Probabilistic Verification via Category Theory: Categorical Generalization of Fair Simulation and Ranking Function by Kleisli Coalgebras, and Its Concretization

圏論による確率的検証：
クライスリ圏の余代数による
公平模倣とランキング関数の圏論的一般化と具体化

1月31日, 2019 PhD thesis presentation

48-167101 小林研究室 卜部夏木

These slides are available on http://group-mmm.org/~nurabe/slides/doctor_final_printing.pdf (search with “Natsuki Urabe”)

Outline

- Overview
- Short Preliminaries on Category Theory
- Categorical Trace Semantics for Büchi and Parity Automata
  (Chapter 3, [U., Shimizu & Hasuo, CONCUR ’16] [U., & Hasuo, CMCS ’18])
- Categorical Fair Simulation (Chapter 4, [U. & Hasuo, LMCS ’17])
- Categorical Ranking Function (Chapter 5, [U., Hara & Hasuo, LICS ’17])
- γ-Scaled Submartingale for Probabilistic Programs and its Synthesis
  (Chapter 6, [Takisaka, Oyabu, U. & Hasuo, ATVA ‘18])
- Conclusion

Goal

- Verification method for **probabilistic** systems

- Verification of nonprobabilistic systems
  - prove a given (non)deterministic system satisfies a qualitative property
  - Example:

  Q. Does the program terminate?

```
x := 10;
while x > 0 {
  if input()=0
    x := x - 1
  else
    x := x + 1
}
```

- Verification of probabilistic systems
  - prove a given probabilistic system satisfies a qualitative property, or
  - prove a given probabilistic system satisfies a quantitative property
  - more difficult than qualitative verification
  - Example:

  Q. Does the program terminate in probability 1?
  Q. In what probability does the program terminate?

```
x := 10;
while x > 0 {
  if prob(0.25)
    x := x - 1
  else
    x := x + 1
}
```

Category Theory and Coalgebra

(see e.g. [Mac Lane, 1971])

- Category theory
  - An abstract and general mathematical theory
  - Theory of **structures** regarding “objects” and “arrows” between them

$$c : X \to \mathcal{P}X$$ **(nondeterministic program)**

$(\mathcal{P}X := \{A \subseteq X\})$

$$c : X \to \mathcal{D}X$$ **(probabilistic program)**

$(\mathcal{D}X := \{d : X \to [0,1] \mid \forall x.\, 0 \leq d(x), 0 \leq \sum_x d(x)\})$

an arrow

$$c : X \to FX$$

- Coalgebra
  - An arrow of a form $X \xrightarrow{c} FX$
  - Model of various transition systems

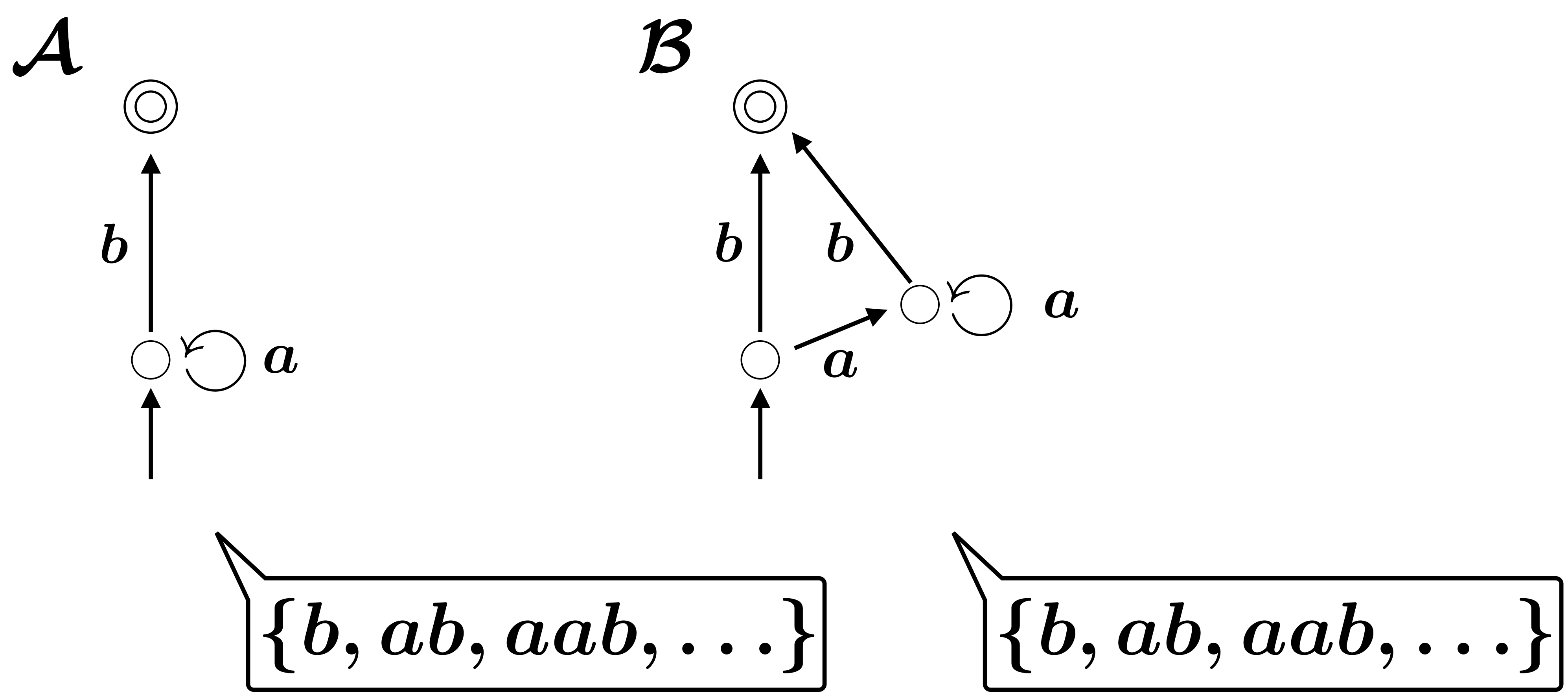
    Example:

    Nondeterministic automaton, Probabilistic automaton, etc…

Example: Bisimulation (see e.g. [Baier & Katoen])

- For proving equivalence between transition systems

- Example:

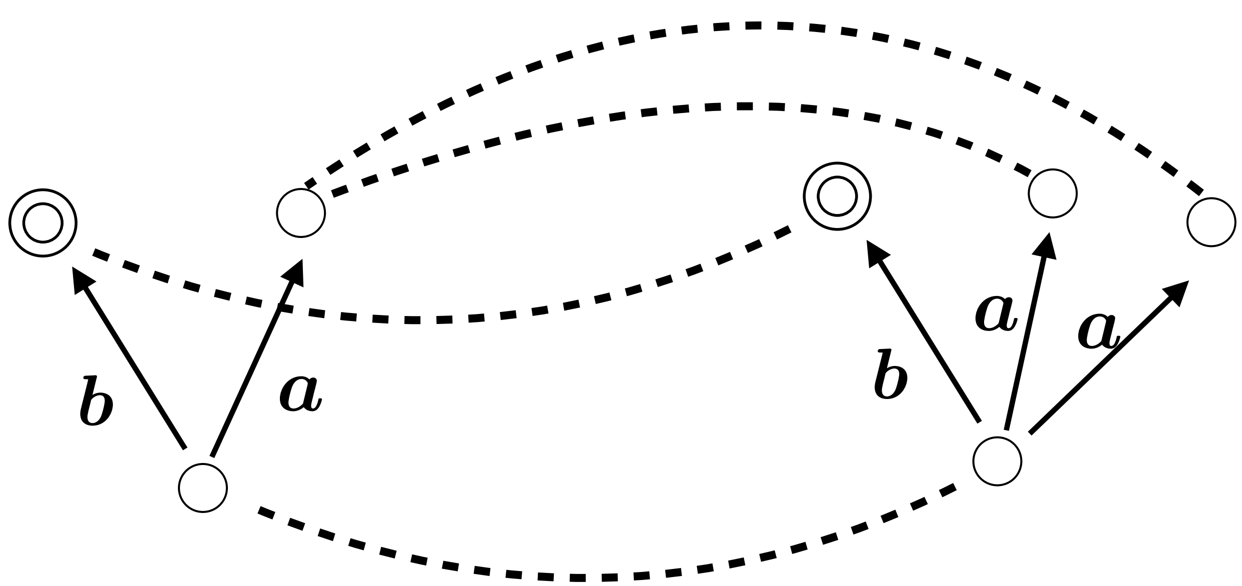


Example: Bisimulation (see e.g. [Baier & Katoen])

Definition

A *bisimulation* from $\mathcal{A}$ to $\mathcal{B}$ is a relation $R \subseteq X \times Y$ between the state spaces such that:

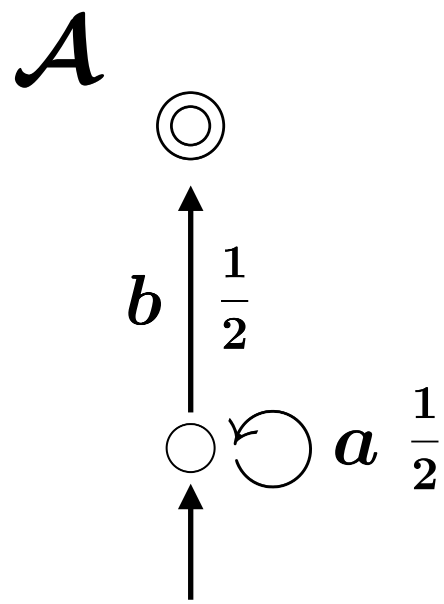
- xRy and $x \xrightarrow{a} x' \;\Rightarrow\; \exists y'.\, y \xrightarrow{a} y'$ and $x'Ry'$
- xRy and $y \xrightarrow{a} y' \;\Rightarrow\; \exists x'.\, x \xrightarrow{a} x'$ and $x'Ry'$
- $xRy \;\Rightarrow\; \big(x : \circledcirc \Leftrightarrow y : \circledcirc\big)$



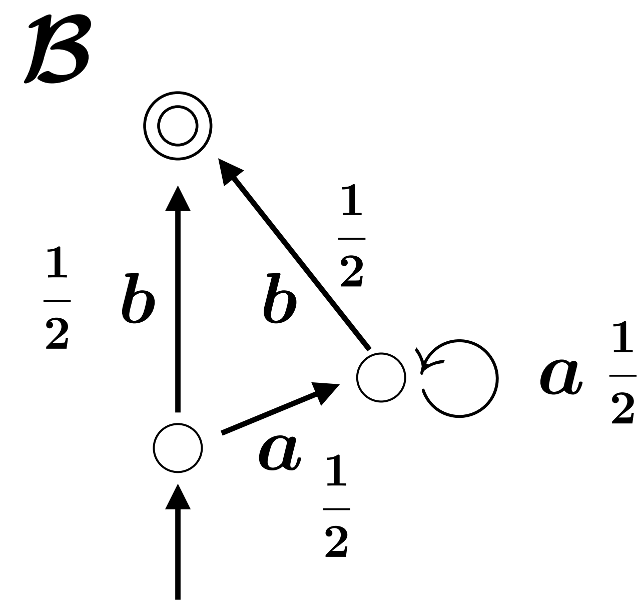
- Bisimulation implies equivalence (**soundness**)

Bisimulation for Probabilistic Systems?

$\mathcal{A}$



$\mathcal{B}$



$$\begin{bmatrix} b \mapsto \frac{1}{2} \\ ab \mapsto \frac{1}{4} \\ aab \mapsto \frac{1}{8} \\ \vdots \end{bmatrix}$$

$$\begin{bmatrix} b \mapsto \frac{1}{2} \\ ab \mapsto \frac{1}{4} \\ aab \mapsto \frac{1}{8} \\ \vdots \end{bmatrix}$$

Probabilistic Bisimulation (see e.g. [Baier & Katoen])

Definition

For $\boldsymbol{R} \subseteq \boldsymbol{X} \times \boldsymbol{Y}$, we define $\overline{\boldsymbol{R}} \subseteq [\mathbf{0},\mathbf{1}]^{\boldsymbol{X}} \times [\mathbf{0},\mathbf{1}]^{\boldsymbol{Y}}$ by:

$$\boldsymbol{d}\overline{\boldsymbol{R}}\boldsymbol{d}' \;\Leftrightarrow\; \exists \boldsymbol{f} : \boldsymbol{X} \times \boldsymbol{Y} \to [\mathbf{0},\mathbf{1}].\; \begin{array}{l} \sum_{y \in Y} f(x,y) = d(x) \\ \sum_{x \in X} f(x,y) = d'(y) \end{array}$$

Definition

A *probabilistic bisimulation* from $\mathcal{A}$ to $\mathcal{B}$ is a relation $\boldsymbol{R} \subseteq \boldsymbol{X} \times \boldsymbol{Y}$ between the state spaces such that:

- $\boldsymbol{xRy}$ and $\boldsymbol{x} \xrightarrow{\boldsymbol{a}} \boldsymbol{d} \;\Rightarrow\; \exists \boldsymbol{d}'.\, \boldsymbol{y} \xrightarrow{\boldsymbol{a}} \boldsymbol{d}'$ and $\boldsymbol{d}\overline{\boldsymbol{R}}\boldsymbol{d}'$
- $\boldsymbol{xRy}$ and $\boldsymbol{y} \xrightarrow{\boldsymbol{a}} \boldsymbol{d}' \;\Rightarrow\; \exists \boldsymbol{d}.\, \boldsymbol{x} \xrightarrow{\boldsymbol{a}} \boldsymbol{d}$ and $\boldsymbol{d}\overline{\boldsymbol{R}}\boldsymbol{d}'$
- $\boldsymbol{xRy} \;\Rightarrow\; \big(\boldsymbol{x} : \circledcirc \;\Leftrightarrow\; \boldsymbol{y} : \circledcirc\big)$

- Bisimulation implies equivalence

Comparison

nondeterministic

Definition

A *bisimulation* from $\mathcal{A}$ to $\mathcal{B}$ is a relation $R \subseteq X \times Y$ between the state spaces such that:

- xRy and $x \xrightarrow{a} x' \;\Rightarrow\; \exists y'.\, y \xrightarrow{a} y'$ and $x'Ry'$
- xRy and $y \xrightarrow{a} y' \;\Rightarrow\; \exists x'.\, x \xrightarrow{a} x'$ and $x'Ry'$
- $xRy \;\Rightarrow\; \left(x : \circledcirc \Leftrightarrow y : \circledcirc\right)$

probabilistic

Definition

A *probabilistic bisimulation* from $\mathcal{A}$ to $\mathcal{B}$ is a relation $R \subseteq X \times Y$ between the state spaces such that:

- xRy and $x \xrightarrow{a} d \;\Rightarrow\; \exists d'.\, y \xrightarrow{a} d'$ and $d\overline{R}d'$
- xRy and $y \xrightarrow{a} d' \;\Rightarrow\; \exists d.\, x \xrightarrow{a} d$ and $d\overline{R}d'$
- $xRy \;\Rightarrow\; \left(x : \circledcirc \Leftrightarrow y : \circledcirc\right)$

Comparison

nondeterministic

Definition

A *bisimulation* from $\mathcal{A}$ to $\mathcal{B}$ is a relation $R \subseteq X \times Y$ between the state spaces such that:

$$\exists r.\quad \begin{array}{ccccc} X^{\Sigma} \times \{0,1\} & \xleftarrow{\pi_1^{\Sigma} \times \mathrm{id}_{\{0,1\}}} & R^{\Sigma} \times \{0,1\} & \xrightarrow{\pi_2^{\Sigma} \times \mathrm{id}_{\{0,1\}}} & Y^{\Sigma} \times \{0,1\} \\ \uparrow c & = & \uparrow r & = & \uparrow d \\ X & \xleftarrow{\pi_1} & R & \xrightarrow{\pi_2} & Y \end{array}$$

probabilistic

Definition

A *probabilistic bisimulation* from $\mathcal{A}$ to $\mathcal{B}$ is a relation $R \subseteq X \times Y$ between the state spaces such that:

$$\exists r.\quad \begin{array}{ccccc} [0,1]^{X \times \Sigma} \times \{0,1\} & \leftarrow & [0,1]^{R \times \Sigma} \times \{0,1\} & \rightarrow & [0,1]^{Y \times \Sigma} \times \{0,1\} \\ \uparrow c & = & \uparrow r & = & \uparrow d \\ X & \xleftarrow{\pi_1} & R & \xrightarrow{\pi_2} & Y \end{array}$$

Unification (see e.g. [Jacobs, ’16])

nondeterministic bisimulation

$$\begin{tikzcd} X^{\Sigma}\times\{0,1\} & R^{\Sigma}\times\{0,1\} \arrow[l, "\pi_1^{\Sigma}\times \mathrm{id}_{\{0,1\}}"'] \arrow[r, "\pi_2^{\Sigma}\times \mathrm{id}_{\{0,1\}}"] & Y^{\Sigma}\times\{0,1\} \\ X \arrow[u, "c"] & R \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] \arrow[u, "r"] & Y \arrow[u, "d"] \end{tikzcd}$$

$F = (\_)^{\Sigma}\times\{0,1\}$

- We can axiomatize soundness at this level

$$\begin{tikzcd} FX & FR \arrow[l, "F\pi_1"] \arrow[r, "F\pi_2"'] & FY \\ X \arrow[u, "c"] & R \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] \arrow[u, "r"] & Y \arrow[u, "d"] \end{tikzcd}$$

$$\begin{tikzcd} {[0,1]^{X\times\Sigma}\times\{0,1\}} & {[0,1]^{R\times\Sigma}\times\{0,1\}} \arrow[l] \arrow[r] & {[0,1]^{Y\times\Sigma}\times\{0,1\}} \\ X \arrow[u, "c"] & R \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] \arrow[u, "r"] & Y \arrow[u, "d"] \end{tikzcd}$$

$F = [0,1]^{(\_)\times\Sigma}\times\{0,1\}$

probabilistic bisimulation

Verification Method via Category Theory

$$\begin{tikzcd}
X^{\Sigma} \times \{0,1\} & R^{\Sigma} \times \{0,1\} \arrow[l, "\pi_1^{\Sigma} \times \mathrm{id}_{\{0,1\}}"'] \arrow[r, "\pi_2^{\Sigma} \times \mathrm{id}_{\{0,1\}}"] & Y^{\Sigma} \times \{0,1\} \\
X \arrow[u, "c"] & R \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] \arrow[u, "r"] & Y \arrow[u, "d"]
\end{tikzcd}$$

nondeterministic bisimulation

$$\begin{tikzcd}
FX & FR \arrow[l, "F\pi_1"] \arrow[r, "F\pi_2"'] & FY \\
X \arrow[u, "c"'] & R \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] \arrow[u, "r"] & Y \arrow[u, "d"']
\end{tikzcd}$$

- We can prove soundness at this level

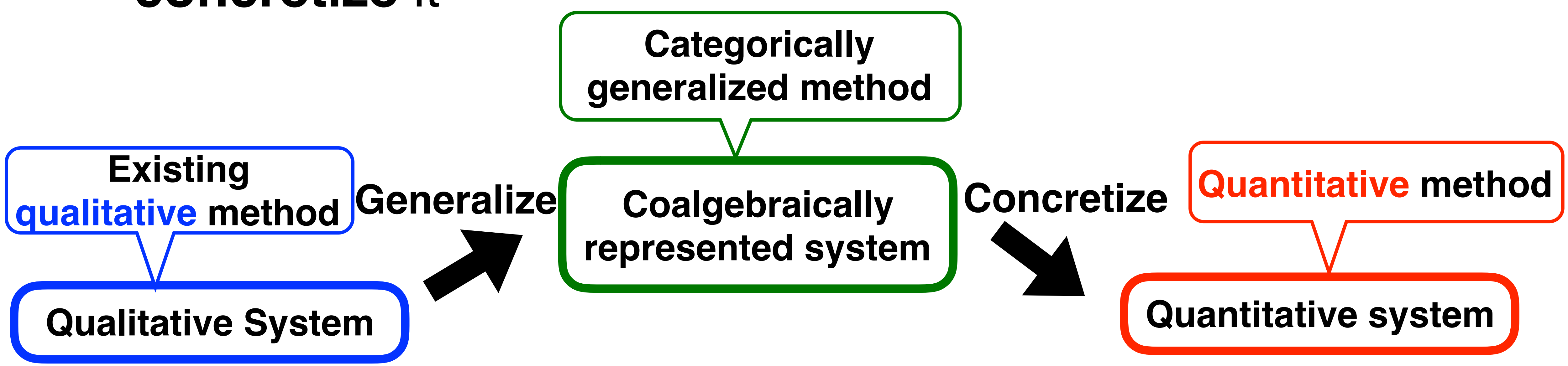
New verification method

e.g. probabilistic bisimulation

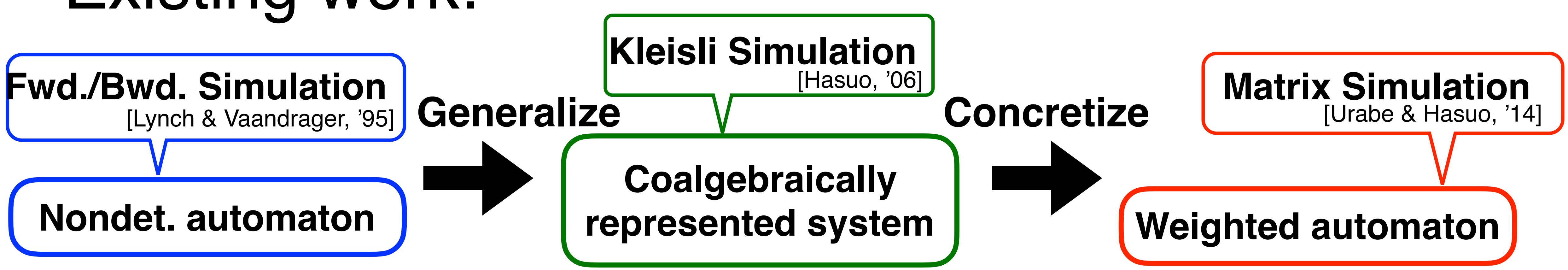
- soundness inherited

Our Strategy

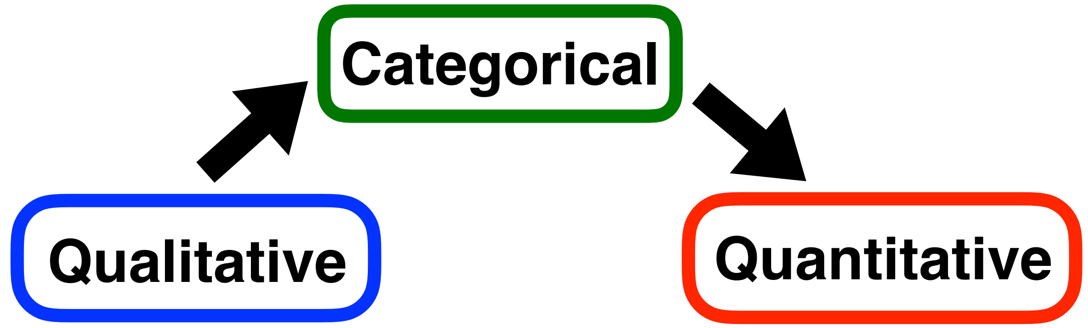
- Induce a quantitative verification method by
  - categorically **generalize** (**axiomatize**) existing qualitative method, and
  - **concretize** it



- Existing work:



Contributions



- Apply the framework to the following qualitative methods
  - **Fair simulation** [Etessami, Wilke & Schuller, ‘05]
  - **Ranking function** [Floyd, ’67]

- Concretize for **probabilistic systems**

“Probabilistic fair simulation”

& “Probabilistic ranking function”

Outline

- Overview
- Short Preliminaries on Category Theory
- Categorical Trace Semantics for Büchi and Parity Automata (Chapter 3, [U., Shimizu & Hasuo, CONCUR ’16] [U., & Hasuo, CMCS ’18])
- Categorical Fair Simulation (Chapter 4, [U. & Hasuo, LMCS ’17])
- Categorical Ranking Function (Chapter 5, [U., Hara & Hasuo, LICS ’17])
- γ-Scaled Submartingale for Probabilistic Programs and its Synthesis (Chapter 6, [Takisaka, Oyabu, U. & Hasuo, ATVA ‘18])
- Conclusion

References

- S. Mac Lane, “Categories for Working mathematician”, 1971
- B. Jacobs, “Introduction to Coalgebra”, 2016
- I. Hasuo, “Generic Weakest Precondition Semantics from Monads Enriched with Order”, CMCS 2014
- B. Jacobs, “New directions in categorical logic, for classical, probabilistic and quantum logic”, LMCS 2015

Coalgebra

- An (F-)*coalgebra* is a function of the following form:

$$\begin{array}{c} FX \\ \uparrow \\ X \end{array}$$

F : functor

$$X \longmapsto FX$$
$$(f : X \to Y) \longmapsto (Ff : FX \to FY)$$

X : carrier

- Coalgebras model **transition systems**

Examples

F	F-coalgebra	
$\mathsf{A} \times (\_)$	$X \to \mathsf{A} \times X$	deterministic (generative) transition system
$1 + \mathsf{A} \times (\_)$ $(1 = \{\checkmark\})$	$X \to 1 + \mathsf{A} \times X$	deterministic transition system with accepting state
$(\_)^{\mathsf{A}} \times \{0,1\}$	$X \to X^{\mathsf{A}} \times \{0,1\}$	deterministic automaton
$\coprod_{i=0}^{\omega} \Sigma_i \times (\_)^i$	$X \to \coprod_{i=0}^{\omega} \Sigma_i \times X^i$	deterministic tree automaton

Final Coalgebra

Def:

For a functor $F : \mathbb{C} \to \mathbb{C}$, a coalgebra $\zeta : \nu F \to F(\nu F)$ is **final** if for each $c : X \to FX$, there exists unique $f : X \to \nu F$ s.t.

$$\begin{tikzcd} FX \arrow[r, dashed, "Ff"] & F(\nu F) \\ X \arrow[u, "c"] \arrow[r, dashed, "f"'] \arrow[ur, phantom, "="] & \nu F \arrow[u, "\zeta"'] \end{tikzcd}$$

unique homomorphism

- "Greatest fixed point" of F (coinductive datatype)
- νF is a domain of **behaviors** of F-coalgebras
- f characterizes **behavior** of an F-coalgebra

Examples

F	F-coalgebra	final coalgebra
$\mathsf{A} \times (\_)$	$X \to \mathsf{A} \times X$	A^ω
$1 + \mathsf{A} \times (\_)$ $(1 = \{\checkmark\})$	$X \to 1 + \mathsf{A} \times X$	$\mathsf{A}^\infty (= \mathsf{A}^* + \mathsf{A}^\omega)$
$(\_)^{\mathsf{A}} \times \{0,1\}$	$X \to X^{\mathsf{A}} \times \{0,1\}$	$\{0,1\}^{\mathsf{A}^*}$
$\coprod_{i=0}^{\omega} \Sigma_i \times (\_)^i$	$X \to \coprod_{i=0}^{\omega} \Sigma_i \times X^i$	$\mathsf{Tree}_\infty(\Sigma)$ (infinitary trees labeled by $\Sigma = (\Sigma_i)_{i \in \omega}$)

Example:

$$\begin{tikzcd} FX \arrow[r, dashed, "Ff"] & F(\nu F) \\ X \arrow[u, "c"] \arrow[r, dashed, "f"] & \nu F \arrow[u, "\zeta"'] \arrow[ul, phantom, "="] \end{tikzcd} = \{0,1\}^{\mathsf{A}^*}$$

unique homomorphism

$$f(x)(a_0 \ldots a_{n-1}) = 1 \iff \begin{array}{l} \exists x_0, \ldots, x_n \in X. \\ x_0 = x,\ x_{i+1} \in \pi_1(c(x_i)(a_i)) \text{ and} \\ \pi_2(c(x)) = 1 \end{array}$$

$(\_)^{\mathsf{A}} \times \{0,1\}$	$X \to X^{\mathsf{A}} \times \{0,1\}$	$\{0,1\}^{\mathsf{A}^*}$
$\coprod_{i=0}^{\omega} \Sigma_i \times (\_)^i$	$X \to \coprod_{i=0}^{\omega} \Sigma_i \times X^i$	$\mathsf{Tree}_\infty(\Sigma)$ (infinitary trees labeled by $\Sigma = (\Sigma_i)_{i\in\omega}$)

Final Coalgebra for Nondeterministic Automata?

Nondeterministic Automaton

$$\mathcal{A} = (X, \mathsf{A}, \delta, \mathsf{Acc})$$

where $\delta \subseteq X \times \mathsf{A} \times X$

in $\mathbf{Sets}$

$$\begin{tikzcd}
FX \arrow[r, dashed, "Ff"] & F(\nu F) \\
X \arrow[u, "c"] \arrow[r, dashed, "f"'] \arrow[ur, phantom, "="] & \nu F \arrow[u, "\cancel{\cong\ \zeta}"']
\end{tikzcd}$$

where $F = \mathcal{P}(\{\checkmark\} + \mathsf{A} \times (\_))$

- $\mathcal{P}$ constitutes a **monad** → **Kleisli category** $\mathcal{K}\ell(\mathcal{P})$

$$\begin{array}{c} f : X \to \mathcal{P}Y \ \text{ in } \ \mathbf{Sets} \\ \hline\hline f : X \nrightarrow Y \ \text{ in } \ \mathcal{K}\ell(\mathcal{P}) \end{array} \qquad \begin{array}{c} c : X \to FX = \mathcal{P}(\{\checkmark\} + \mathsf{A} \times X) \\ \hline\hline c : X \nrightarrow F'X = \{\checkmark\} + \mathsf{A} \times X \end{array}$$

- Rem: $\{f : X \nrightarrow Y\} = \{f : X \to \mathcal{P}Y\}$ carries an order

Coalgebraic Trace Semantics via Weak Finality

$$\begin{tikzcd}[ampersand replacement=\&]
\mathcal{K}\ell(\mathcal{P}) \& FX \arrow[rr, "\shortmid" marking] \& \& F\nu F \\
\& X \arrow[u, "\shortmid" marking, "c"] \arrow[rr, "\shortmid" marking, "\text{exists}"'] \arrow[rru, phantom, "="] \& \& \nu F = \mathsf{A}^* \cup \mathsf{A}^\omega \arrow[u, "\shortmid" marking, "J\zeta", "\text{weakly final}"']
\end{tikzcd}$$

$(F = \{\checkmark\} + \mathsf{A} \times (\_))$

in $\mathbf{Sets}$ [Jacobs, '04]

$$\begin{tikzcd}[ampersand replacement=\&]
F\nu F \\
\nu F = \mathsf{A}^* \cup \mathsf{A}^\omega \arrow[u, "\zeta", "\text{final}"']
\end{tikzcd}$$

- Take the **least**/**greatest** homomorphism
- **Least** homomorphism is given by:

$$\begin{tikzcd}[ampersand replacement=\&]
FX \arrow[rr, "\shortmid" marking] \& \& F\nu F \\
X \arrow[u, "\shortmid" marking, "c"] \arrow[rr, "\shortmid" marking] \arrow[rru, phantom, "=_\mu"] \& \& \nu F \arrow[u, "\shortmid" marking, "J\zeta"']
\end{tikzcd}$$

$$x \mapsto \left\{ \begin{array}{r|l} a_1 \ldots a_n & \exists x_0, \ldots, x_n \in X.\ x = x_0, \\ \in \mathsf{A}^* & (a_{i+1}, x_{i+1}) \in c(x_i), \checkmark \in c(x_n) \end{array} \right\}$$

finite trace

- **Greatest** homomorphism is given by:

$$\begin{tikzcd}[ampersand replacement=\&]
FX \arrow[rr, "\shortmid" marking] \& \& F\nu F \\
X \arrow[u, "\shortmid" marking, "c"] \arrow[rr, "\shortmid" marking] \arrow[rru, phantom, "=_\nu"] \& \& \nu F \arrow[u, "\shortmid" marking, "J\zeta"']
\end{tikzcd}$$

$$x \mapsto \textbf{above} \cup \left\{ \begin{array}{r|l} a_1 a_2 \ldots & \exists x_0, x_1, \ldots \in X.\ x = x_0, \\ \in \mathsf{A}^\omega & (a_{i+1}, x_{i+1}) \in c(x_i) \end{array} \right\}$$

infinitary trace

Summary

- Coalgebra is a model for **state-based dynamics**
- **Final coalgebra** captures the behavior

$$
\begin{tikzcd}
FX \arrow[rr, dashed, "\overline{F}(\mathsf{beh}(c))"] & & FZ \\
X \arrow[u, "c"] \arrow[rr, dashed, "\mathsf{beh}(c)"'] \arrow[rru, phantom, "="] & & Z \arrow[u, "\zeta"', "\cong"]
\end{tikzcd}
$$

final in $\mathbf{Sets}$

- For nondeterministic automata,
  - a weakly final coalgebra in the **Kleisli category** captures **finite** and **infinitary** trace semantics

$$
\begin{tikzcd}
FX \arrow[rr, "\shortmid" marking] & & F\nu F \\
X \arrow[u, "\shortmid" marking, "c"'] \arrow[rr, "\shortmid" marking] \arrow[rru, phantom, "=_{\mu}"] & & \nu F \arrow[u, "\shortmid" marking, "J\zeta"]
\end{tikzcd}
\qquad
\begin{tikzcd}
FX \arrow[rr, "\shortmid" marking] & & F\nu F \\
X \arrow[u, "\shortmid" marking, "c"'] \arrow[rr, "\shortmid" marking] \arrow[rru, phantom, "=_{\nu}"] & & \nu F \arrow[u, "\shortmid" marking, "J\zeta"]
\end{tikzcd}
$$

weakly final

in $\mathcal{K}\ell(\mathcal{P})$

Extension to Various Systems

- $F = 1 + \mathbf{A} \times (\_)$ ➡ $F' = \coprod_i \Sigma_i \times (\_)^i$ (polynomial functor)
  - **Words** to **Trees**

- $T = \mathcal{P}$ ➡ $T = \mathcal{G}$ (the sub-Giry monad)
  - **Nondeterministic** to (generative) **Probabilistic**

Outline

- Overview
- Short Preliminaries on Category Theory
- Categorical Trace Semantics for Büchi and Parity Automata (Chapter 3, [U., Shimizu & Hasuo, CONCUR ’16] [U., & Hasuo, CMCS ’18])
- Categorical Fair Simulation (Chapter 4, [U. & Hasuo, LMCS ’17])
- Categorical Ranking Function (Chapter 5, [U., Hara & Hasuo, LICS ’17])
- γ-Scaled Submartingale for Probabilistic Programs and its Synthesis (Chapter 6, [Takisaka, Oyabu, U. & Hasuo, ATVA ‘18])
- Conclusion

Overview

- Theoretical foundation for categorically generalizing fair simulation (simulation notion for **Büchi automata**)

- We introduce two categorical characterization of languages of Büchi automata
  - **Logical fixed point**-based characterization
  - **Categorical fixed point**-based characterization

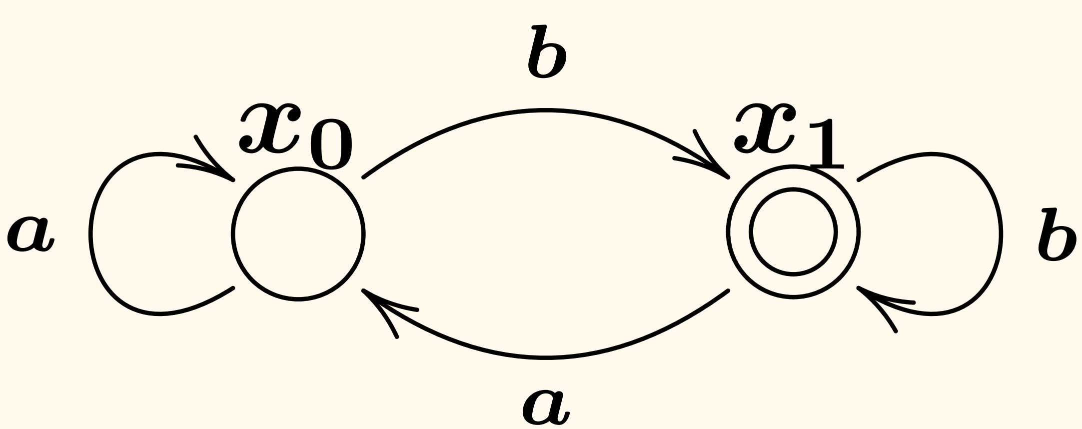
- They make use of well-known relationship between Büchi (and parity) automata and **alternating fixed point**

- They differ in how “alternating fixed point” is involved

Büchi Automaton and Its Language

- **Büchi automaton**: an automaton accepting infinite words
- A run is **accepting** if it visits $\circledcirc$ infinitely many times
- A word is **accepted** if it labels an accepting run
- **Language** $L^{\mathsf{B}}_{\mathcal{A}} : X \to \mathcal{P}\mathsf{A}^{\omega}$ assigns the set of accepted words

Example:



$$L^{\mathsf{B}}_{\mathcal{A}}(x_0) = L^{\mathsf{B}}_{\mathcal{A}}(x_1) = \left\{ w \,\middle|\, w \text{ contains infinitely many } \boldsymbol{b}\text{'s} \right\}$$

- Linear temporal logic formula → Büchi automaton

(see e.g. [Baier & Katoen])

Characterization via Logical Fixed Point

- Recall:

$$\begin{tikzcd} FX \arrow[r, "|" marking] & F\nu F \\ X \arrow[u, "c", "|" marking] \arrow[r, "|" marking] \arrow[ur, phantom, "=_\mu"] & \nu F \arrow[u, "J\zeta"', "|" marking] \end{tikzcd}$$

weakly final

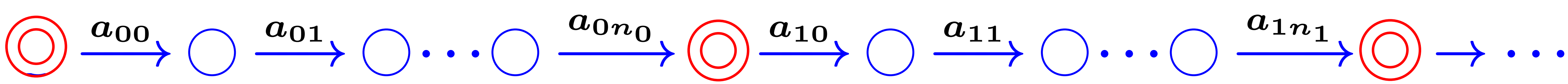
: finite trace

$$\begin{tikzcd} FX \arrow[r, "|" marking] & F\nu F \\ X \arrow[u, "c", "|" marking] \arrow[r, "|" marking] \arrow[ur, phantom, "=_\nu"] & \nu F \arrow[u, "J\zeta"', "|" marking] \end{tikzcd}$$

weakly final

: infinitary trace

- Büchi condition is known to be their **alternation**



$\{\bigcirc\}\{\circledcirc\}$

X_1, X_2

$$\begin{tikzcd} FX \arrow[r, dashed, "|" marking] & F\nu F \\ X \arrow[u, "c", "|" marking] \arrow[r, dashed, "|" marking] \arrow[ur, phantom, "="] & \nu F \arrow[u, "J\zeta"', "|" marking] \end{tikzcd}$$

$$\begin{tikzcd} FX \arrow[r, dashed, "|" marking] & F\nu F \\ X_1 \arrow[u, "c_1", "|" marking] \arrow[r, dashed, "|" marking] \arrow[ur, phantom, "=_\mu"] & \nu F \arrow[u, "J\zeta"', "|" marking] \end{tikzcd}$$

$$\begin{tikzcd} FX \arrow[r, dashed, "|" marking] & F\nu F \\ X_2 \arrow[u, "c_2", "|" marking] \arrow[r, dashed, "|" marking] \arrow[ur, phantom, "=_\nu"] & \nu F \arrow[u, "J\zeta"', "|" marking] \end{tikzcd}$$

$$\frac{\mathbf{tr}^{\mathrm{B}}(c) : X_1 + X_2 \nrightarrow \nu F}{\mathbf{tr}^{\mathrm{B}}(c) : X_1 + X_2 \to \mathcal{P}(\nu F)}$$

Thm:

This characterizes Büchi languages

Discussion and Next Step

- Logical fixed point-based characterization

$$\mathbf{tr}^{\mathrm{B}}(\boldsymbol{c}) : \boldsymbol{X}_1 + \boldsymbol{X}_2 \nrightarrow \boldsymbol{\nu F}$$

language as alternating fixed-point

greatest fixed-point

datatype as final coalgebra (i.e. greatest fixed-point)

alternating fixed-point

Final Coalgebra & Initial Algebra

- F-algebra: $FX \to X$

Final coalgebra

$$\begin{tikzcd} FX \arrow[r, dashed, "Ff"] & FZ \\ X \arrow[u, "c"] \arrow[r, dashed, "f"', "\text{unique}"'] \arrow[ur, phantom, "="] & Z \arrow[u, "\cong"', "\zeta"] \end{tikzcd}$$

- "Greatest fixed point" of F
- Z collects **infinitary behaviors** of F-coalgebras
- Coinductive datatype

Initial algebra

$$\begin{tikzcd} FI \arrow[r, dashed, "Ff"] \arrow[d, "\iota"', "\cong"] \arrow[dr, phantom, "="] & FX \arrow[d, "a"] \\ I \arrow[r, dashed, "f", "\text{unique}"'] & X \end{tikzcd}$$

- "Least fixed point" of F
- I collects **finite behaviors** of F-coalgebras
- Inductive datatype

- We **alternate** them

Alternating Fixed Point of Functor

- We use **parameterized fixed point**

- For $f : L_1 \times L_2 \to L_1 \times L_2$, $(L_1, L_2 : \text{complete lattices})$
  - Fix $u_2 \in L_2$ ➡ $\pi_1 \circ f(\_, u_2) : L_1 \to L_1$

  ⇨ We can consider its least/greatest fixed point **(parameterized fixed point)**

- For a functor $F : \mathbb{C} \to \mathbb{C}$,
  - Fix $Y \in \mathbb{C}$ ➡ $F(\_ + Y) : \mathbb{C} \to \mathbb{C}$

  $(+ : \text{coproduct (disjoint sum)})$

  ⇨
  - The carrier of **initial** $F(\_ + Y)$-algebra $F^{+}Y$
  - The carrier of **final** $F(\_ + Y)$ -coalgebra $F^{\oplus}Y$

- We alternate and obtain $F^{+\oplus}\mathbf{0}$ $(\text{i.e. } (F^{+})^{\oplus}\mathbf{0})$

Examples

- For $F = \mathbf{A} \times (\_)$

$$F^{+\oplus}0 \cong (\mathbf{A}^{+})^{\omega}$$

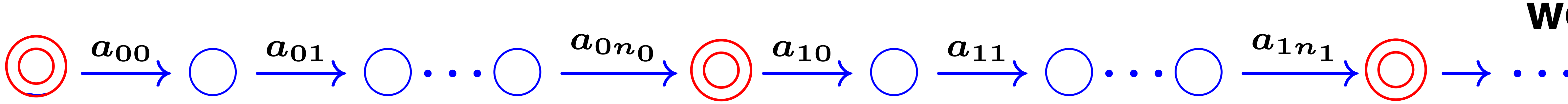
inductive datatypes (least fixed-point)

$$= \underbrace{\overbrace{\mathbf{A}^{+}}\ \overbrace{\mathbf{A}^{+}}\ \overbrace{\mathbf{A}^{+}}\ \overbrace{\mathbf{A}^{+}}\ \ldots}_{\text{coinductive datatype (greatest fixed-point)}}$$

Note:
Büchi condition satisfied

$$\frac{(a_{00}a_{01}\ldots a_{0n_0})(a_{10}a_{11}\ldots a_{1n_1})\ldots \in (\mathbf{A}^{+})^{\omega}}{\qquad}$$

decorated word



The first state is accepting

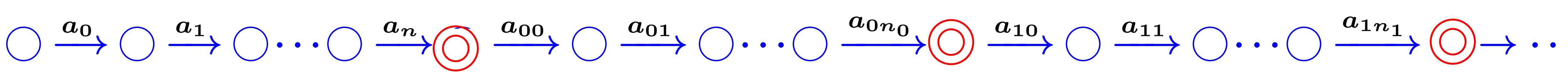
Examples

- For $F = \mathsf{A} \times (\_\,)$

$$F^+(F^{+\oplus}0) \cong \mathsf{A}^+ \times (\mathsf{A}^+)^\omega$$

$$= \mathsf{A}\dots\mathsf{A}(\overbrace{\underbrace{\overbrace{\mathsf{A}^+}\ \ \overbrace{\mathsf{A}^+}\ \ \overbrace{\mathsf{A}^+}\ \ \overbrace{\mathsf{A}^+}\ \ \dots}_{\text{coinductive datatype (greatest fixed-point)}}}^{\text{inductive datatypes (least fixed-point)}})$$

$$a_0 a_1 \dots a_n (a_{00} a_{01} \dots a_{0n_0})(a_{10} a_{11} \dots a_{1n_1}) \dots \in \mathsf{A}^+(\mathsf{A}^+)^\omega$$



The first state is nonaccepting

Language via Categorical Fixed Point

- We can consider the following function

$$x \mapsto \left\{ \bullet_0 \xrightarrow{a_0} \bullet_1 \xrightarrow{a_1} \bullet_2 \to \cdots \;\middle|\; \begin{array}{l} x_0 \xrightarrow{a_0} x_1 \xrightarrow{a_1} x_2 \to \cdots : \text{a run on } \mathcal{A} \\ \bullet_i \in \{\bigcirc, \circledcirc\},\ x_i : \bullet_i, \\ \bullet_i = \circledcirc \text{ for infinitely many } i\text{'s} \end{array} \right\}$$

- We gave categorical definition

Def:

We define $\mathbf{dtr}_1(\mathcal{A}) : X_1 \longrightarrow \mathcal{P}(\mathsf{A}^+(\mathsf{A}^+)^\omega)$ and $\mathbf{dtr}_2(\mathcal{A}) : X_2 \longrightarrow \mathcal{P}((\mathsf{A}^+)^\omega)$ by:

$$\begin{tikzcd}
F(X_1+X_2) \arrow[r, "\overline{F}(\mathbf{dtr}_1(c)+\mathbf{dtr}_2(c))"] & F(F^+(F^{+\oplus}0)+F^{+\oplus}0) \\
X_1 \arrow[u, "c_1"] \arrow[r, "\mathbf{dtr}_1(c)"'] \arrow[ur, phantom, "=_\nu"] & F^+(F^{+\oplus}0) \arrow[u, "J\iota^{-1}", "\cong"']
\end{tikzcd}
\qquad
\begin{tikzcd}
F(X_1+X_2) \arrow[r, "\overline{F}(\mathbf{dtr}_1(c)+\mathbf{dtr}_2(c))"] & F(F^+(F^{+\oplus}0)+F^{+\oplus}0) \\
 & F^+(F^{+\oplus}0) \arrow[u, "J\iota^{-1}", "\cong"'] \\
X_2 \arrow[uu, "c_2"] \arrow[r, "\mathbf{dtr}_2(c)"'] \arrow[uur, phantom, "=_\nu"] & F^{+\oplus}0 \arrow[u, "J\zeta", "\cong"']
\end{tikzcd}$$

Logical Fixed Point vs. Categorical Fixed Point

$$\begin{tikzcd}
FX \arrow[r, dashed, "|" marking] & F\nu F \\
X_1 \arrow[u, "c_1" marking] \arrow[r, dashed, "|" marking] \arrow[ur, phantom, "\color{red}=_\mu"] & \nu F \arrow[u, "J\zeta" marking]
\end{tikzcd} \; = \mathbf{A}^\omega
\qquad
\begin{tikzcd}[column sep=large]
F(X_1+X_2) \arrow[r, "\overline{F}(\mathbf{dtr}_1(c)+\mathbf{dtr}_2(c))"] & F(F^+(F^{+\oplus}0)+F^{+\oplus}0) \\
X_1 \arrow[u, "c_1"] \arrow[r, "\mathbf{dtr}_1(c)"] \arrow[ur, phantom, "\color{blue}=_\nu"] & F^+(F^{+\oplus}0) \arrow[u, "J\iota^{-1}", "\cong"']
\end{tikzcd} = \mathbf{A}^+(\mathbf{A}^+)^\omega$$

v.s.

$$\begin{tikzcd}
FX \arrow[r, dashed, "|" marking] & F\nu F \\
X_2 \arrow[u, "c_2" marking] \arrow[r, dashed, "|" marking] \arrow[ur, phantom, "\color{blue}=_\nu"] & \nu F \arrow[u, "J\zeta" marking]
\end{tikzcd} \; = \mathbf{A}^\omega
\qquad
\begin{tikzcd}[column sep=large]
F(X_1+X_2) \arrow[r, "\overline{F}(\mathbf{dtr}_1(c)+\mathbf{dtr}_2(c))"] & F(F^+(F^{+\oplus}0)+F^{+\oplus}0) \\
 & F^+(F^{+\oplus}0) \arrow[u, "J\iota^{-1}", "\cong"'] \\
X_2 \arrow[uu, "c_2"] \arrow[r, "\mathbf{dtr}_2(c)"] \arrow[uur, phantom, "\color{blue}=_\nu"] & F^{+\oplus}0 \arrow[u, "J\zeta", "\cong"']
\end{tikzcd} = (\mathbf{A}^+)^\omega$$

- There exist functions that "removes" decorations

$$\begin{tikzcd}
 & \mathbf{A}^+(\mathbf{A}^+)^\omega \arrow[dl, "p_1"'] \\
\mathbf{A}^\omega & \\
 & (\mathbf{A}^+)^\omega \arrow[ul, "p_2"]
\end{tikzcd}$$

- $\mathbf{dtr}(c)$ and $\mathbf{tr}^B(c)$ are connected by the "flattening function"

$$\begin{tikzcd}
 & \mathbf{A}^+(\mathbf{A}^+)^\omega + (\mathbf{A}^+)^\omega \arrow[dr, bend left, "{[p_1, p_2]}"] & \\
X_1 + X_2 \arrow[ur, bend left, "\mathbf{dtr}(\mathcal{A})"] \arrow[rr, bend right, "\mathbf{tr}^B(\mathcal{A})"'] \arrow[rr, phantom, "="] & & \mathbf{A}^\omega
\end{tikzcd}$$

- We gave categorical counterpart

Extension

- **Words** to **Trees**

$$F = \mathsf{A} \times (\_) \quad \Rightarrow \quad F = \coprod_i \Sigma_i \times (\_)^i$$

(polynomial functor)

- **Nondeterministic** to (generative) **Probabilistic**

$$T = \mathcal{P} \quad \Rightarrow \quad T = \mathcal{G}$$

(the sub-Giry monad)

- **Büchi** to **Parity**

$$\begin{tikzcd} FX \arrow[r, rightsquigarrow, "\overline{F}([u_1,\dots,u_{2n}])"] & F\Sigma^\omega \\ X_1 \arrow[u, "c_1"] \arrow[r, rightsquigarrow, "u_1"] \arrow[ur, phantom, "=_\mu"] & \Sigma^\omega \arrow[u, "\zeta", "\wr"'] \end{tikzcd} , \quad \begin{tikzcd} FX \arrow[r, rightsquigarrow, "\overline{F}([u_1,\dots,u_{2n}])"] & F\Sigma^\omega \\ X_2 \arrow[u, "c_2"] \arrow[r, rightsquigarrow, "u_2"] \arrow[ur, phantom, "=_\nu"] & \Sigma^\omega \arrow[u, "\zeta", "\wr"'] \end{tikzcd} , \quad \dots , \quad \begin{tikzcd} FX \arrow[r, rightsquigarrow, "\overline{F}([u_1,\dots,u_{2n}])"] & F\Sigma^\omega \\ X_{2n} \arrow[u, "c_{2n}"] \arrow[r, rightsquigarrow, "u_{2n}"] \arrow[ur, phantom, "=_\nu"] & \Sigma^\omega \arrow[u, "\zeta", "\wr"'] \end{tikzcd}$$

Summary

- Logical fixed point-based characterization

$$\mathbf{tr}^{\mathrm{B}}(\boldsymbol{c})\colon \boldsymbol{X}_1 + \boldsymbol{X}_2 \to \mathcal{P}\mathbf{A}^{\omega}$$

language as
alternating fixed-point

datatype as
greatest fixed-point

- Categorical fixed point-based characterization

$$\mathbf{dtr}(\boldsymbol{c})\colon \boldsymbol{X}_1 + \boldsymbol{X}_2 \to \mathcal{P}(\mathbf{A}^{+})^{\omega} + \mathcal{P}\mathbf{A}^{+}(\mathbf{A}^{+})^{\omega}$$

language as
greatest fixed-point

datatypes as
alternating fixed-point

- They coincide

Related Work

- Deterministic Muller automaton as a coalgebra

  [Ciancia & Venema, CMCS '12]

  - Trick with **lasso characterization**

    ➡ Coalgebra on $\mathbf{Sets}^{\mathbf{2}}$

  - Compared to our characterization:
    - Final coalgebra-based characterization → well-behaved

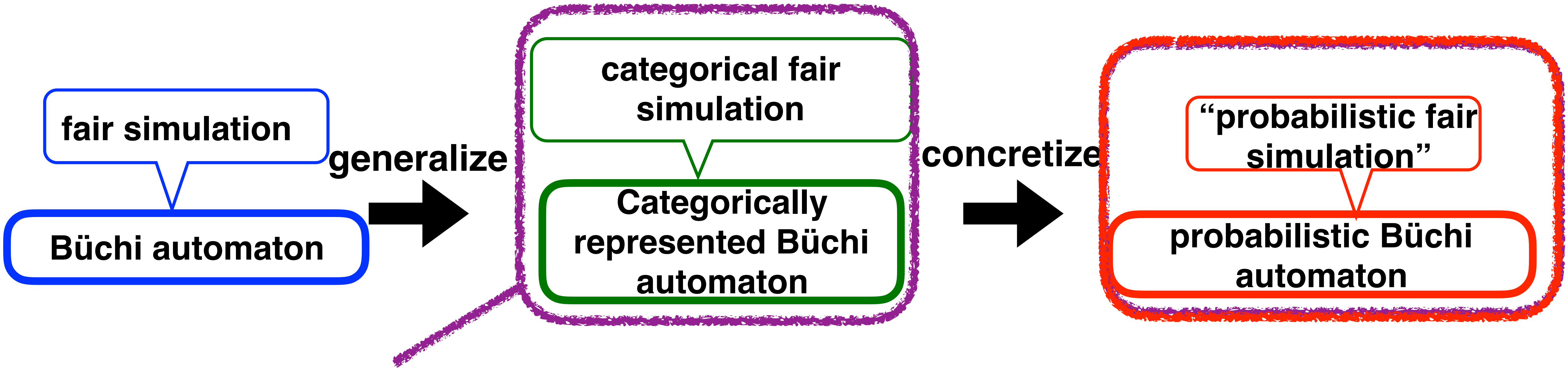
      Thm: **Bisimilarity** and **language equivalence** coincide

    - Characterization of simulation seems difficult
    - Finite-state restriction

Outline

- Overview
- Short Preliminaries on Category Theory
- Categorical Trace Semantics for Büchi and Parity Automata
(Chapter 3, [U., Shimizu & Hasuo, CONCUR ’16] [U., & Hasuo, CMCS ’18])
- Categorical Fair Simulation (Chapter 4, [U. & Hasuo, LMCS ’17])
- Categorical Ranking Function (Chapter 5, [U., Hara & Hasuo, LICS ’17])
- γ-Scaled Submartingale for Probabilistic Programs and its Synthesis
(Chapter 6, [Takisaka, Oyabu, U. & Hasuo, ATVA ‘18])
- Conclusion

Overview



Categorically prove soundness → **soundness**

↑

We use the categorical characterization of Büchi automata

Simulation

- Used to prove **inclusion** between transition systems
- Example：

$L(\mathcal{A}) \subseteq L(\mathcal{B})$ the set of accepted words

- Problem: language inclusion is often a difficult problem

Prove that $\mathcal{B}$ can **simulate** $\mathcal{A}$ in a step-wise manner

(step-wise language inclusion)

- A simulation from $\mathcal{A}$ to $\mathcal{B}$ exists

$$\Longrightarrow L(\mathcal{A}) \subseteq L(\mathcal{B})$$

(soundness of simulation)

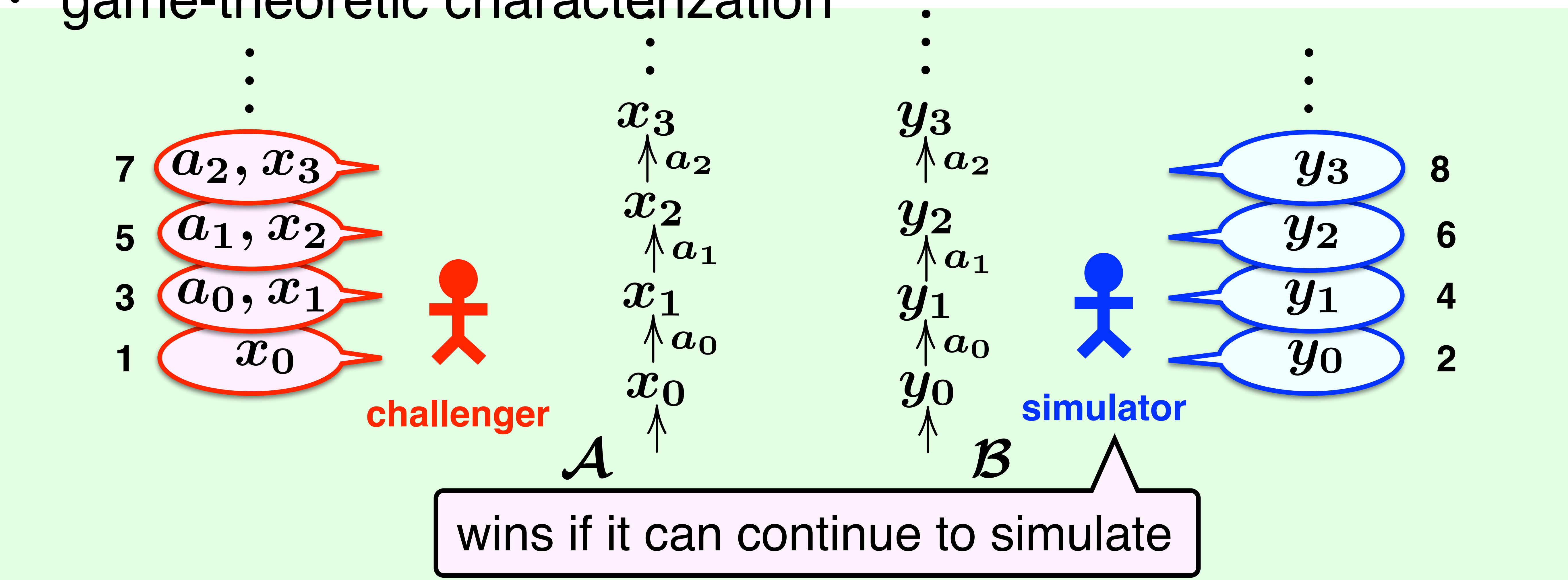
Forward Simulation [Lynch & Vaandrager, ‘95]

- Simulation notion for nondeterministic automata

Def:

$$\mathcal{A} \sqsubseteq_{\mathbf{F}} \mathcal{B} \overset{\text{def}}{\iff} \exists R. \quad \mathcal{A}\ \begin{tikzcd} x' & \\ x \arrow[u, "a"] \arrow[r, dash, dashed, "R"] & y \end{tikzcd}\ \mathcal{B} \quad \Longrightarrow \quad \mathcal{A}\ \begin{tikzcd} x' \arrow[r, dash, dashed, "R"] & \exists y' \\ x \arrow[u, "a"] \arrow[r, dash, dashed, "R"] & y \arrow[u, "a"] \end{tikzcd}\ \mathcal{B}$$

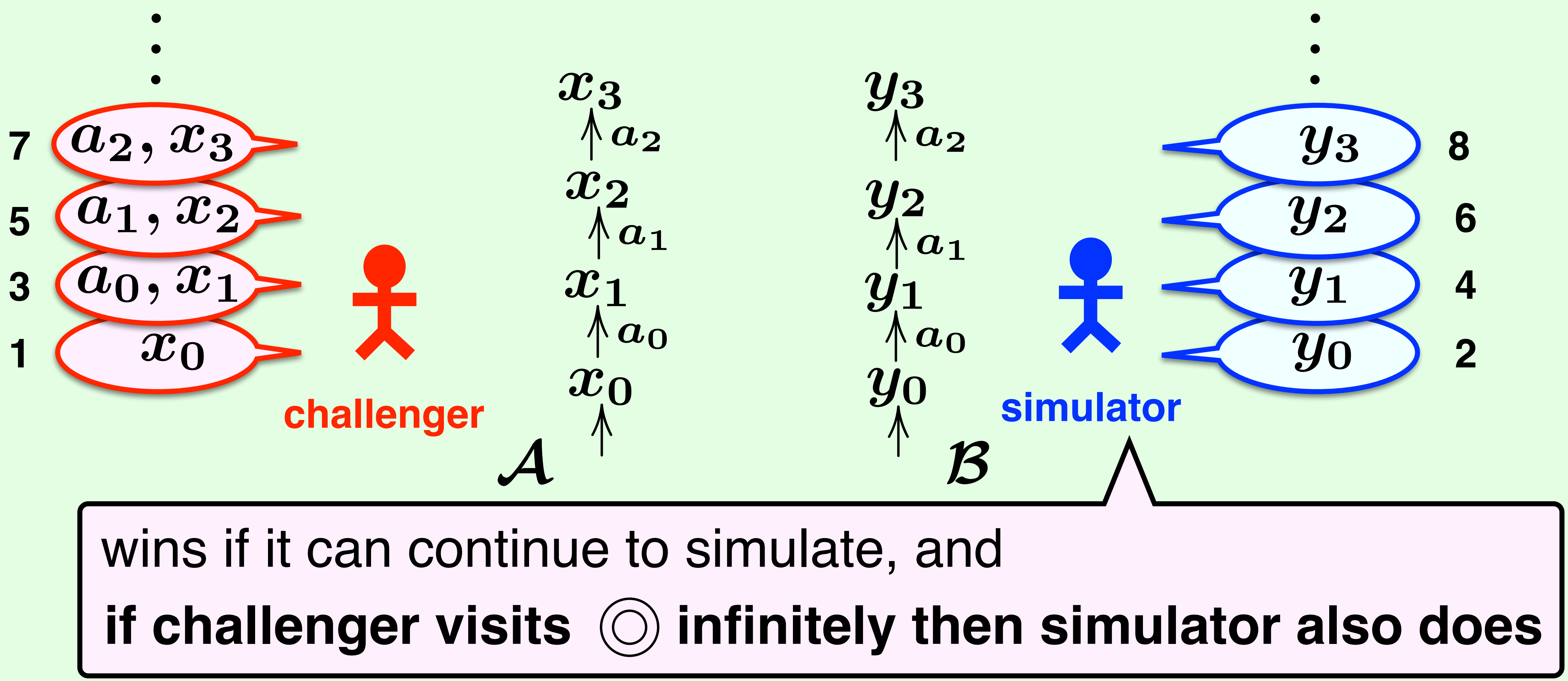
- game-theoretic characterization



simulator wins $\Leftrightarrow$ forward simulation exists

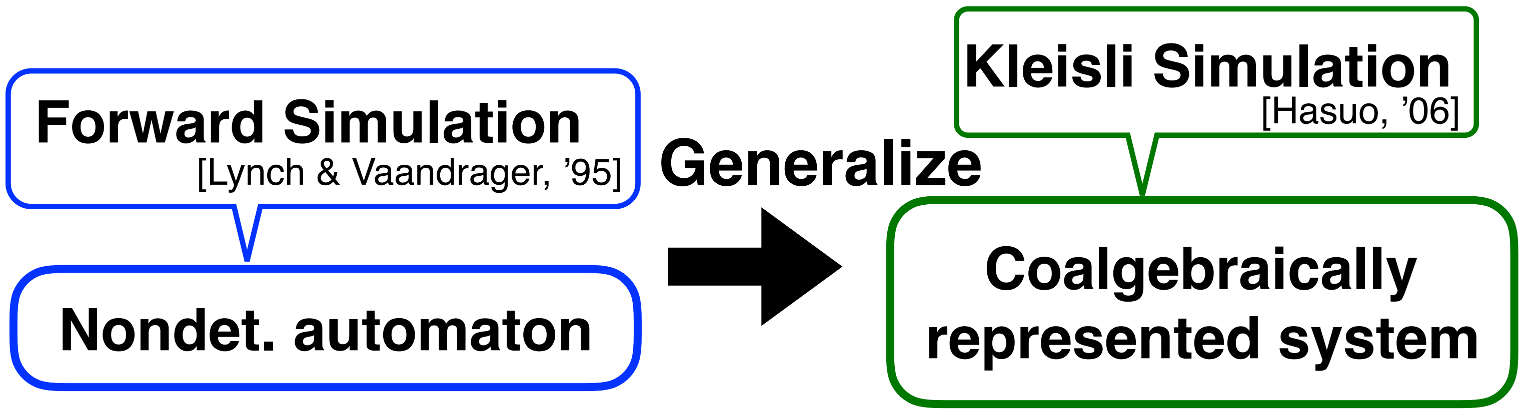
Fair Simulation [Etessami et al., ’05]

- Simulation notion for Büchi automata



- Representable as a **parity game**

Kleisli Simulation [Hasuo ‘06]



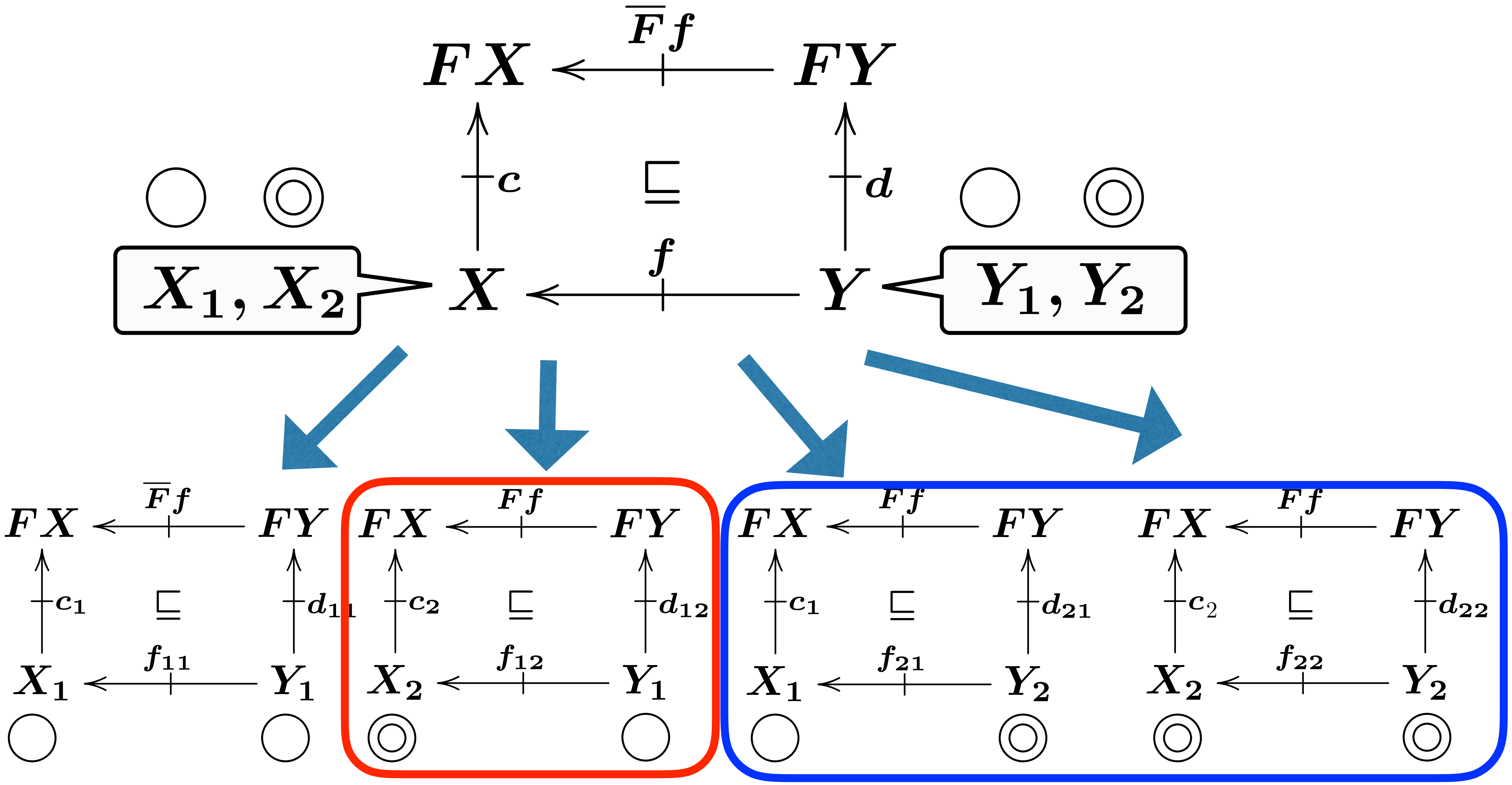
- Categorical generalization of forward simulation

Def:

A forward Kleisli simulation from $c : X \nrightarrow FX$ to $d : Y \nrightarrow FY$ is

$$f : Y \nrightarrow X \quad \text{s.t.} \quad \begin{tikzcd} FX & FY \arrow[l, "\overline{F}f"'] \\ X \arrow[u, "c"] \arrow[ur, phantom, "\sqsubseteq"] & Y \arrow[l, "f"] \arrow[u, "d"'] \end{tikzcd} \quad \text{in } \mathcal{K}\ell(T)$$

Towards Kleisli Fair Simulation



- Definition of fair simulation requires if ◎ ○ occurs infinitely then ○ ◎ or ◎ ◎ occurs infinitely

➡ We count down ◎ ○ until ○ ◎ or ◎ ◎ occurs

Kleisli Fair Simulation with Dividing

Def:

A *(Kleisli, $\bar{\mathfrak{a}}$-bounded) fair simulation with dividing* from $\mathcal{X}$ to $\mathcal{Y}$ is an arrow $f : Y \rightarrow\!\!\!\!\!\rightarrow X$ that satisfies the following conditions.

A. The arrow $f : Y \rightarrow\!\!\!\!\!\rightarrow X$ is a forward Kleisli simulation from $\mathcal{X}$ to $\mathcal{Y}$.

B. There exist a pair $d_{11}, d_{12} : Y_1 \rightarrow\!\!\!\!\!\rightarrow \overline{F}Y$ of arrows such that $[\mathrm{id}_{\overline{F}Y}, \mathrm{id}_{\overline{F}Y}] \odot \langle\!\langle d_{11}, d_{12} \rangle\!\rangle = d_1$ and a pair of increasing transfinite sequences

$$f_{11}^{\langle 0 \rangle} \sqsubseteq f_{11}^{\langle 1 \rangle} \sqsubseteq \cdots \sqsubseteq f_{11}^{\langle \bar{\mathfrak{a}} \rangle} : Y_1 \rightarrow\!\!\!\!\!\rightarrow X_1 \text{ and } f_{12}^{\langle 0 \rangle} \sqsubseteq f_{12}^{\langle 1 \rangle} \sqsubseteq \cdots \sqsubseteq f_{12}^{\langle \bar{\mathfrak{a}} \rangle} : Y_1 \rightarrow\!\!\!\!\!\rightarrow X_2,$$

such that a codomain join $\langle\!\langle f_{11}^{\langle \mathfrak{a} \rangle}, f_{12}^{\langle \mathfrak{a} \rangle} \rangle\!\rangle$ exists for each $\mathfrak{a} \leq \bar{\mathfrak{a}}$, and the following conditions are satisfied:

(a) **(Approximate f_{11} and f_{12})** We have $f_{11}^{\langle \bar{\mathfrak{a}} \rangle} = f_{11}$ and $f_{12}^{\langle \bar{\mathfrak{a}} \rangle} = f_{12}$.

(b) **($f_{11}^{\langle \mathfrak{a} \rangle}$)** For each $\mathfrak{a}$, $c_1 \odot f_{11}^{\langle \mathfrak{a} \rangle} \sqsubseteq \overline{F}[\langle\!\langle f_{11}^{\langle \mathfrak{a} \rangle}, f_{12}^{\langle \mathfrak{a} \rangle} \rangle\!\rangle, \langle\!\langle f_{21}, f_{22} \rangle\!\rangle] \odot d_{11}$.

(c) **($f_{12}^{\langle \mathfrak{a} \rangle}$, the base case)** If $\mathfrak{a} = 0$, then $f_{12}^{\langle \mathfrak{a} \rangle} = \bot$.

(d) **($f_{12}^{\langle \mathfrak{a} \rangle}$, the step case)** If $\mathfrak{a}$ is a successor ordinal, then $c_2 \odot f_{12}^{\langle \mathfrak{a} \rangle} \sqsubseteq \overline{F}[\langle\!\langle f_{11}^{\langle \mathfrak{a}-1 \rangle}, f_{12}^{\langle \mathfrak{a}-1 \rangle} \rangle\!\rangle, \langle\!\langle f_{21}, f_{22} \rangle\!\rangle] \odot d_{12}$.

(e) **($f_{12}^{\langle \mathfrak{a} \rangle}$, the limit case)** If $\mathfrak{a}$ is a limit ordinal, then the supremum $\bigsqcup_{\mathfrak{a}' < \mathfrak{a}} f_{12}^{\langle \mathfrak{a}' \rangle}$ exists and $f_{12}^{\langle \mathfrak{a} \rangle} \sqsubseteq \bigsqcup_{\mathfrak{a}' < \mathfrak{a}} f_{12}^{\langle \mathfrak{a}' \rangle}$.

Counts downs ◎ ○

We call the pair d_{11}, d_{12} of arrows a *dividing* of d_1, and the sequences $f_{11}^{\langle 0 \rangle} \sqsubseteq \cdots \sqsubseteq f_{11}^{\langle \bar{\mathfrak{a}} \rangle}$ and $f_{12}^{\langle 0 \rangle} \sqsubseteq \cdots \sqsubseteq f_{12}^{\langle \bar{\mathfrak{a}} \rangle}$ *approximating sequences.*

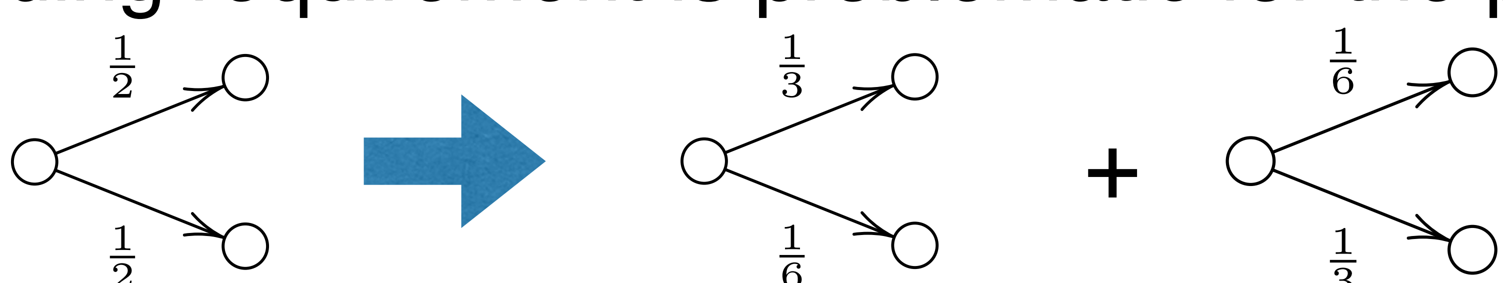
simulate nonacc. states

$$\begin{tikzcd} \overline{F}Y \arrow[r, "{\overline{F}[\langle\!\langle f_{11}^{\langle \mathfrak{a} \rangle}, f_{12}^{\langle \mathfrak{a} \rangle} \rangle\!\rangle, \langle\!\langle f_{21}, f_{22} \rangle\!\rangle]}"] \arrow[d, phantom, "\sqsupseteq"] & \overline{F}X \\ Y_1 \arrow[u, "d_{11}"] \arrow[r, "f_{11}^{\langle \mathfrak{a} \rangle}"'] & X_1 \arrow[u, "c_1"'] \end{tikzcd}$$

simulate acc. states

$$\begin{tikzcd} \overline{F}Y \arrow[r, "{\overline{F}[\langle\!\langle f_{11}^{\langle \mathfrak{a} \rangle}, f_{12}^{\langle \mathfrak{a} \rangle} \rangle\!\rangle, \langle\!\langle f_{21}, f_{22} \rangle\!\rangle]}"] & \overline{F}X \\ Y_1 \arrow[u, "d_{12}"] \arrow[r, "f_{12}^{\langle \mathfrak{a}+1 \rangle}"'] & X_2 \arrow[u, "c_2"'] \end{tikzcd}$$

- Sound
- Dividing requirement is problematic for the probabilistic setting



Kleisli Fair Simulation without Dividing?

Def:

A *(Kleisli $\bar{\mathfrak{a}}$-bounded) fair simulation without dividing* from $\mathcal{X} = \big(X, c, (X_1, X_2),\big)$ to $\mathcal{Y} = \big(Y, d, (Y_1, Y_2),\big)$ is defined almost the same way as one with dividing, except that Condition 1 is replaced by the following condition.

1' There exists a pair of increasing transfinite sequences The components $f_{11} \colon Y_1 \nrightarrow X_1$ and $f_{12} \colon Y_1 \nrightarrow X_2$ come

$$f_{11}^{\langle 0 \rangle} \sqsubseteq f_{11}^{\langle 1 \rangle} \sqsubseteq \cdots \sqsubseteq f_{11}^{\langle \bar{\mathfrak{a}} \rangle} : Y_1 \nrightarrow X_1 \text{ and } f_{12}^{\langle 0 \rangle} \sqsubseteq f_{12}^{\langle 1 \rangle} \sqsubseteq \cdots \sqsubseteq f_{12}^{\langle \bar{\mathfrak{a}} \rangle} : Y_1 \nrightarrow X_2,$$

that satisfies Conditions 1(a), 1(c) and 1(e) and the following two conditions.

(b') $(f_{11}^{\langle \mathfrak{a} \rangle})$ For each $\mathfrak{a}$, $c_1 \odot f_{11}^{\langle \mathfrak{a} \rangle} \sqsubseteq \overline{F}\big[\langle\!\langle f_{11}^{\langle \mathfrak{a} \rangle}, f_{12}^{\langle \mathfrak{a} \rangle} \rangle\!\rangle, \langle\!\langle f_{21}, f_{22} \rangle\!\rangle\big] \odot d_1$.

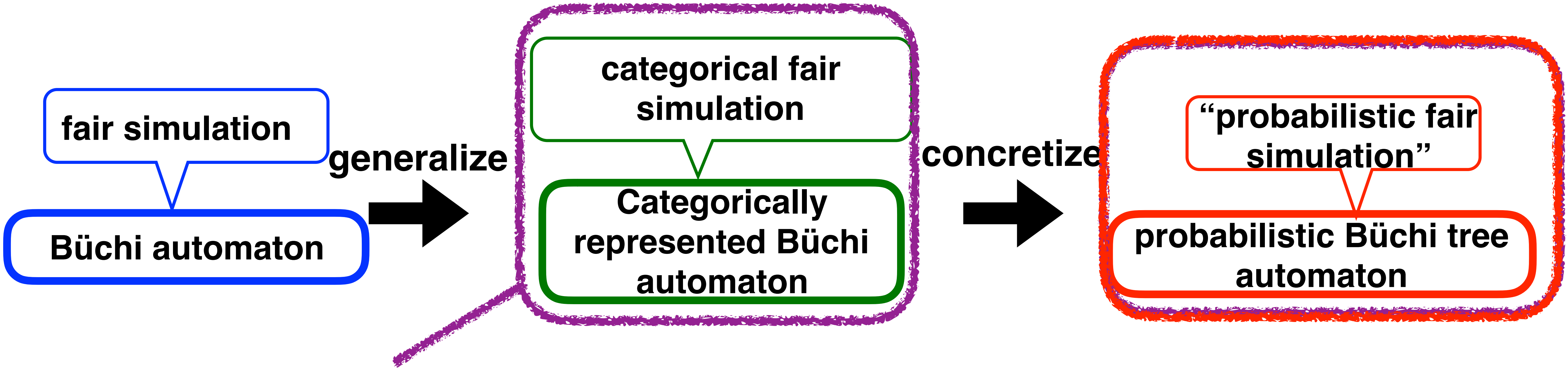
(d') **($f_{12}^{\langle \mathfrak{a} \rangle}$, the step case)** If $\mathfrak{a}$ is a successor ordinal, then $c_2 \odot f_{12}^{\langle \mathfrak{a} \rangle} \sqsubseteq \overline{F}\big[\langle\!\langle f_{11}^{\langle \mathfrak{a}-1 \rangle}, f_{12}^{\langle \mathfrak{a}-1 \rangle} \rangle\!\rangle, \langle\!\langle f_{21}, f_{22} \rangle\!\rangle\big] \odot d_{12}$.

$$\begin{tikzcd} FY \arrow[r, "\overline{F}\left[\langle\!\langle f_{11}^{\langle \mathfrak{a} \rangle}, f_{12}^{\langle \mathfrak{a} \rangle} \rangle\!\rangle, \langle\!\langle f_{21}, f_{22} \rangle\!\rangle\right]"] \arrow[dr, phantom, "\sqsupseteq"] & FX \\ Y_1 \arrow[u, "d_1"] \arrow[r, "f_{11}^{\langle \mathfrak{a} \rangle}"'] & X_1 \arrow[u, "c_1"'] \end{tikzcd} \qquad \begin{tikzcd} FY \arrow[r, "\overline{F}\left[\langle\!\langle f_{11}^{\langle \mathfrak{a} \rangle}, f_{12}^{\langle \mathfrak{a} \rangle} \rangle\!\rangle, \langle\!\langle f_{21}, f_{22} \rangle\!\rangle\right]"] \arrow[dr, phantom, "\sqsupseteq"] & FX \\ Y_1 \arrow[u, "d_1"] \arrow[r, "f_{12}^{\langle \mathfrak{a}+1 \rangle}"'] & X_2 \arrow[u, "c_2"'] \end{tikzcd}$$

- **Not** necessarily sound
- Two (categorical) **additional** conditions for soundness

(proposition 4.3.11 & 4.3.13)

Kleisli Fair Simulation for Probabilistic Büchi Automata



Categorically prove soundness ➡ **soundness**

Fair Simulation with Dividing for Probabilistic Büchi Tree Automata

Def:

ın ($\bar{\mathfrak{a}}$-*bounded) fair simulation with dividing* from $\mathscr{A}$ to $\mathscr{B}$ is a measurable function $f : (Y, \mathfrak{F}_Y) \to \mathcal{G}(X, \mathfrak{F}_X)$ that satisfies the following cond
$i, j \in \{1, 2\}$, we define $f_{ji} : (Y_j, \mathfrak{F}_{Y_j}) \to \mathcal{G}(X_i, \mathfrak{F}_{X_i})$ by $f_{ji}(y)(A) := f(y)(A \cap X_i)$ for $y \in Y_j$ and $A \in \mathfrak{F}_{X_i}$).

For each $y \in Y$, $n \in \mathbb{N}$, $a \in \Sigma_n$ and $A_1, \dots, A_n \in \mathfrak{F}_X$, we have:

$$\int_{x \in X} \tau(x)(\{a\} \times A_1 \times \cdots \times A_n) f(y)(\mathrm{d}x) \leq \int_{y_1, \dots, y_n \in Y} f(y_1)(A_1) \cdot \cdots \cdot f(y_n)(A_n) \cdot \theta(y)(\{a\} \times \mathrm{d}y_1 \times \cdots \times \mathrm{d}y$$

There exists a pair $\theta_{11}, \theta_{12} : Y_1 \to \mathcal{G}\left(\coprod_{i \in \mathbb{N}} \Sigma_n \times Y^n\right)$ of measurable functions such that $\theta_{11}(y)(A) + \theta_{12}(y)(A) = \theta(y)(A)$ for each $y \in Y$
$A \in \mathfrak{F}_{\coprod_{i \in \mathbb{N}} \Sigma_n \times Y^n}$. There also exist increasing transfinite sequences

$$f_{11}^{\langle 0 \rangle} \leq f_{11}^{\langle 1 \rangle} \leq \cdots \leq f_{11}^{\langle \bar{\mathfrak{a}} \rangle} : Y_1 \to \mathcal{G}X_1 \text{ and } f_{12}^{\langle 0 \rangle} \leq f_{12}^{\langle 1 \rangle} \leq \cdots \leq f_{12}^{\langle \bar{\mathfrak{a}} \rangle} : Y_1 \to \mathcal{G}X_2,$$

of measurable functions with respect to the pointwise order such that the following conditions are satisfied:

(a) **(Approximate f_{11} and f_{12})** We have $f_{11}^{\langle \bar{\mathfrak{a}} \rangle} = f_{11}$ and $f_{12}^{\langle \bar{\mathfrak{a}} \rangle} = f_{12}$.

(b) **($f_{11}^{\langle \mathfrak{a} \rangle}$)** For each $\mathfrak{a}$, $y \in Y_1$ and $A_1, \dots, A_n \in \mathfrak{F}_X$,

$$\int_{x \in X_1} \tau(x)(\{a\} \times A_1 \times \cdots \times A_n) f_{11}^{\langle \mathfrak{a} \rangle}(y)(\mathrm{d}x) \leq \int_{y_1, \dots, y_n \in Y} f^{\langle \mathfrak{a} \rangle}(y_1)(A_1) \cdot \cdots \cdot f^{\langle \mathfrak{a} \rangle}(y_n)(A_n) \cdot \theta_{11}(y)(\{a\} \times \mathrm{d}y_1 \times \cdots \times \mathrm{d}y$$

Here $f^{\langle \mathfrak{a} \rangle} : Y \to \mathcal{G}X$ is defined by

$$f^{\langle \mathfrak{a} \rangle}(y)(A) := \begin{cases} f_{11}^{\langle \mathfrak{a} \rangle}(y)(A) + f_{12}^{\langle \mathfrak{a} \rangle}(y)(A) & (y \in Y_1) \\ f_{21}(y)(A) + f_{22}(y)(A) & (y \in Y_2)\,. \end{cases}$$

(c) **($f_{12}^{\langle \mathfrak{a} \rangle}$, the base case)** If $\mathfrak{a} = 0$, then $f_{12}^{\langle \mathfrak{a} \rangle}(y)(X_2) = 0$ for each $y \in Y_1$.

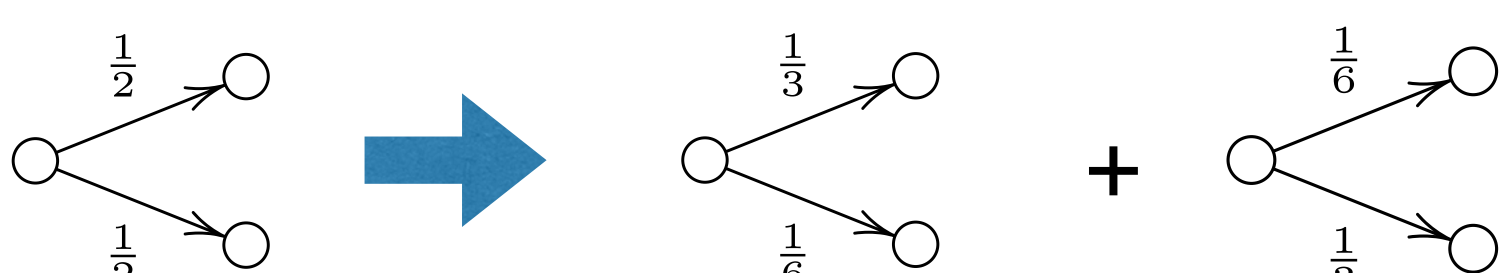
(d) **($f_{12}^{\langle \mathfrak{a} \rangle}$, the step case)** If $\mathfrak{a}$ is a successor ordinal, then for each $y \in Y_1$ and $A_1, \dots, A_n \in \mathfrak{F}_X$,

$$\int_{x \in X_2} \tau(x)(\{a\} \times A_1 \times \cdots \times A_n) f_{12}^{\langle \mathfrak{a} \rangle}(y)(\mathrm{d}x) \leq \int_{y_1, \dots, y_n \in Y} f^{\langle \mathfrak{a}-1 \rangle}(y_1)(A_1) \cdot \cdots \cdot f^{\langle \mathfrak{a}-1 \rangle}(y_n)(A_n) \cdot \theta_{12}(y)(\{a\} \times \mathrm{d}y_1 \times \cdots \times \mathrm{d}y$$

Here $f^{\langle \mathfrak{a} \rangle}$ is defined as above.

(e) **($f_{12}^{\langle \mathfrak{a} \rangle}$, the limit case)** If $\mathfrak{a}$ is a limit ordinal, then for each $y \in Y_1$ and $A \in \mathfrak{F}_{X_2}$, $f_{12}^{\langle \mathfrak{a} \rangle}(y)(A) \leq \bigvee_{\mathfrak{a}' < \mathfrak{a}} f_{12}^{\langle \mathfrak{a}' \rangle}(y)(A)$.

- Dividing requirement



Fair Simulation without Dividing for Probabilistic Büchi Automata

- For **finite-state** probabilistic Büchi **word** automata, we can remove the dividing requirement

Def:

A *fair matrix simulation from $\mathscr{A}$ to $\mathscr{B}$* is a matrix $A \in [0,1]^{Y \times X}$ satisfying the following conditions. (Here $M_{\mathscr{A},i}(a) \in [0,1]^{X_i \times X}$, $M_{\mathscr{B},j}(a) \in [0,1]^{Y_j \times Y}$ and $A_{ji} \in [0,1]^{Y_j \times X_i}$ are the obvious partial matrices of $M_{\mathscr{A}}(a) \in [0,1]^{X \times X}$, $M_{\mathscr{B}}(a) \in [0,1]^{Y \times Y}$ and $A \in [0,1]^{Y \times X}$, respectively. Moreover, $\leq$ denotes the elementwise order between matrices.)

O. The matrix A is a substochastic matrix, i.e. $\forall y \in Y.\ \sum_{x \in X} A_{y,x} \leq 1$.

A. The matrix A is a *forward matrix simulation from $\mathscr{A}$ to $\mathscr{B}$*, i.e. $\forall a \in \mathsf{A}.\ A \cdot M_{\mathcal{X}}(a) \leq M_{\mathcal{Y}}(a) \cdot A$.

B. There exist a pair of increasing sequences of matrices of length $\overline{\mathfrak{a}} \leq \omega$

$$A_{11}^{\langle 0 \rangle} \leq A_{11}^{\langle 1 \rangle} \leq \cdots \leq A_{11}^{\langle \overline{\mathfrak{a}} \rangle} \in [0,1]^{Y_1 \times X_1} \quad \text{and} \quad A_{12}^{\langle 0 \rangle} \leq A_{12}^{\langle 1 \rangle} \leq \cdots \leq A_{12}^{\langle \overline{\mathfrak{a}} \rangle} \in [0,1]^{Y_1 \times X_2}$$

such that:

(a) **(Approximate A_{11} and A_{12})** We have $A_{11}^{\langle \overline{\mathfrak{a}} \rangle} = A_{11}$ and $A_{12}^{\langle \overline{\mathfrak{a}} \rangle} = A_{12}$.

(b) **($A_{11}^{\mathfrak{a}}$)** For each $\mathfrak{a} \leq \overline{\mathfrak{a}}$ and $a \in \mathsf{A}$ we have: $A_{11}^{\langle \mathfrak{a} \rangle} \cdot M_{\mathcal{X},1}(a) \ \leq\ M_{\mathcal{Y},1}(a) \cdot \begin{pmatrix} A_{11}^{\langle \mathfrak{a} \rangle} & A_{12}^{\langle \mathfrak{a} \rangle} \\ A_{21} & A_{22} \end{pmatrix}$.

(c) **($A_{12}^{\mathfrak{a}}$, the base case)** The 0-th approximant $A_{12}^{\langle 0 \rangle}$ is the zero matrix O.

(d) **($A_{12}^{\mathfrak{a}}$, the step case)** For each $\mathfrak{a} < \overline{\mathfrak{a}}$ and $a \in \mathsf{A}$: $A_{12}^{\langle \mathfrak{a}+1 \rangle} \cdot M_{\mathcal{X},2}(a) \ \leq\ M_{\mathcal{Y},1}(a) \cdot \begin{pmatrix} A_{11}^{\langle \mathfrak{a} \rangle} & A_{11}^{\langle \mathfrak{a} \rangle} \\ A_{21} & A_{22} \end{pmatrix}$.

(e) **($A_{12}^{\mathfrak{a}}$, the limit case)** When $\overline{\mathfrak{a}} = \omega$, $(A_{12}^{\langle \omega \rangle})_{y,x} = \sup_{\mathfrak{a}' < \omega} (A_{12}^{\langle \mathfrak{a}' \rangle})_{y,x}$ for each $y \in Y_1$ and $x \in X_2$.

Applicability and Future Work

- Our notion can prove (quantitative) inclusion between **generative** probabilistic Büchi automata

$$\forall C \subseteq \mathsf{A}^{\omega}.\ \mathbf{Pr}\big(w \in C \text{ is accepted by } \mathcal{A}\big) \leq \mathbf{Pr}\big(w \in C \text{ is accepted by } \mathcal{B}\big)$$

  - For comparing probabilistic systems wrt. a logic

$$\underbrace{\mathcal{A}}_{\textbf{PrA}} \otimes \underbrace{B_{\varphi}}_{\textbf{BA}} \sqsubseteq \underbrace{\mathcal{B}}_{\textbf{PrA}} \otimes \underbrace{B_{\varphi}}_{\textbf{BA}} \implies \mathbf{Pr}(\mathcal{A} \models \varphi) \leq \mathbf{Pr}(\mathcal{B} \models \varphi)$$

  - Matrix simulation for probable innocence [Hasuo et al., '10] → security verification?

- **Reactive** probabilistic Büchi automata are more extensively studied as a (qualitative) language acceptor **[Baier & Größer, '05]**

$$L^{\mathsf{B}}_{>0}(x) = \Big\{ w \mid \mathbf{Pr}\big(w \text{ is accepted}\big) > 0 \Big\}$$

  - More expressible than nondeterministic Büchi **[Baier & Größer, '05]**
  - Language inclusion is undecidable **[Baier et. al., '08]**

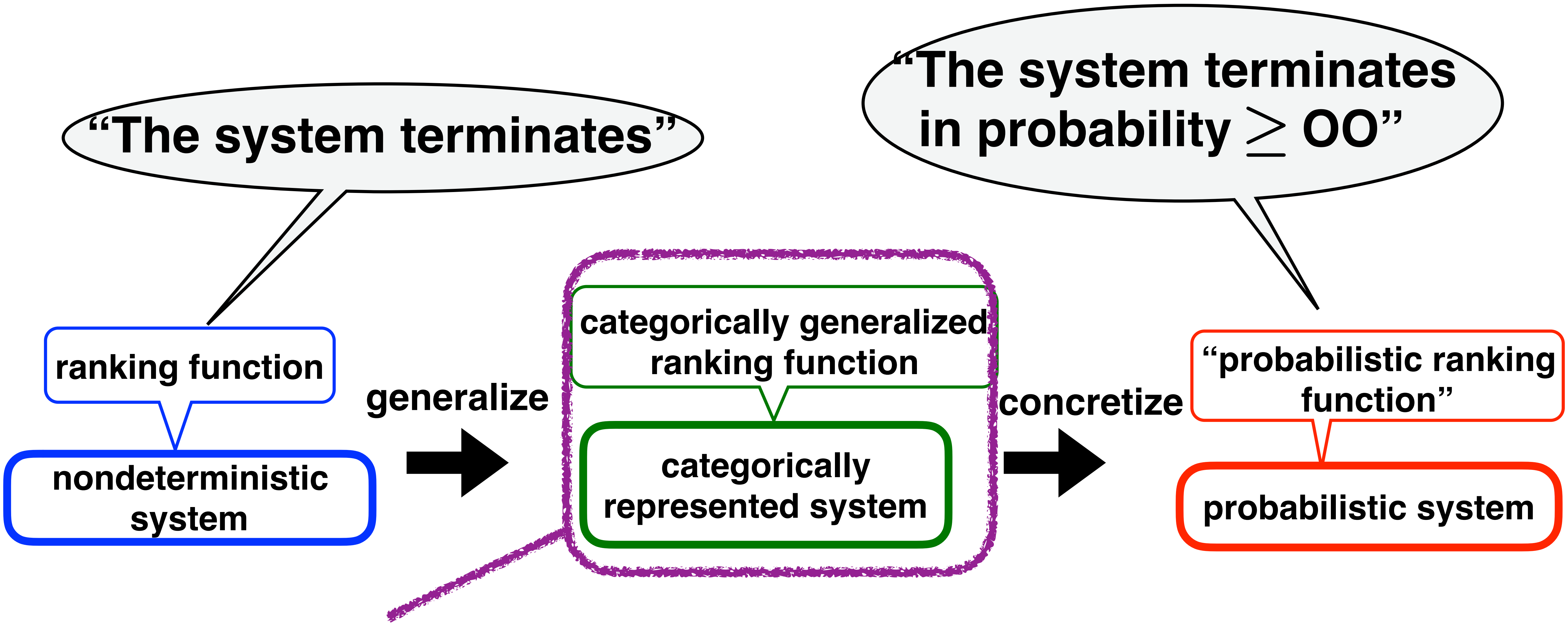
➡ **Future work**

generative: $X \to \mathcal{D}(\mathsf{A} \times X)$ **reactive:** $X \times \mathsf{A} \to \mathcal{D}(X)$

Outline

- Overview
- Short Preliminaries on Category Theory
- Categorical Trace Semantics for Büchi and Parity Automata
(Chapter 3, [U., Shimizu & Hasuo, CONCUR ’16] [U., & Hasuo, CMCS ’18])
- Categorical Fair Simulation (Chapter 4, [U. & Hasuo, LMCS ’17])
- Categorical Ranking Function (Chapter 5, [U., Hara & Hasuo, LICS ’17])
- γ-Scaled Submartingale for Probabilistic Programs and its Synthesis
(Chapter 6, [Takisaka, Oyabu, U. & Hasuo, ATVA ‘18])
- Conclusion

Overview



We prove soundness at this level ➡ **soundness**

- We follow existing result [Hasuo, ’15] for categorically characterizing behaviors of systems

Ranking Function [Floyd, '67]

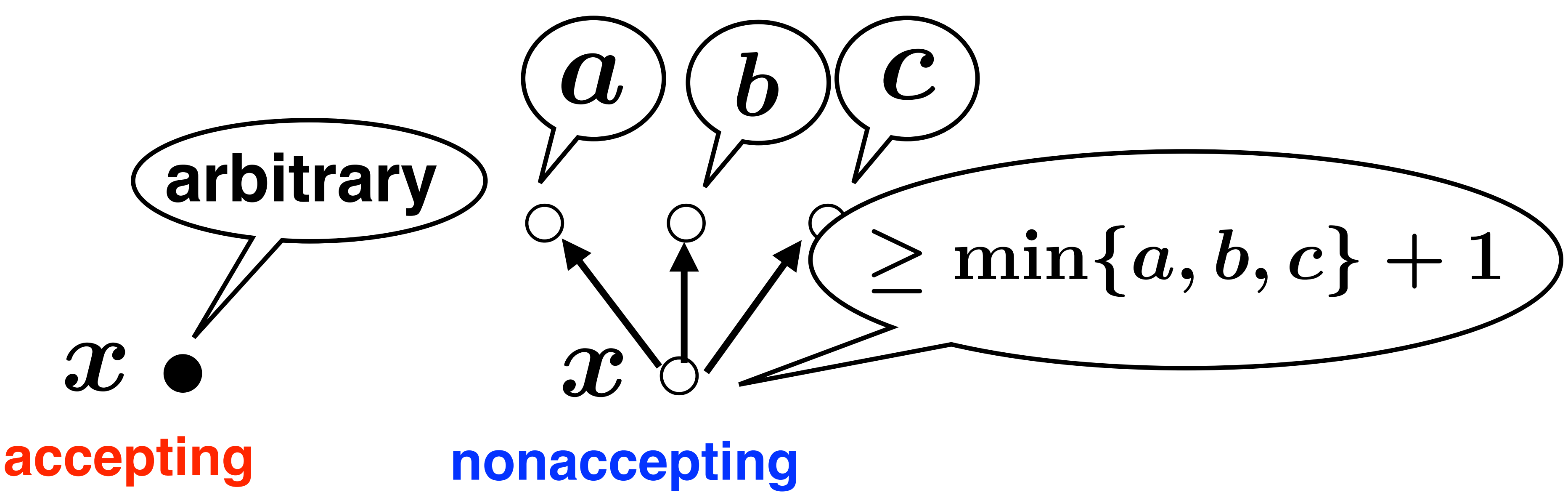
- A method for checking reachability

Def:

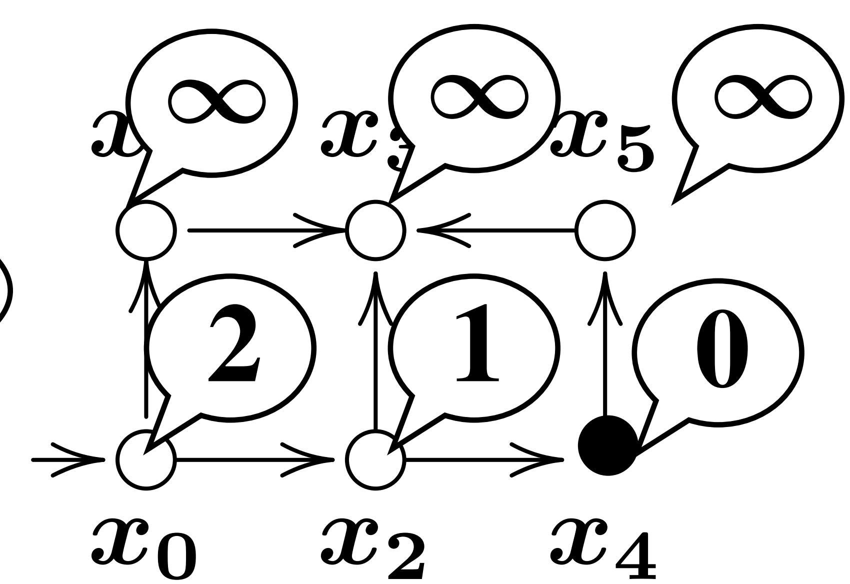
A function $\boldsymbol{b : X \to \mathbb{N}_\infty}$ is a **ranking function** if:

$$\min_{x \to x'} b(x') + 1 \leq b(x)$$

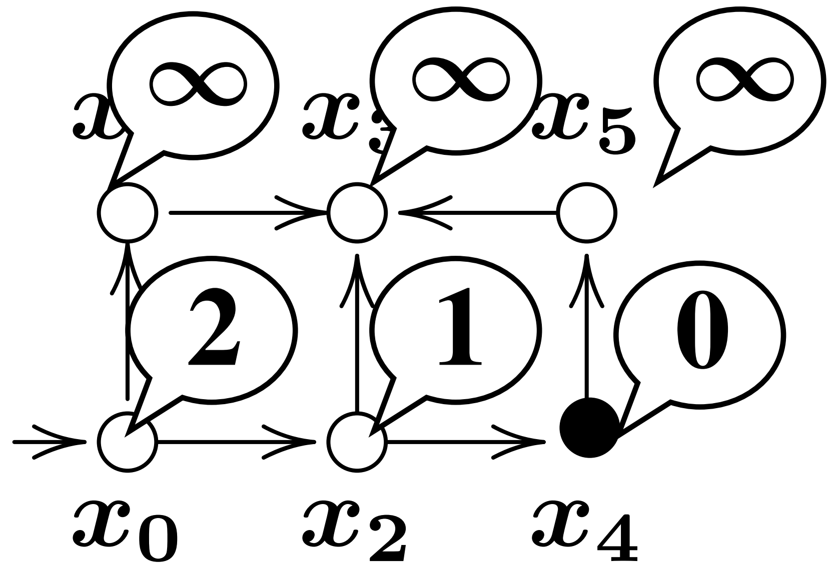
for each nonaccepting state $\boldsymbol{x}$ $\quad$ ($\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$)



- Example:



Soundness of Ranking Functions



$$\boldsymbol{b}(\boldsymbol{x}) \geq \begin{pmatrix} \text{distance to an} \\ \text{accepting state from } \boldsymbol{x} \end{pmatrix}$$

Thm: (see e.g. [Floyd, PSAM '67])

$\boldsymbol{b}$ is a ranking function and $\boldsymbol{b}(\boldsymbol{x}) < \infty$ $\Rightarrow$ an accepting state is reachable from $\boldsymbol{x}$

Ranking Function → Ranking Arrow

Def:

A function $b : X \to \mathbb{N}_\infty$ is a **ranking function** if:

$$\min_{x \to x'} b(x') + 1 \leq b(x)$$

for each nonaccepting state x $\quad (\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\})$

Def:

A *ranking domain* wrt. $\sigma : F\Omega \to \Omega$ is a triple

$$(r : FR \to R,\ q : R \to \Omega,\ \sqsubseteq_R) \quad \text{s.t.}$$

1. R is a complete lattice and $\Phi_{c,r}$ is monotone
2. q is monotone, $\perp$-preserving and continuous
3. $q \circ r \sqsubseteq \sigma \circ Fq$ 4. r is corecursive

Def:

An arrow $b : X \to R$ is a *ranking arrow* wrt. $(r, q, \sqsubseteq_R)$ if:

$$b \sqsubseteq_R r \circ Fb \circ c$$

Categorical Ranking Function

Def:

A *ranking domain* wrt. $\sigma : F\Omega \to \Omega$ is a triple

$$(\, r : FR \to R,\ q : R \to \Omega,\ \sqsubseteq_R \,) \quad \text{s.t.}$$

1. R is a complete lattice and $\Phi_{c,r}$ is monotone
2. q is monotone, $\bot$-preserving and continuous
3. $q \circ r \sqsubseteq \sigma \circ Fq$ 4. r is corecursive

Def:

An arrow $b : X \to R$ is a *ranking arrow* wrt. $(r, q, \sqsubseteq_R)$ if:

$$b \sqsubseteq_R r \circ Fb \circ c$$

58

fix a ranking domain

notion of ranking function

$$\begin{tikzcd}
FX \arrow[r, "Fb"'] \arrow[dr, phantom, "\rotatebox{90}{$\sqsubseteq$}"] & FR \arrow[r, "Fq"'] \arrow[d, "r"'] \arrow[dr, phantom, "\sqsubseteq"] & F\Omega \arrow[d, "\sigma"'] \\
X \arrow[u, "c"'] \arrow[r, "b"] & R \arrow[r, "q"] & \Omega
\end{tikzcd}$$

Categorical Soundness Theorem

Thm: (see e.g. [Floyd, PSAM '67])

$\boldsymbol{b}$ is a ranking function and $\boldsymbol{b}(\boldsymbol{x}) < \infty$ $\Rightarrow$ an accepting state is reachable from $\boldsymbol{x}$

?

Categorical Characterization of Reachability

(see e.g. [Hasuo '15])

- Reachability is often modeled as the **least fixed point**
- We model reachability as the **least coalgebra-algebra homomorphism**

$$\begin{tikzcd} & FX \arrow[r, "F[\![\mu\sigma]\!]_c"] & F\Omega \arrow[d, "\sigma"] & \\ \textbf{coalgebra} & X \arrow[u, "c"] \arrow[r, "[\![\mu\sigma]\!]_c"] \arrow[ur, phantom, "=_\mu"] & \Omega & \leftarrow\textbf{ordered} \end{tikzcd}$$

algebra

Categorical Soundness Theorem

Thm: (see e.g. [Floyd, PSAM '67])

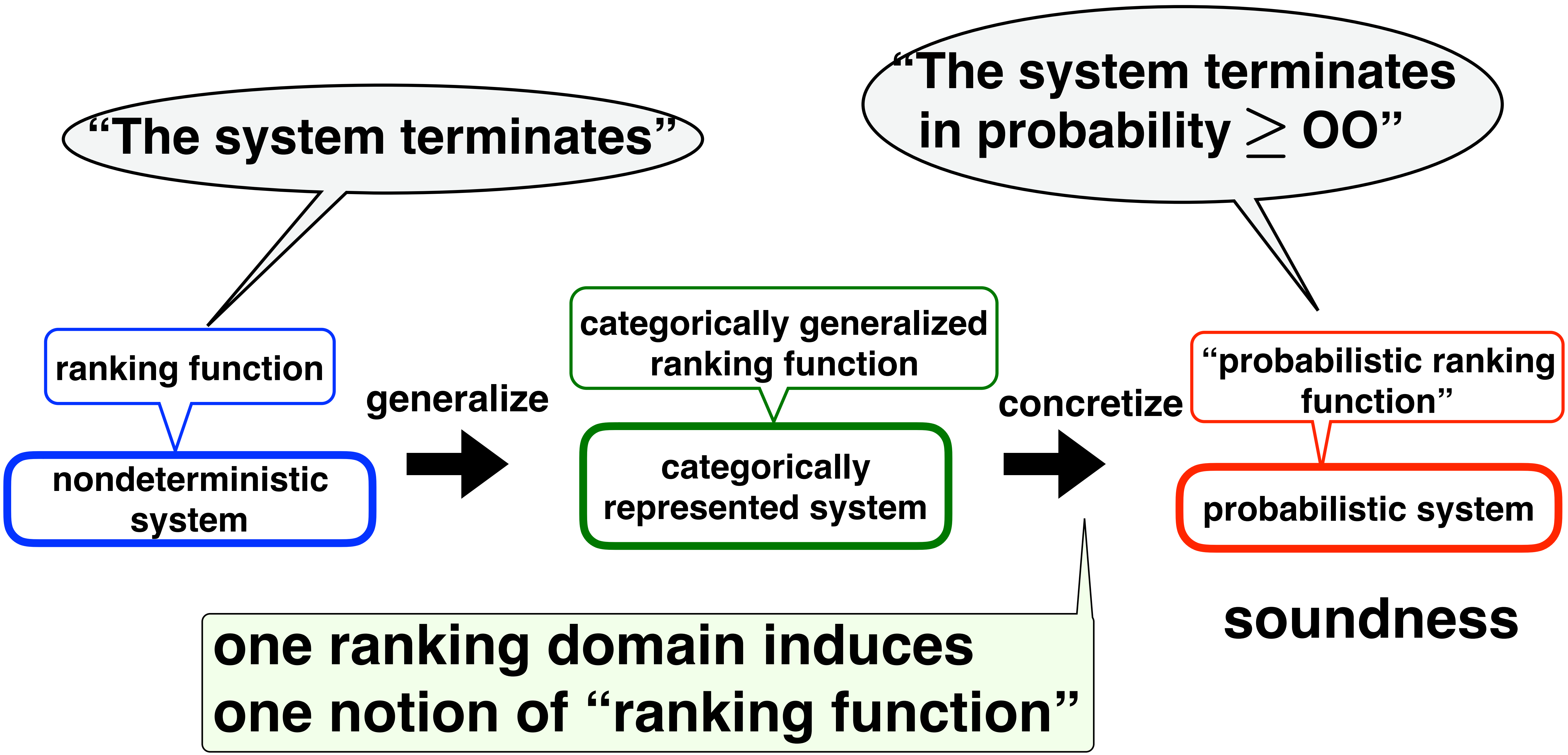
$$\boldsymbol{b} \text{ is a ranking function} \implies \begin{aligned} &\{x \mid b(x) < \infty\} \\ &\subseteq \left\{ x \;\middle|\; \begin{array}{r} \text{accepting states} \\ \text{reachable} \end{array} \right\} \end{aligned}$$

$$\begin{tikzcd}
FX \arrow[r, "Fb"'] \arrow[dr, phantom, "\rotatebox{90}{$\sqsubseteq$}"] & FR \arrow[r, "Fq"'] \arrow[d, "r"'] \arrow[dr, phantom, "\sqsubseteq"] & F\Omega \arrow[d, "\sigma"'] \\
X \arrow[u, "c"'] \arrow[r, "b"] \arrow[rr, bend right, "{[\![\mu\sigma]\!]_c}"'] & R \arrow[r, "q"] \arrow[d, phantom, "\rotatebox{-90}{$\sqsubseteq$}"] & \Omega \\
& {} &
\end{tikzcd}$$

Thm (soundness):

$$\boldsymbol{b} \text{ is a ranking arrow wrt. } (\boldsymbol{r}, \boldsymbol{q}, \sqsubseteq_{\boldsymbol{R}}) \implies \boldsymbol{q} \circ \boldsymbol{b} \sqsubseteq [\![\boldsymbol{\mu\sigma}]\!]_{\boldsymbol{c}}$$

Concretization



- We induced two definitions of “probabilistic ranking function”

Distribution-valued Ranking Function

Def:

For a probabilistic transition system, a function $b : X \to \mathcal{D}\mathbb{N}_\infty$ is a **distribution-valued ranking function** if:

$$\forall a \in \mathbb{N}_\infty. \left(\sum_{x' \in X} \mathrm{Pr}(x \to x') \cdot b(x') \right)([0, a-1]) \;\geq\; b(x)([0, a])$$

By soundness of (categorical) ranking arrows,

Thm:

$$b(x)([0, \infty)) \;\leq\; \mathbf{Pr}\begin{pmatrix} \text{an accepting state} \\ \text{is reached from } x \end{pmatrix}$$

Quantitative reasoning

γ-scaled Submartingale

Def:

For $\gamma \in (0,1)$, a function $\boldsymbol{b} : \boldsymbol{X} \to [\mathbf{0},\mathbf{1}]$ is a γ **-scaled submartingale** if:

$$\gamma \cdot \sum_{x' \in X} \mathbf{Pr}(x \to x') \cdot b(x') \;\geq\; b(x)$$

By soundness of (categorical) ranking arrows,

Thm:

$$b(x) \;\leq\; \mathbf{Pr}\left(\begin{array}{c}\text{an accepting state}\\ \text{is reached from } x\end{array}\right)$$

Quantitative reasoning

Related Work

- More popular problem: **almost-sure termination**

$$\mathbf{Pr}\big(\text{an accepting state is reached}\big) = \mathbf{1}$$

  - Many existing work

(e.g. [Esparza et. al., CAV ’12], [Fioriti & Hermanns, POPL ’15], etc…)

  - A ranking function-notion is known (**ranking supermartingale**)

[Chakarov & Sankaranarayanan, CAV ’13]

- In contrast, our notions can prove

$$\mathbf{Pr}\big(\text{an accepting state is reached}\big) \geq \bigcirc\bigcirc$$

(quantitative reasoning)

  - Existing algorithm: [Chatterjee, Novotný & Žikelić, ’17]
  - We shall compare in the next part
  - “basic and fundamental questions for the static analysis of probabilistic programs” ([Chatterjee, Novotný & Žikelić, ’17])

Outline

- Overview
- Short Preliminaries on Category Theory
- Categorical Trace Semantics for Büchi and Parity Automata
  (Chapter 3, [U., Shimizu & Hasuo, CONCUR ’16] [U., & Hasuo, CMCS ’18])
- Categorical Fair Simulation (Chapter 4, [U. & Hasuo, LMCS ’17])
- Categorical Ranking Function (Chapter 5, [U., Hara & Hasuo, LICS ’17])
- γ-Scaled Submartingale for Probabilistic Programs and its Synthesis
  (Chapter 6, [Takisaka, Oyabu, U. & Hasuo, ATVA ‘18])
- Conclusion

Target

Probabilistic Program + invariant + terminal configuration

- probabilistic program
  - while program
    + probabilistic branching if prob(0.2) then …
    + probabilistic assignment x := Gauss(0,1)
  - model for:
    - randomized algorithms
    - physical phenomena

Example

```
                v := 10
{0 <= v}        [v < 1]
                while 1 <= v do
{1 <= v}          if prob(0.75) then
{1 <= v}            v := v - 1
                  else
{1 <= v}            v := v + 1
                  fi
                od
```

- invariant
  - specify reachable states
  - make synthesis of γ-scaled submartingale easy
  - synthesis algorithm exists (e.g. [Katoen et al., SAS ’10])
- terminal configuration
  - specify accepting states

Template-based Synthesis of Ranking Supermartingale

[Chakarov & Sankaranarayanan, CAV 2013], [Chatterjee et al., CAV 2016]

- Existing algorithm for **ranking supermartingale** is applicable

Def ([Chakarov & Sankaranarayanan, CAV ’13]):

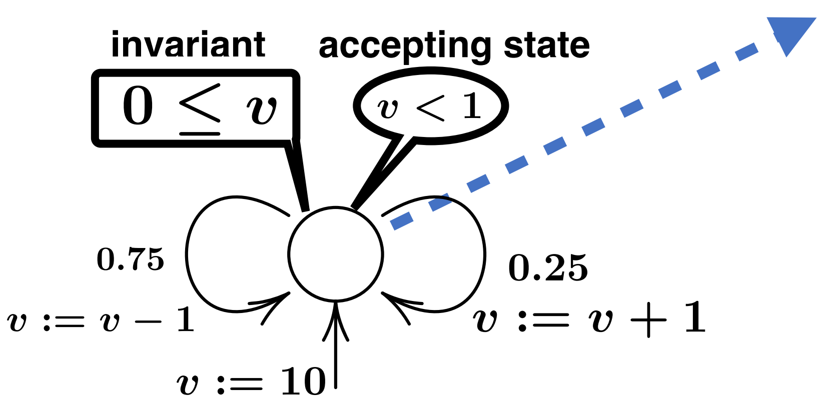
A function $b : X \to [0, \infty]$ is a **ranking supermartingale** if:

$$\sum_{x' \in X} \Pr(x \to x') \cdot b(x') + 1 \;\leq\; b(x)$$

Thm:

b is a ranking supermartingale and $b(x) < \infty$ $\Longrightarrow$ $\Pr\left(\begin{array}{r}\text{an accepting state}\\ \text{is reached}\end{array}\right) = 1$

① translate the program to a **probabilistic control flow graph**



② assign each location a **template**

$$av + b$$

(linear template)

③ reduce the axioms to constraints on the parameters

$\forall v \in \mathbb{R}$

$$v \geq 0 \Rightarrow av + b \geq 0$$

$$v \geq 1 \Rightarrow$$

$$av + b \geq$$

$$0.75(a(v-1)+b) + 0.25(a(v+1)+b) + 1$$

Farkas’ lemma

④ turn to a form solvable with numeric solvers

linear programming problem

(solvable with **LP solver**)

Our Implementation

- Implemented in OCaml
- Input:
  - probabilistic program
  - $\gamma \in [\mathbf{0}, \mathbf{1})$
- Output:
  - an input for an LP solver (glpk)
- Experiments conducted on MacBook Pro laptop with a Core i5 processor (2.6 GHz, 2 cores) and 16 GB RAM

Experimental Results I

- Linear template-based algorithm for probabilistic programs in literature

	param.	time (s)	bound	true prob.
1	$\mathbf{n = 10}$ $\mathbf{p = 0.1}$	0.023638	$\geq \mathbf{0.90437}$	$\mathbf{1 - 1.3127 \times 10^{-86}}$
	$\mathbf{n = 90}$ $\mathbf{p = 0.1}$	0.021892	$\geq \mathbf{0.10757}$	$\mathbf{1 - 2.8680 \times 10^{-10}}$
	$\mathbf{n = 10}$ $\mathbf{p = 0.9}$	0.018067	$\geq \mathbf{0}$	$\mathbf{2.8680 \times 10^{-10}}$
	$\mathbf{n = 50}$ $\mathbf{p = 0.5}$	0.018341	$\geq \mathbf{0}$	0.5
2	$\mathbf{C = 1}$	0.047402	$\geq \mathbf{0}$	—
	$\mathbf{C = 10}$	0.049987	$\geq \mathbf{0.75037}$	—
	$\mathbf{C = 20}$	0.053965	$\geq \mathbf{0.93285}$	—
	$\mathbf{C = 100}$	0.071837	$\geq \mathbf{0.95676}$	—
3	$\mathbf{C = -0.01}$ $\mathbf{D = 0.01}$	0.028786	$\geq \mathbf{0}$	—
	$\mathbf{C = -1}$ $\mathbf{D = 1}$	0.027086	$\geq \mathbf{0}$	—
	$\mathbf{C = -1}$ $\mathbf{D = 9}$	0.025237	$\geq \mathbf{0}$	—
	$\mathbf{C = -1}$ $\mathbf{D = 99}$	0.025537	$\geq \mathbf{0}$	—

simple random walk (gambler's ruin problem) [Ash, '70]

a model of air-conditioning control system [Chakarov et al, TACAS '16]

an approximated model of pendulum [Steinhardt et al, '12]

Experimental Results II

- Comparison with existing algorithm [Chatterjee, Novotný & Žikelić, ’17]
  - underapproximate reachability probability by synthesizing a **repulsing supermartingale**

- implementation is not provided

we compared probability bounds

	param.	algorithm by Chatterjee et al.	our algorithm	true prob.
4	$x = 10$	$\geq 1 - 5.2959 \times 10^{-15}$	≥ 0.90347	—
	$x = 50$	$\geq 1 - 1.25427 \times 10^{-14}$	≥ 0.58836	—
	$x = 100$	$\geq 1 - 1.8083 \times 10^{-13}$	≥ 0.19448	—
5	$\mathbf{x, y} = 1000, 10$	$\geq 1 - 1.7674 \times 10^{-16}$	≥ 0	—
	$\mathbf{x, y} = 500, 40$	$\geq 1 - 1.2930 \times 10^{-6}$	$\geq 5.9952 \times 10^{-15}$	—
	$\mathbf{x, y} = 400, 50$	$\geq 1 - 1.4439 \times 10^{-4}$	≥ 0	—
6	$\mathbf{x, y, z} = 100, 100, 100$	$\geq 1 - 1.91158 \times 10^{-70}$	$\geq 6.5725 \times 10^{-14}$	—
	$\mathbf{x, y, z} = 100, 150, 200$	$\geq 1 - 1.5420 \times 10^{-54}$	$\geq 3.2085 \times 10^{-14}$	—
	$\mathbf{x, y, z} = 300, 100, 150$	$\geq 1 - 2.1891 \times 10^{-44}$	≥ 0	—
7	$\mathbf{n, p} = 10, 0.1$	≥ 0.010200	≥ 0.90437	$1 - 1.3127 \times 10^{-86}$
	$\mathbf{n, p} = 90, 0.1$	≥ 0	≥ 0.10757	$1 - 2.8680 \times 10^{-10}$
	$\mathbf{n, p} = 10, 0.9$	≥ 0	≥ 0	2.8680×10^{-10}
	$\mathbf{n, p} = 50, 0.5$	infeasible	≥ 0	0.5

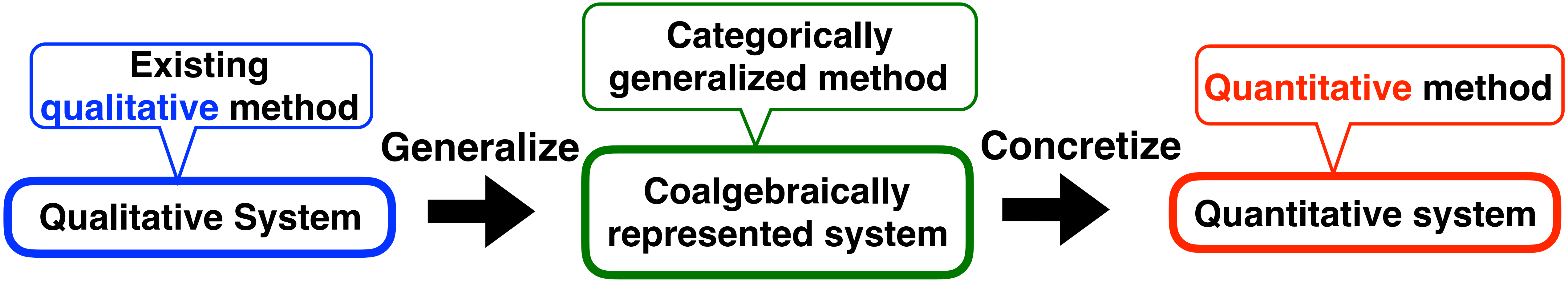
- 4-6: examples used in [Chatterjee, Novotný & Žikelić, ’17]

- 7: simple random walk

Outline

- Overview
- Short Preliminaries on Category Theory
- Categorical Trace Semantics for Büchi and Parity Automata
  (Chapter 3, [U., Shimizu & Hasuo, CONCUR ’16] [U., & Hasuo, CMCS ’18])
- Categorical Fair Simulation (Chapter 4, [U. & Hasuo, LMCS ’17])
- Categorical Ranking Function (Chapter 5, [U., Hara & Hasuo, LICS ’17])
- γ-Scaled Submartingale for Probabilistic Programs and its Synthesis
  (Chapter 6, [Takisaka, Oyabu, U. & Hasuo, ATVA ‘18])
- Conclusion

Conclusion



- For fair simulation,
  - categorical characterization of Büchi automata
  - categorical generalization of fair simulation
  - concretization to probabilistic systems

    ⇒ "probabilistic fair simulation"

- For ranking function,
  - categorical generalization of ranking function
  - concretization to probabilistic systems

    ⇒ two types of "probabilistic ranking function"
  - Implementation for γ-scaled submartingale

Refereed papers

[1] **Natsuki Urabe** and Ichiro Hasuo, “Generic Forward and Backward Simulations III: Quantitative Simulations by Matrices”. In *25th International Conference on Concurrency Theory (CONCUR 2014)*, 2014.

[2] **Natsuki Urabe** and Ichiro Hasuo, “Coalgebraic Infinite Traces and Kleisli Simulations”. In *6th Conference on Algebra and Coalgebra in Computer Science (CALCO 2015)*, 2015.

[3] **Natsuki Urabe**, Shunsuke Shimizu and Ichiro Hasuo, “Coalgebraic Trace Semantics for Büchi and Parity Automata”. In 27th International Conference on Concurrency Theory (CONCUR 2016), 2016.

[4] **Natsuki Urabe**, Masaki Hara and Ichiro Hasuo, “Categorical Liveness Checking by Corecursive Algebras”. In 2017 32nd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS), 2017.

[5] **Natsuki Urabe** and Ichiro Hasuo, “Categorical Buechi and Parity Conditions via Alternating Fixed Points of Functors”. In Coalgebraic Methods in Computer Science - 14th IFIP WG 3.1 International Workshop (CMCS), 2018.

[6] Toru Takisaka, Yuichiro Oyabu, **Natsuki Urabe** and Ichiro Hasuo, “Ranking and Repulsing Supermartingales for Approximating Reachability”. In the proceedings of ATVA 2018.

[7] Satoshi Kura, **Natsuki Urabe** and Ichiro Hasuo, “Tail Probabilities for Randomized Program Runtimes via Martingales for Higher Moments”. To appear in TACAS 2019.

[8] **Natsuki Urabe** and Ichiro Hasuo, “Quantitative Simulations by Matrices”. Information and Computation 252, 2017. (journal version of [1])

[9] **Natsuki Urabe** and Ichiro Hasuo, “Fair Simulation for Nondeterministic and Probabilistic Buechi Automata: a Coalgebraic Perspective”. Logical Methods in Computer Science 13(3), 2017.

[10] **Natsuki Urabe** and Ichiro Hasuo, “Coalgebraic Infinite Traces and Kleisli Simulations”. Logical Methods in Computer Science 14(3). (journal version of [2])

Oral presentations

1. “Generic Forward and Backward Simulations III: Quantitative Simulations by Matrices”. CONCUR 2014, Rome, Italy. September, 2014. (Presentation for [1] above)
2. “Coalgebraic Infinite Traces and Kleisli Simulations”. CALCO 2015, Nijmegen, the Netherlands. June, 2015. (Presentation for [2] above)
3. “Coalgebraic Trace Semantics for Büchi and Parity Automata”. CONCUR 2016, Quebec City, Canada. August, 2016. (Presentation for [3] above)
4. “Categorical Liveness Checking by Corecursive Algebras”. LICS 2017, Reykjavik, Iceland. June, 2017. (Presentation for [4] above)
5. “Categorical Buechi and Parity Conditions via Alternating Fixed Points of Functors”. CMCS 2018. Thessaloniki, Greece. April, 2018. (Presentation for [5] above)