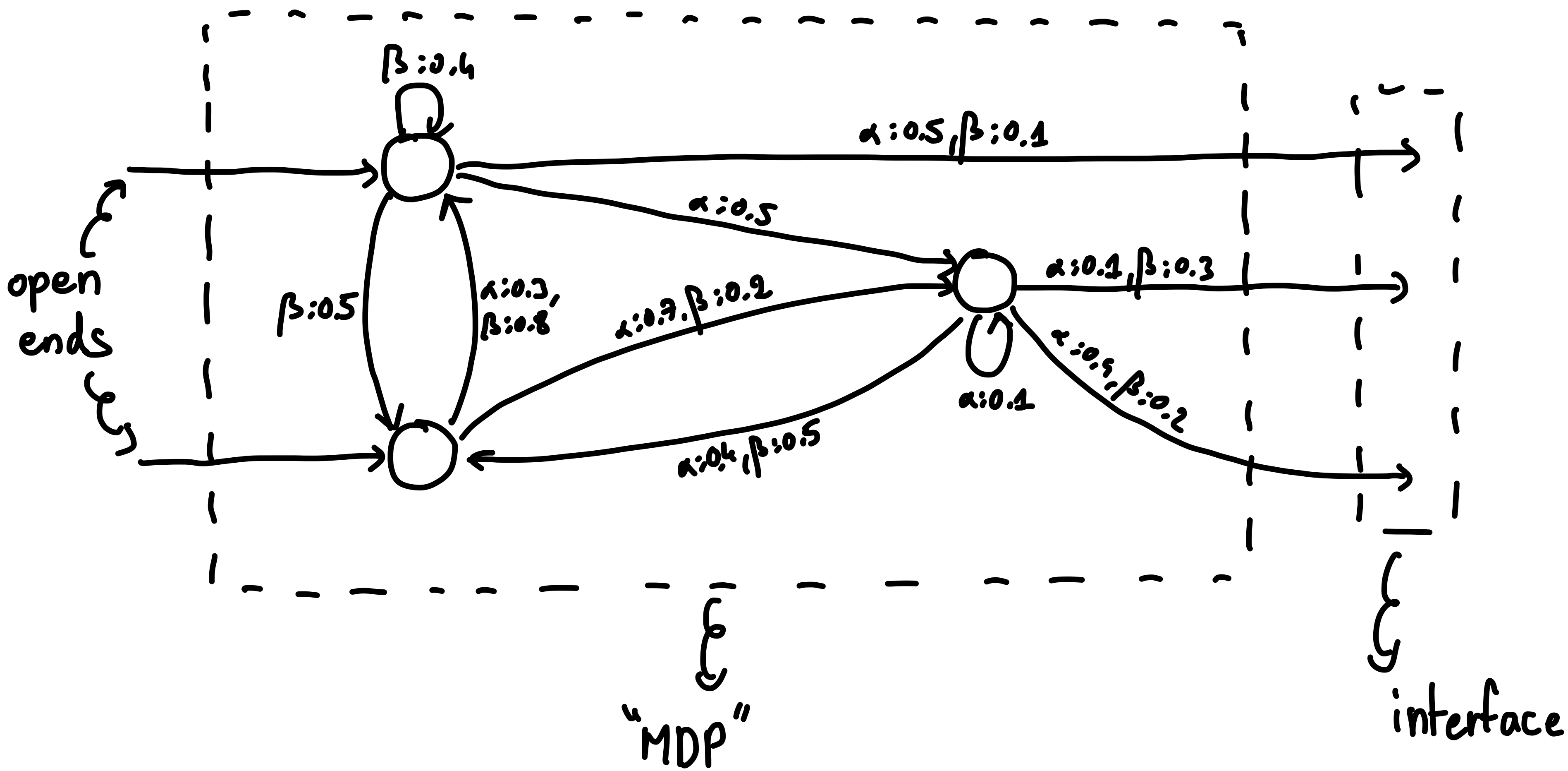
(coalgebras
$X \to (\mathcal{D}_{\leq 1} X)^{\Sigma} \times \mathbb{Q}$
(where $\Sigma = \{a_1, \dots, a_n\}$))

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



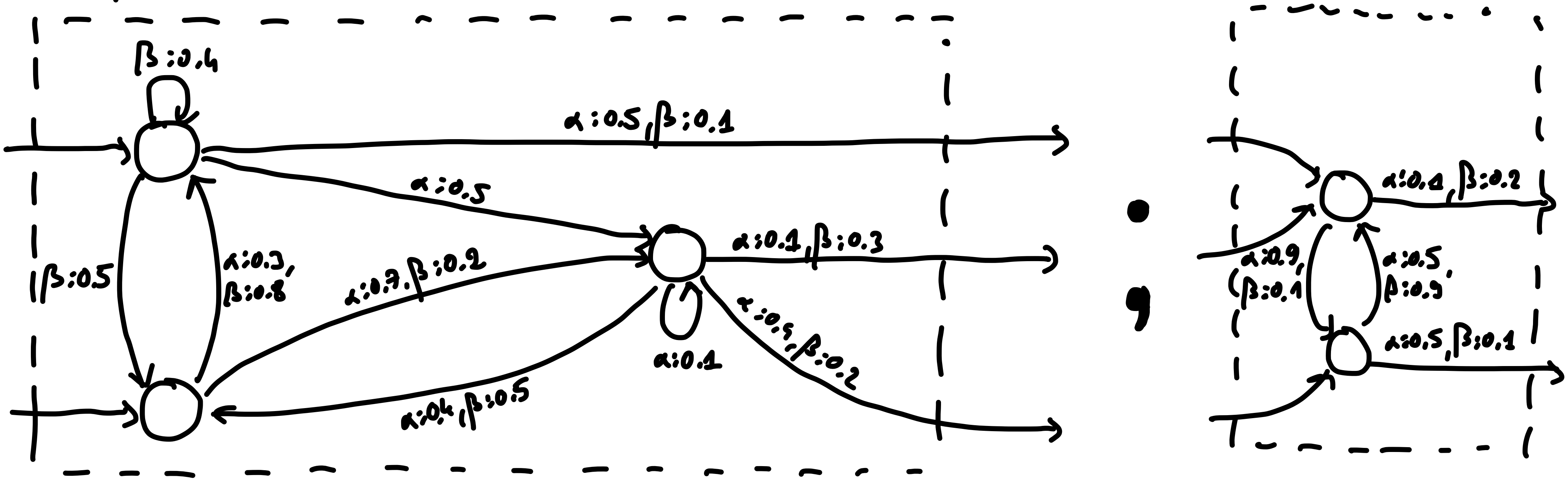
Problem: given $\mathcal{M}, q_i, q_f$, find the maximum expected reward from q_i to q_f.

Open MDPs

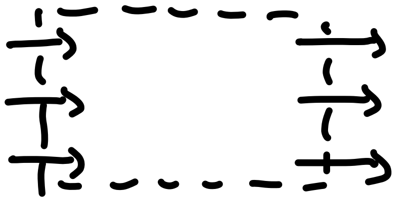

β:0.4
α:0.5, β:0.1
α:0.5
β:0.5
α:0.3, β:0.8
α:0.7, β:0.2
α:0.1, β:0.3
α:0.1
α:0.9, β:0.2
α:0.4, β:0.5
open ends
"MDP"
interface

Composition of OMDPs

composition:



identities:

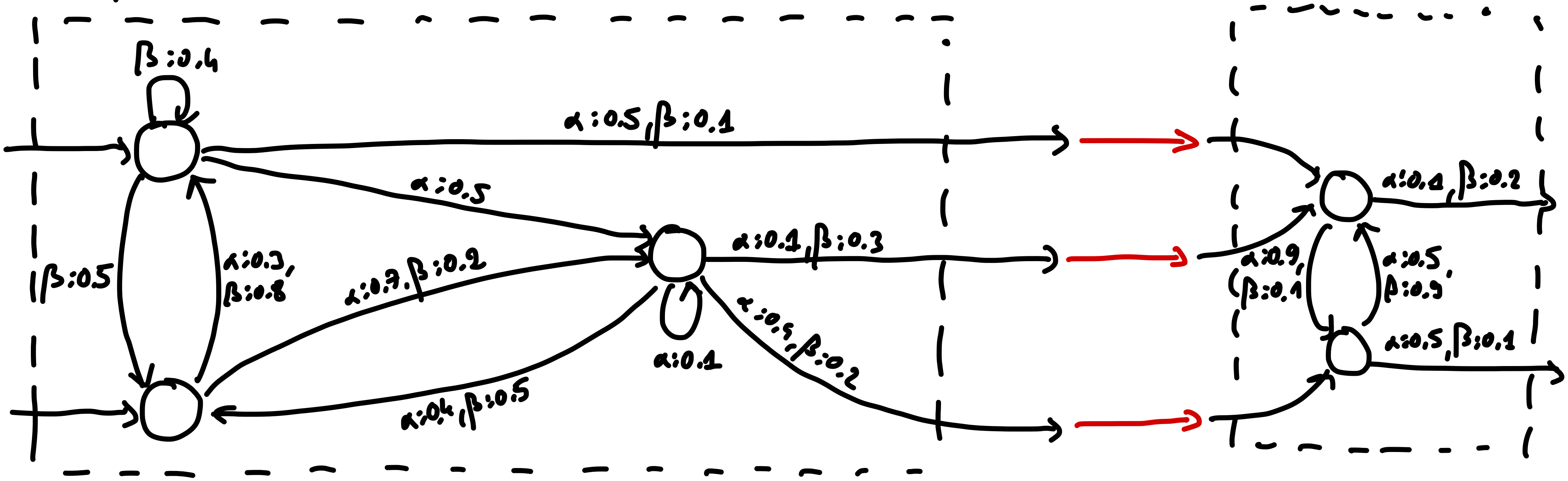


Lemma: OMDP ; - objects : natural numbers
- morphisms $m \to n$: OMDPs with m (n) open ends on the left (right)

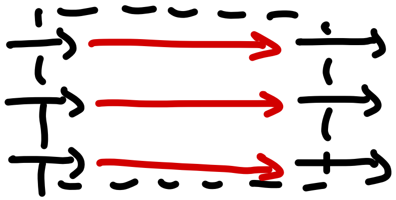
forms a category.

Composition of OMDPs

composition:



identities:

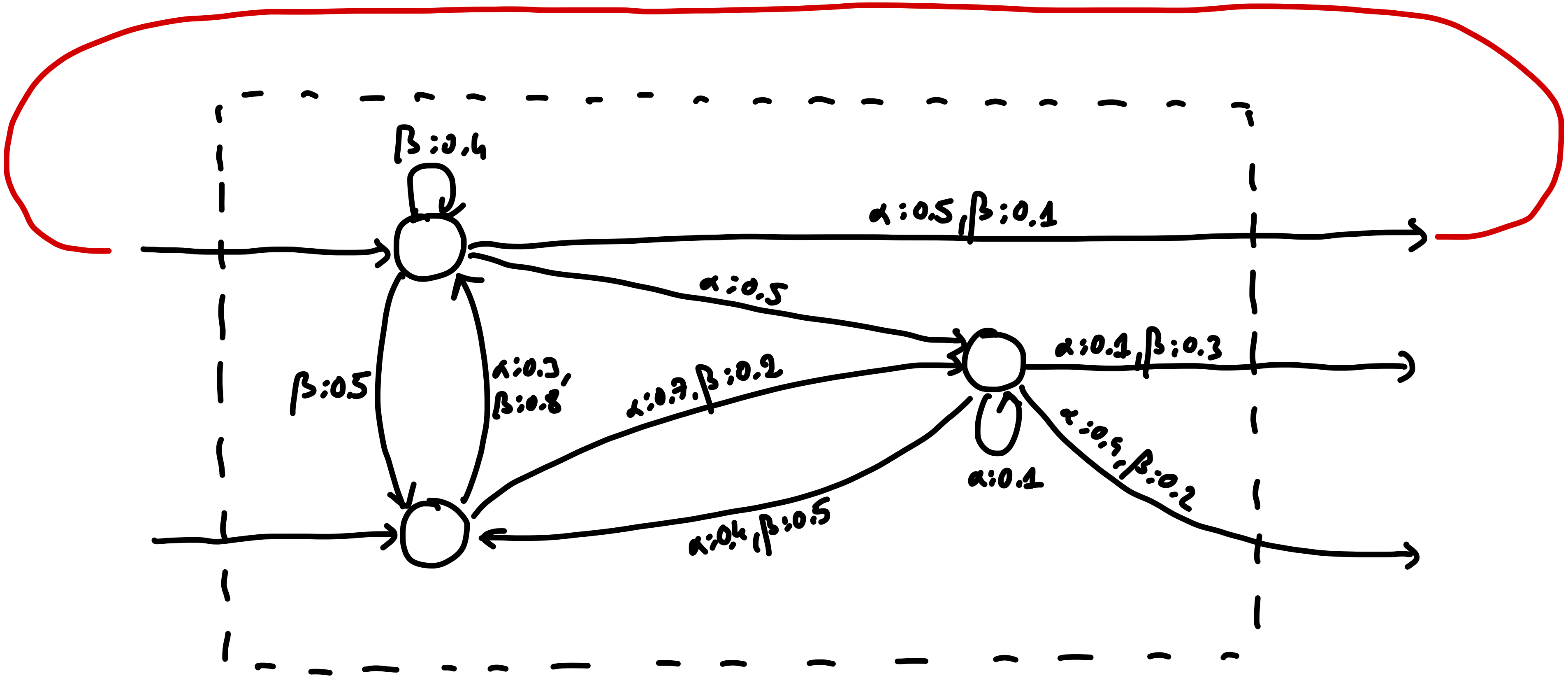


Lemma: OMDP: - objects: natural numbers

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

forms a category.

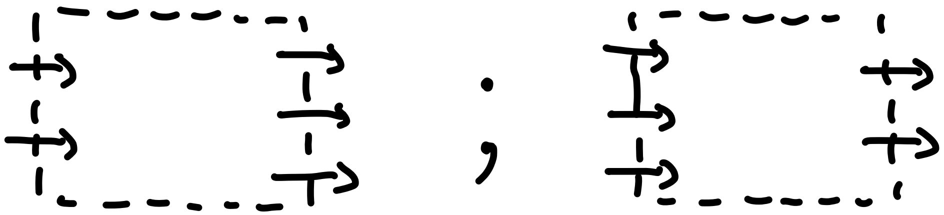
Trace of OMDPs



<u>Lemma</u>: <u>OMDP</u> 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: $RP_{\mathcal{A}_l;\mathcal{A}_r}(i,k) = \sum_{j=1}^{n} RP_{\mathcal{A}_l}(i,j)\, RP_{\mathcal{A}_r}(j,k)$

Expected reward: $ER_{\mathcal{A}_l;\mathcal{A}_r}(i,k) = \sum_{j=1}^{n} ER_{\mathcal{A}_l}(i,j)\, RP_{\mathcal{A}_r}(j,k) + RP_{\mathcal{A}_l}(i,j)\, ER_{\mathcal{A}_r}(j,k)$

To compute expected rewards compositionally, we need to know:

- expected rewards
- reachability probabilities

Semantic Category for OMDPs

Definition of $\mathbb{S}$:

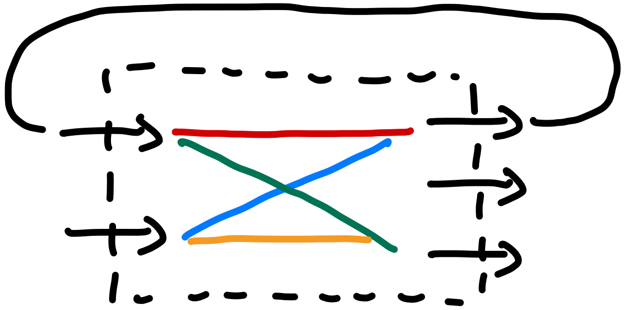
- objects : natural numbers
- morphisms $m \to n$: (sets of) mappings $[n] \to T^{PR}[m]$
  where $\underbrace{T^{PR}}_{\text{probabilistic reward monad}} X = \{ (\underbrace{p_x}_{\text{probability}}, \underbrace{r_x}_{\text{reward}})_{x \in X} \mid \sum_{x \in X} p_x \leq 1, \forall x \in X.\ p_x \geq 0,\ p_x = 0 \Rightarrow r_x = 0 \}$

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

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



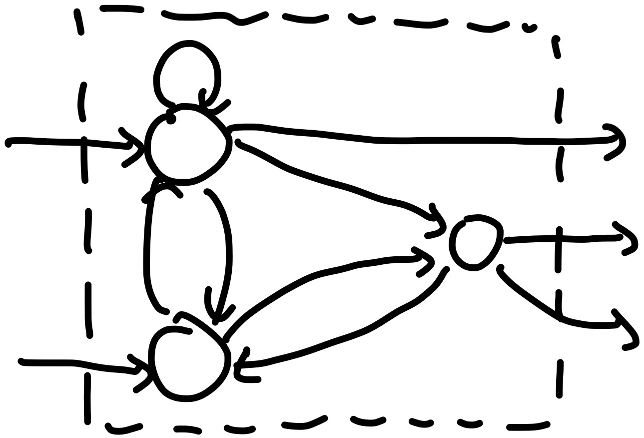
$$RP_f = \left[\begin{array}{c|c} RP_{loop} & RP_{out} \\ \hline RP_{in} & RP_{through} \end{array}\right] \quad \left(\text{same for } ER_f\right)$$

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

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

$\boxed{\underline{\text{Lemma:}}\ \$ \text{ is a TSMC.}}$

Interpretation of OMDPs



$\rightsquigarrow$ morphism $2 \to 3$ in $\mathcal{S}$
(i.e. a set of mappings $2 \to T^{PR}\, 3$)

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

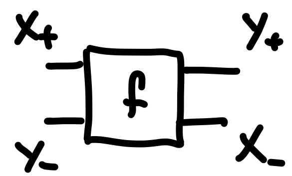
Lemma: $[\![-]\!]$ is a traced symmetric monoidal functor.

↳ We can compute expected rewards compositionally!

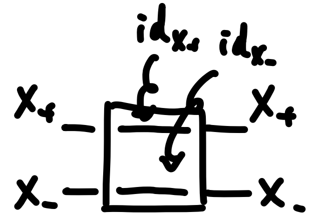
Bidirectionality and Int-construction

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

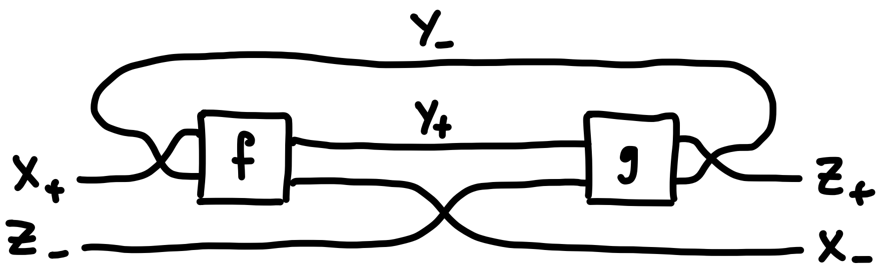
- morphisms $(X_+, X_-) \longrightarrow (Y_+, Y_-)$: $f \in \mathbb{C}(X_+ \otimes Y_-, Y_+ \otimes X_-)$



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



composition :



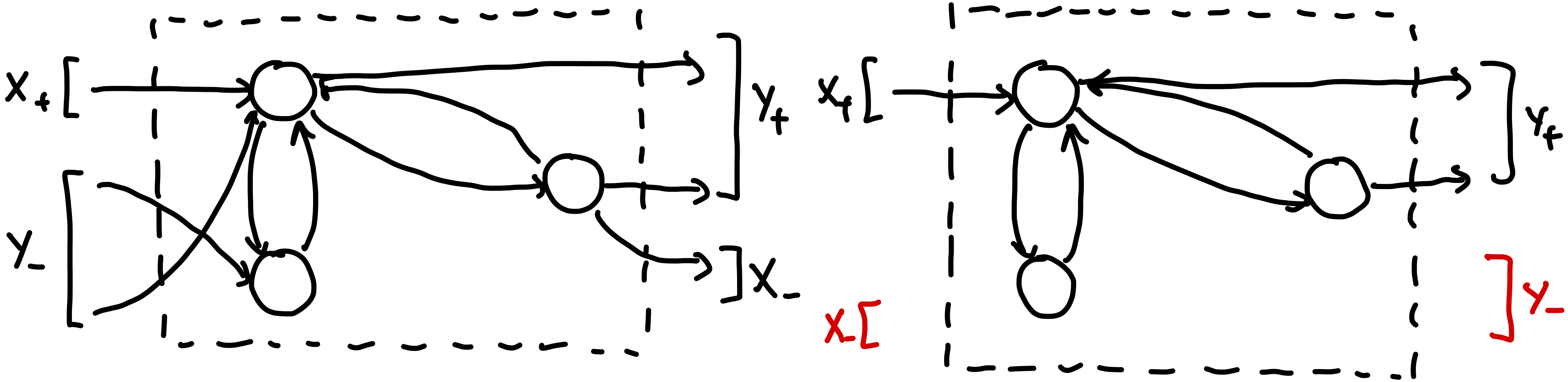
Lemma : $\mathrm{Int}(\mathbb{C})$ is compact closed.

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

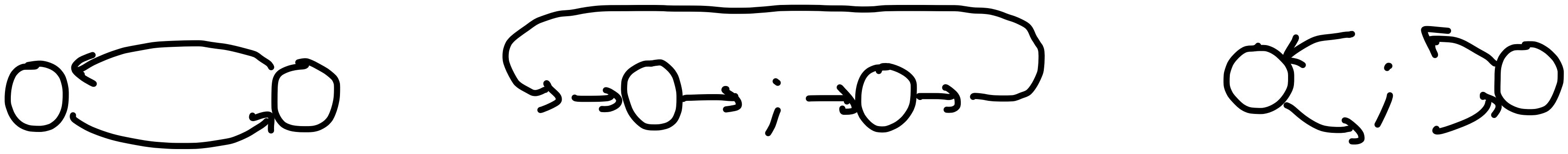
$= \mathbb{C}(X_+ \otimes X_-, X_+ \otimes X_-)$

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

Int-construction : example

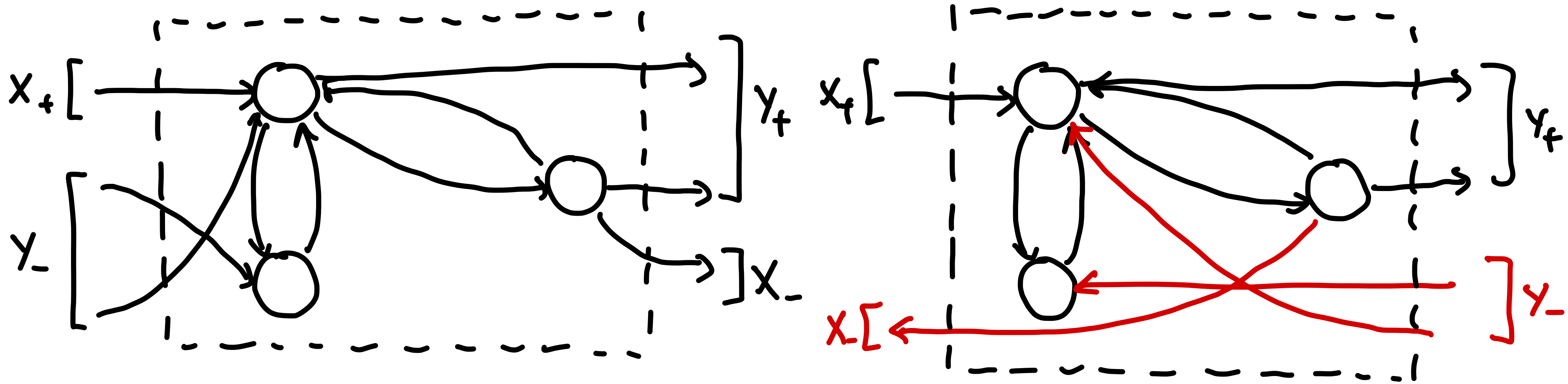


usefulness : ease of modelling

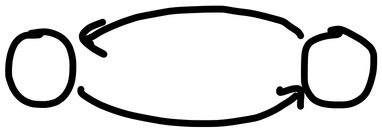


graph　　　　in TSMC　　　　in CompCC

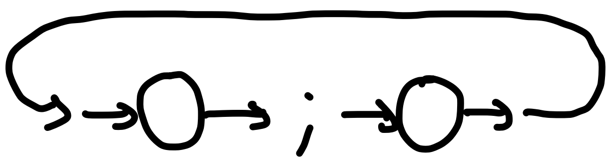
Int-construction: example



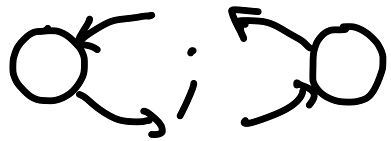
usefulness: ease of modelling



graph



in TSMC



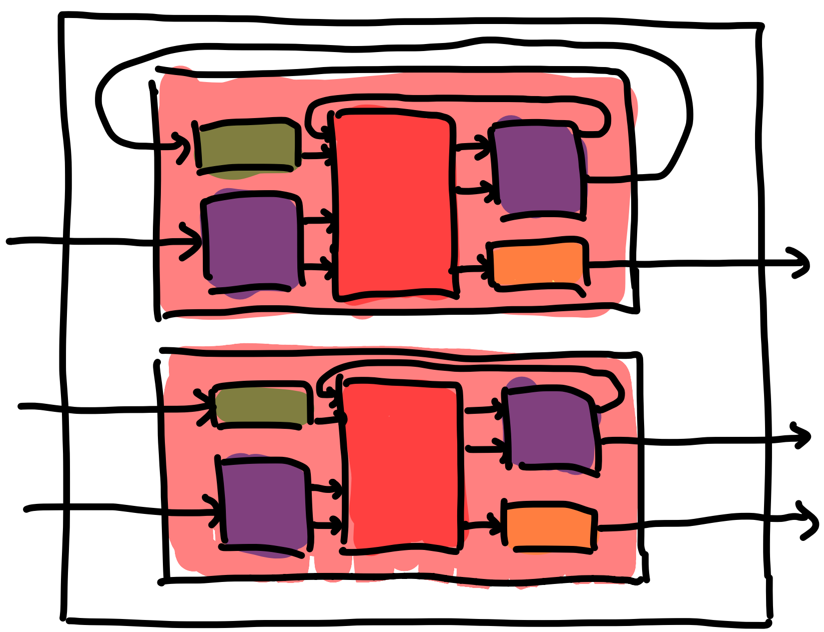
in CompCC

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 $\mathcal{M} = tr_p(\mathcal{M}') \dots$)
- 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

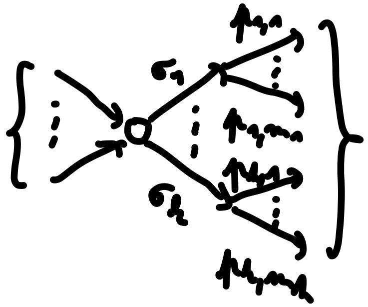
Free Syntax

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 $\Sigma^{MDP} = \{(n, k, ((p_{\sigma_1,1}, \dots, p_{\sigma_1,m_1}), \dots (p_{\sigma_k,1}, \dots, p_{\sigma_k,m_k}))) : n \to \sum_{i=1}^{k} m_i\}$

$(n, k, ((p_{\sigma_1,1}, \dots), \dots, (p_{\sigma_k,1}, \dots))) \leftrightsquigarrow$ n  $\sum_{i=1}^{k} m_i$

Realisation functor : $\mathcal{R} : \mathbb{F}_{tr}(\Sigma^{MDP}) \longrightarrow \underline{\mathbf{OMDP}}$

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

Algorithm (in depth)

$$\begin{tikzcd}
\mathbb{F}_{tr}(\Sigma^{MDP}) \arrow[rr, "\mathcal{R}"] \arrow[dr, "\mathcal{I}"'] & & \underline{OMDP} \arrow[dl, "[\![-]\!]"] \\
& \mathbb{S} &
\end{tikzcd}$$

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

<u>Lemma</u>. $[\![-]\!] \circ \mathcal{R} = \mathcal{I}$.

Algo :

actually not exact

Data : a morphism $f : m \to n$ in $\mathbb{F}_{tr}(\Sigma^{MDP})$

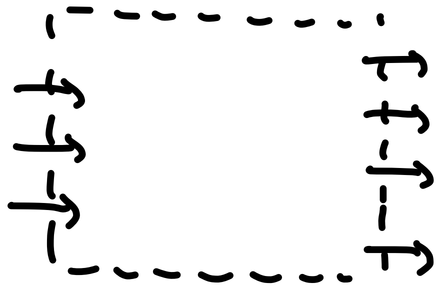
Returns: $\mathcal{I}(f)$

```
if (f = f_1 ; f_2) { return I(f_1) ; I(f_2) }
elif (f = f_1 ⊗ f_2) { return I(f_1) ⊗ I(f_2) }
elif (f = Tr(f')) { return Tr(I(f')) }
elif (f generator) { enumerate all schedulers }
```

- inductive on structure of f
- can be done while remembering $\mathcal{I}(g)$ for sub-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.
↳ TACAS, Wednesday, 15:00

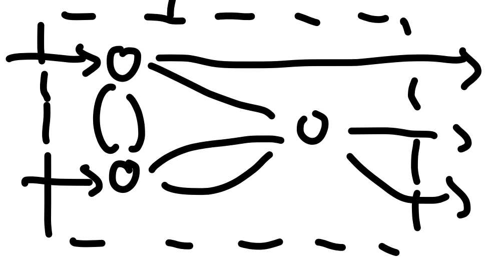
If you're interested

- Watanabe, E., Asada, Hasuo. <u>A Compositional Approach to Parity Games.</u> MFPS '21.
  ↳ best account of the categorical techniques used in our approach (arXiv version has appendices)
- Watanabe, E., Asada, Hasuo. <u>Compositional Probabilistic Model Checking with String Diagrams of MDPs.</u> CAV '23.
  ↳ gives algorithm and experimental results
- Watanabe, E., Asada, Hasuo. <u>Compositional Solution of Mean Payoff Games by String Diagrams.</u>
  ↳ develops a "meager semantics"
- Watanabe, van der Vegt, Hasuo, Rot, Junges. <u>Pareto Curves for Compositionally Model Checking String Diagrams of MDPs.</u> TACAS '24.
  ↳ develops a sound heuristic based on compositionality
- Lechenne, E., Hasuo. <u>A Compositional Approach to Petri Nets.</u> CMCS '24
  ↳ interesting case of Petri nets

Conclusion

categorical side

syntax



$\rightsquigarrow$

semantics

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

algorithmic side

We get a nice algorithm from a categorical approach.

Related work

- open parity games [Watanabe+, MFPS'21]
- efficient heuristics for OMDPs [Watanabe+, TACAS'24]
- open Petri nets [Lechenne+, CMCS'24]