Categorical Liveness Checking
by
Corecursive Algebras

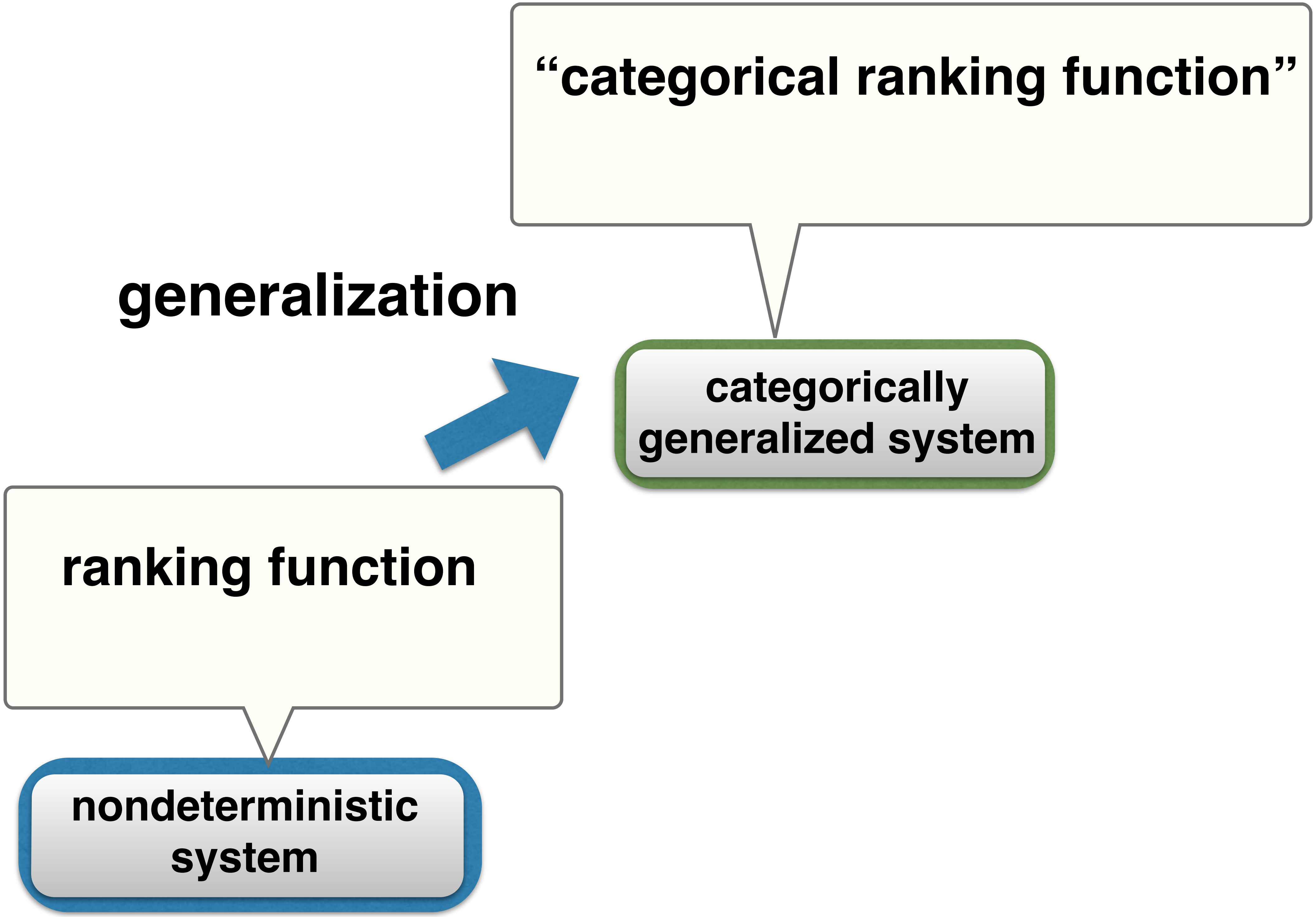
Natsuki Urabe, Masaki Hara & Ichiro Hasuo
June 20, 2017

Motivation

ranking function

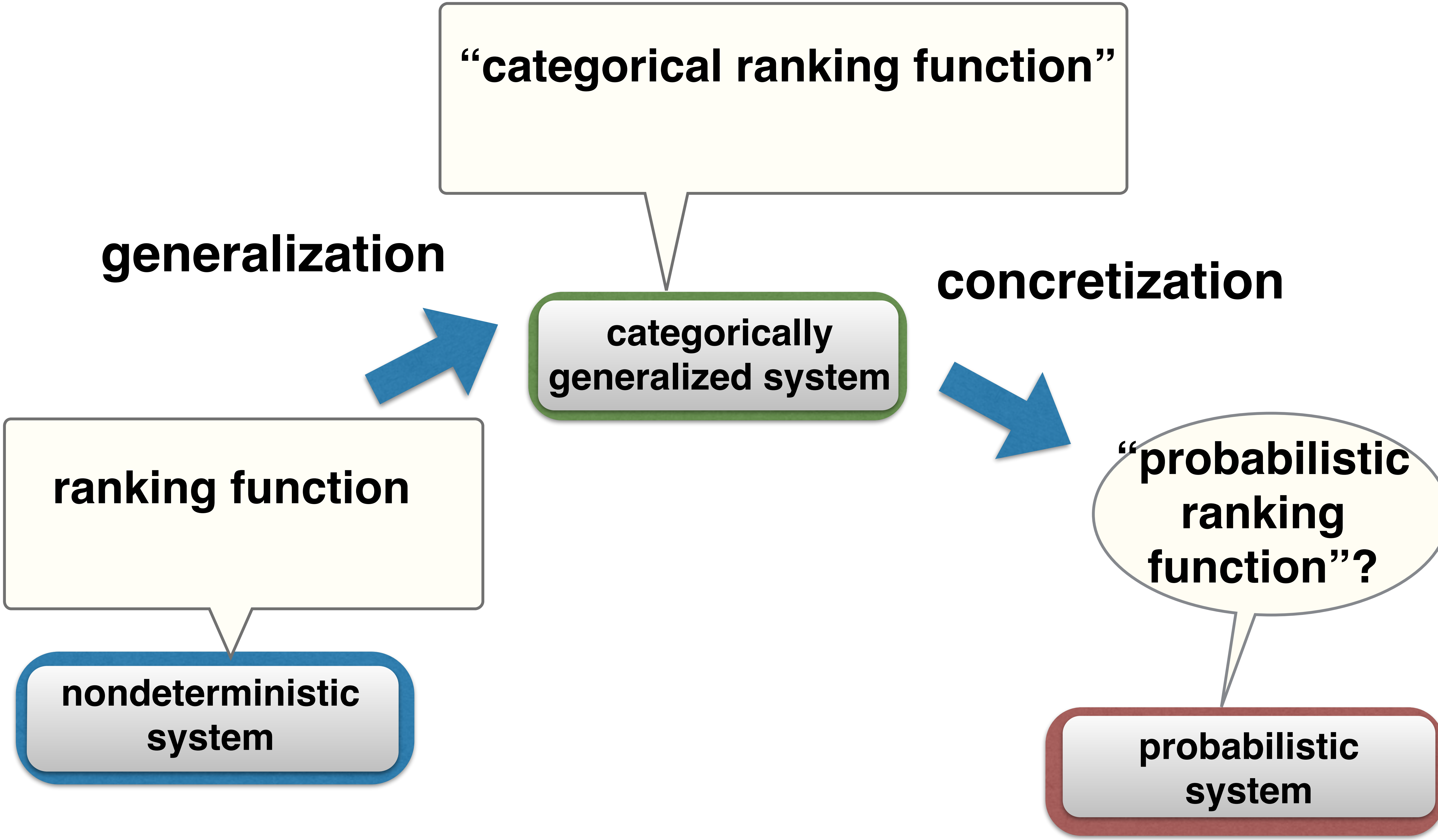
nondeterministic system

Motivation



“categorical ranking function”
generalization
categorically generalized system
ranking function
nondeterministic system

Motivation


“categorical ranking function”
generalization
categorically generalized system
concretization
ranking function
“probabilistic ranking function”?
nondeterministic system
probabilistic system

Outline

- Preliminary
  - Ranking Function
  - Coalgebra and Coalgebra-Algebra Homomorphism
- Contribution
  - Coalgebraic Ranking Function
  - Probabilistic Ranking Function
- Conclusion and Future Work

Outline

- Preliminary
  - Ranking Function
  - Coalgebra and Coalgebra-Algebra Homomorphism
- Contribution
  - Coalgebraic Ranking Function
  - Probabilistic Ranking Function
- Conclusion and Future Work

Ranking Function (see e.g. [Floyd, '67])

- A method for checking reachability

Def:

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

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

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

Ranking Function (see e.g. [Floyd, '67])

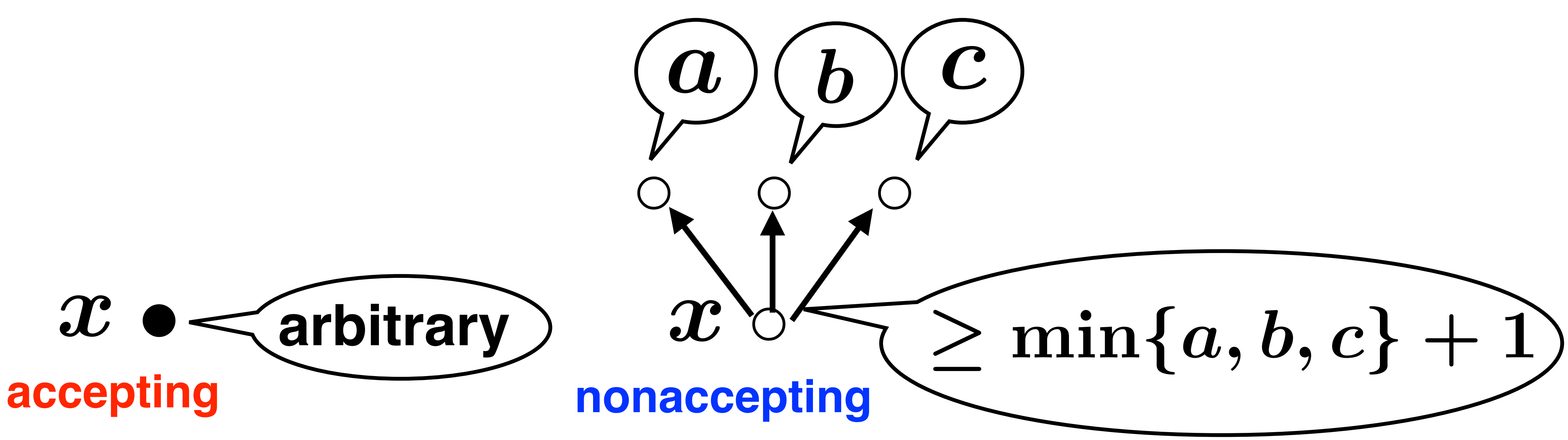
- A method for checking reachability

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 ($\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$)



Ranking Function (see e.g. [Floyd, '67])

- A method for checking reachability

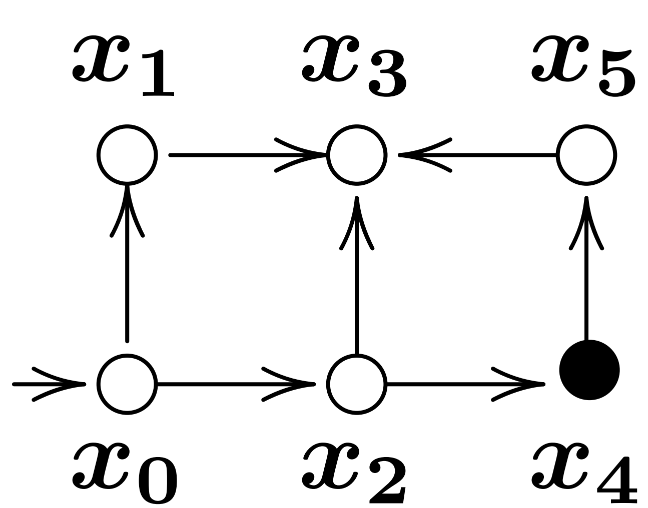
Def:

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 ($\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$)

- Example:



Ranking Function (see e.g. [Floyd, '67])

- A method for checking reachability

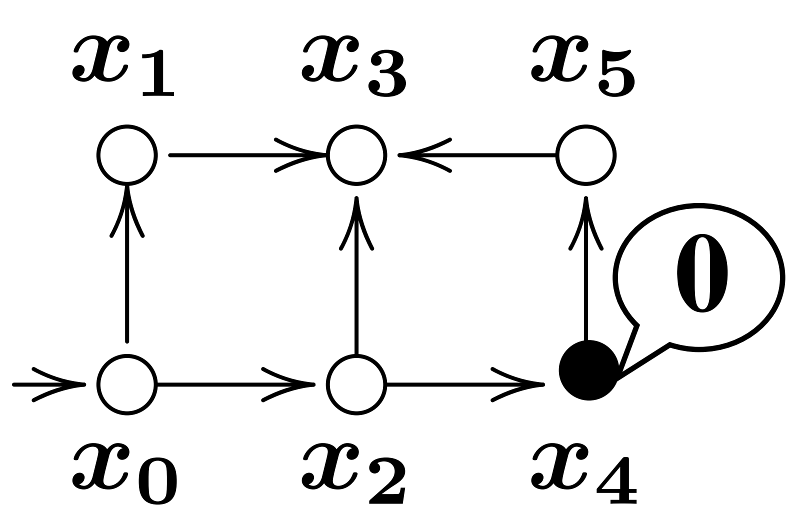
Def:

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 $\quad$ ($\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$)

- Example:



Ranking Function (see e.g. [Floyd, '67])

- A method for checking reachability

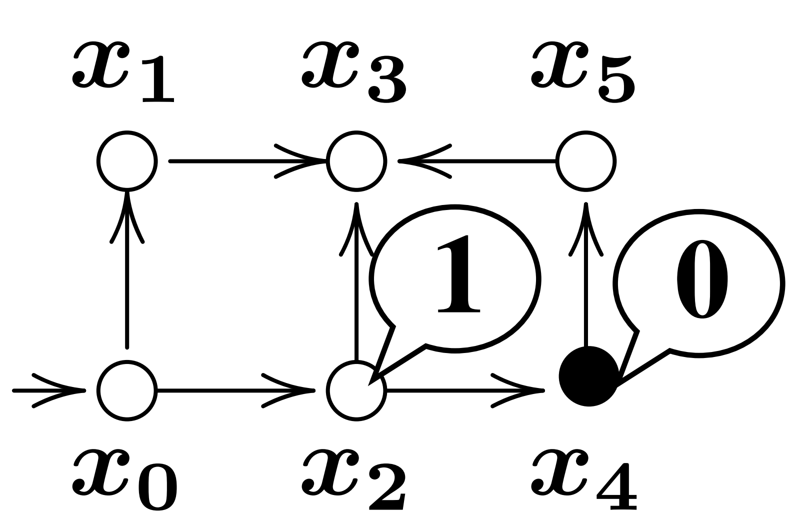
Def:

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

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

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

- Example:



Ranking Function (see e.g. [Floyd, '67])

- A method for checking reachability

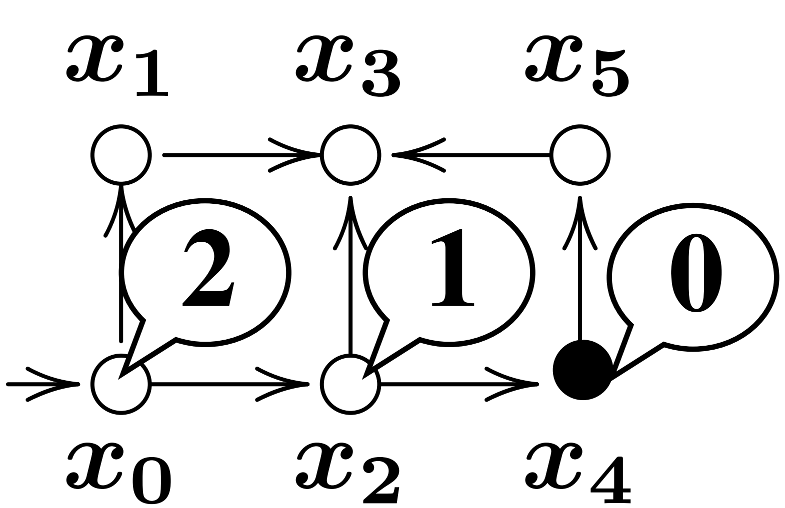
Def:

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 $\quad (\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\})$

- Example:



Ranking Function (see e.g. [Floyd, '67])

- A method for checking reachability

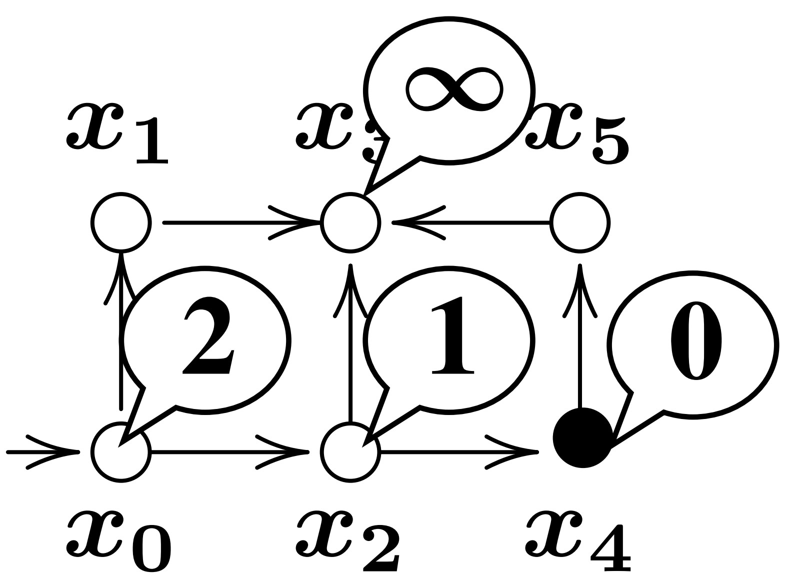
Def:

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 $\quad (\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\})$

- Example:



Ranking Function (see e.g. [Floyd, '67])

- A method for checking reachability

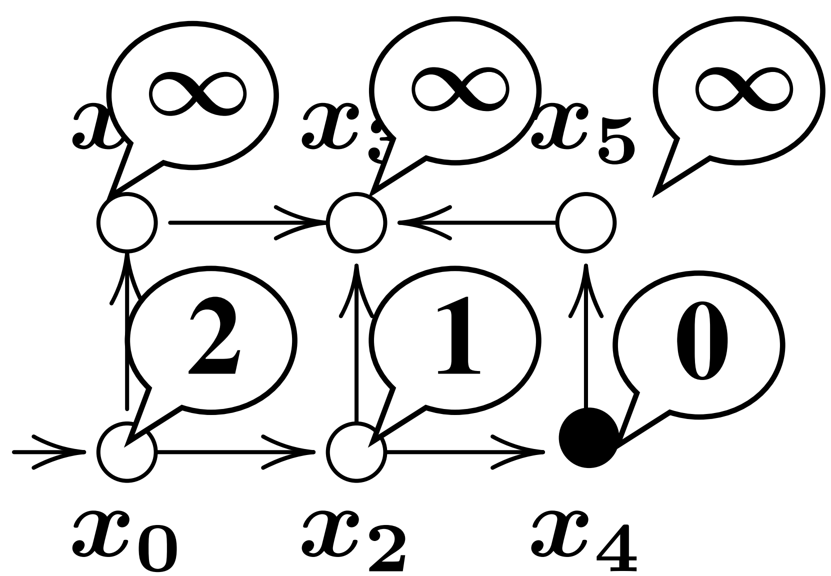
Def:

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

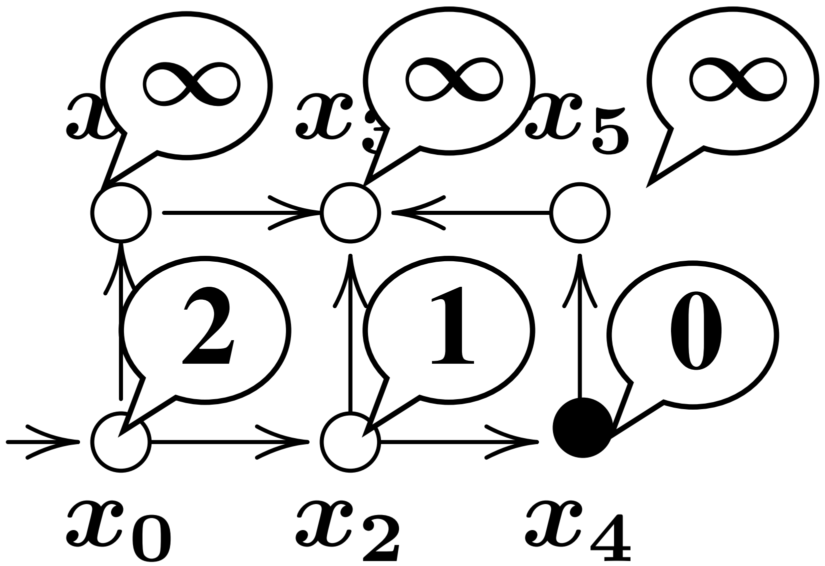
$$\min_{x \to x'} b(x') + 1 \leq b(x)$$

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

- Example:

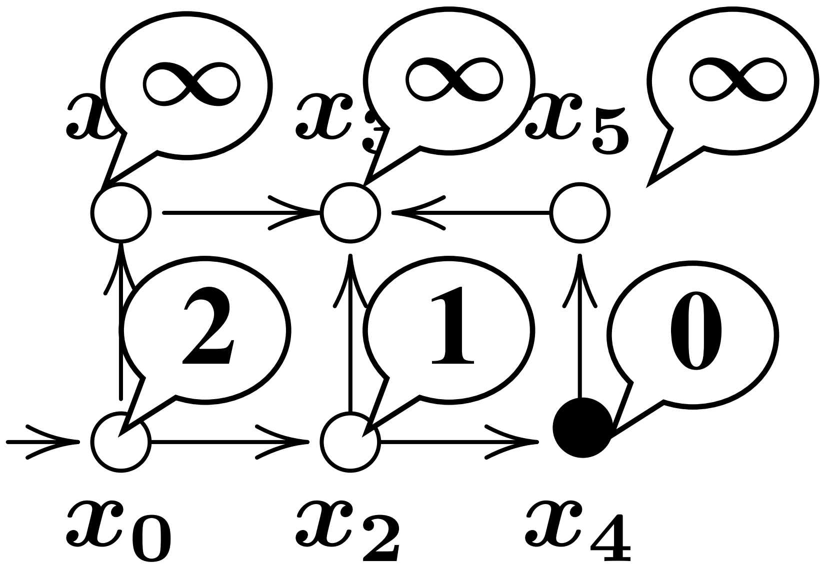


Soundness of Ranking Functions



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

Soundness of Ranking Functions

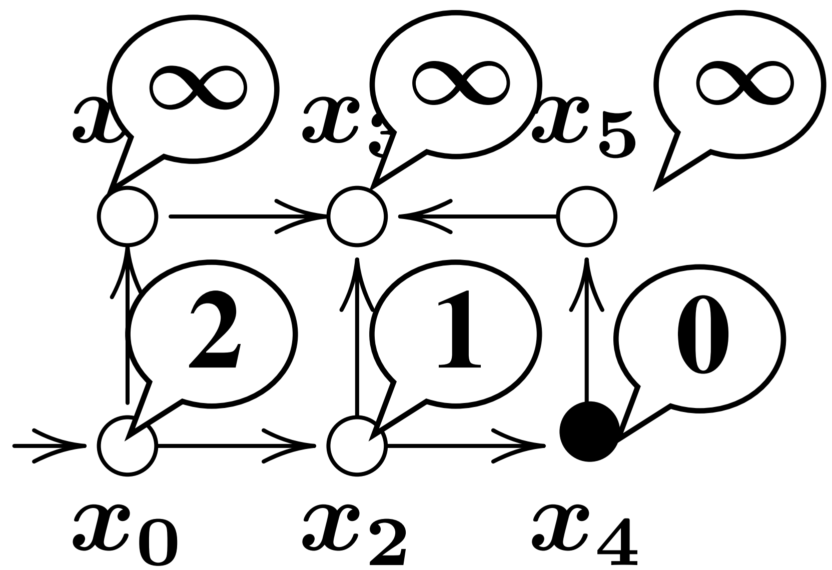


$$\boldsymbol{b}(\boldsymbol{x}) \geq \left(\begin{array}{l}\text{distance to an} \\ \text{accepting state from } \boldsymbol{x}\end{array}\right)$$

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 $\boldsymbol{x}$

Soundness of Ranking Functions



$$\boldsymbol{b}(\boldsymbol{x}) \geq \left(\begin{array}{l}\text{distance to an} \\ \text{accepting state from } \boldsymbol{x}\end{array}\right)$$

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 $\boldsymbol{x}$

➡ under-approximates the **reaching set**

Outline

- Preliminary
  - Ranking Function
  - Coalgebra and Coalgebra-Algebra Homomorphism
- Contribution
  - Coalgebraic Ranking Function
  - Probabilistic Ranking Function
- Conclusion and Future Work

Towards Categorical Generalization

- Our first goal:
  categorical generalization of **ranking function**

- We have to categorically characterize:
  - a transition system
  - a reachability to accepting states

Coalgebra

- An ($\boldsymbol{F}$-)*coalgebra* is a function of the following form:

$$\boldsymbol{X \to FX}$$

$\boldsymbol{F}$: a functor

$$\begin{array}{rcl} \boldsymbol{X} & \longmapsto & \boldsymbol{FX} \\ (\boldsymbol{f : X \to Y}) & \longmapsto & (\boldsymbol{Ff : FX \to FY}) \end{array}$$

- Coalgebras model **transition systems**

Coalgebra

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

$$X \to FX$$

F : a functor

$$\begin{array}{rcl} X & \mapsto & FX \\ (f : X \to Y) & \mapsto & (Ff : FX \to FY) \end{array}$$

- Coalgebras model **transition systems**

- Dual notion: *algebra*

$$FX \to X$$

- Algebras model **modalities**

Example I: Nondeterministic Transition System with Accepting States

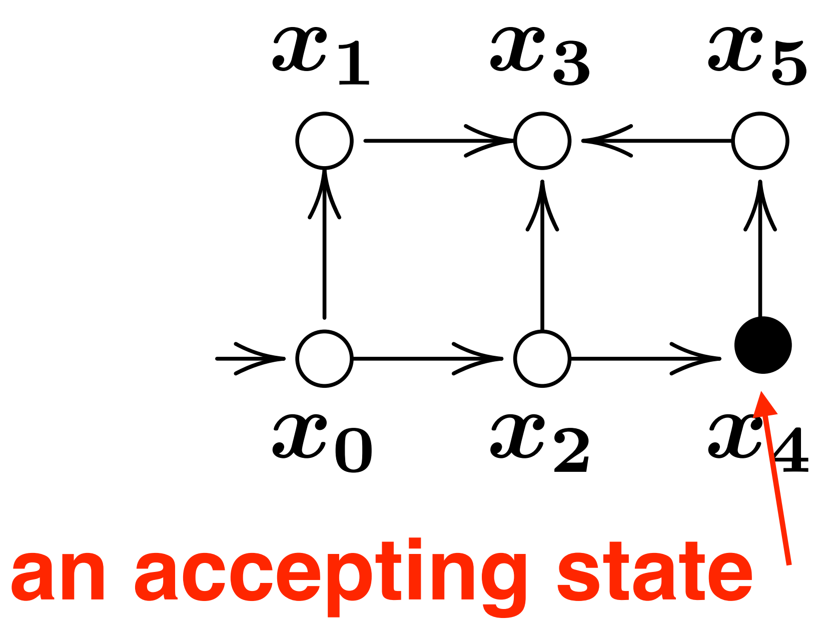
$$c : X \to \mathcal{P}X \times \{0,1\} \text{ where } \mathcal{P}X = \{A \subseteq X\}$$

$$F = \mathcal{P}(\_) \times \{0,1\}$$

Example I:
Nondeterministic Transition System with Accepting States

$$c : X \to \mathcal{P}X \times \{0,1\} \text{ where } \mathcal{P}X = \{A \subseteq X\}$$

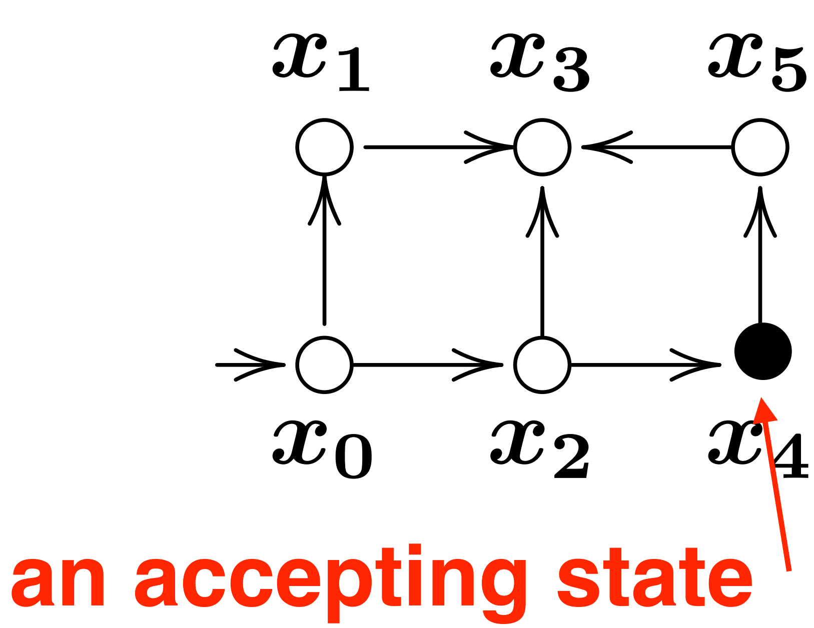
$$F = \mathcal{P}(\_) \times \{0,1\}$$



Example I:
Nondeterministic Transition System with Accepting States

$$c : X \to \mathcal{P}X \times \{0,1\} \text{ where } \mathcal{P}X = \{A \subseteq X\}$$

$$F = \mathcal{P}(\_) \times \{0,1\}$$



$$X = \{x_0, x_1, x_2, x_3, x_4, x_5\}$$

$$c : \begin{cases} x_0 \mapsto (\{x_1, x_2\}, 0) \\ x_1 \mapsto (\{x_3\}, 0) \\ \vdots \\ x_4 \mapsto (\{x_5\}, 1) \\ \vdots \end{cases}$$

Example II: Probabilistic Transition System with Accepting States

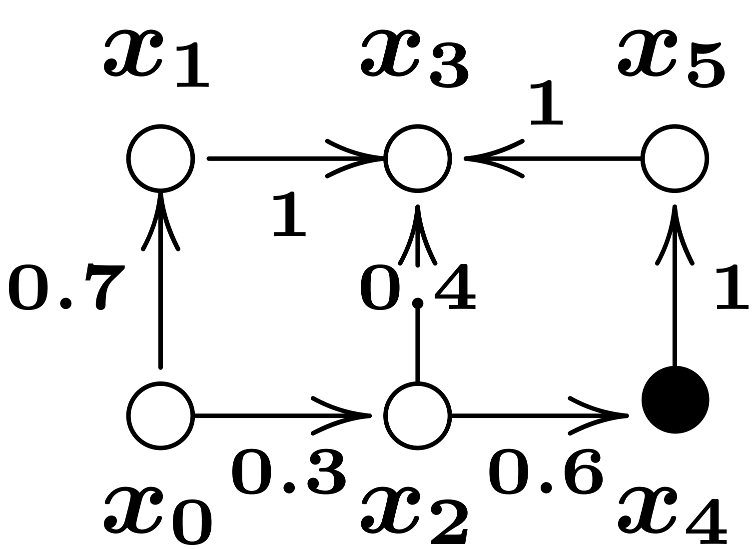
$c : X \to \mathcal{D}X \times \{0,1\}$ where

$F = \mathcal{D}(\_) \times \{0,1\}$

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

Example II: Probabilistic Transition System with Accepting States

$c : X \to \mathcal{D}X \times \{0,1\}$ where
$F = \mathcal{D}(\_) \times \{0,1\}$
$\mathcal{D}X = \{d : X \to [0,1] \mid \sum_x d(x) = 1\}$

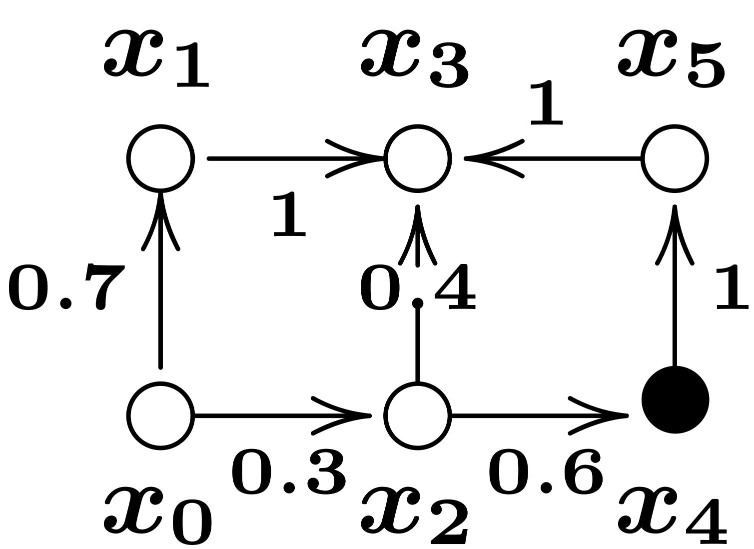


Example II: Probabilistic Transition System with Accepting States

$c : X \to \mathcal{D}X \times \{0,1\}$ where

$$F = \mathcal{D}(\_) \times \{0,1\}$$

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



$$X = \{x_0, x_1, x_2, x_3, x_4, x_5\}$$

$$c : \begin{cases} x_0 \mapsto ([x_1 \mapsto 0.7, x_2 \mapsto 0.3], 0) \\ x_1 \mapsto ([x_3 \mapsto 1], 0) \\ x_2 \mapsto ([x_3 \mapsto 0.4, x_4 \mapsto 0.6], 0) \\ \quad \vdots \end{cases}$$

Coalgebra-Algebra Homomorphism

Def:

A ***coalgebra-algebra homomorphism*** from $c : X \to FX$ to $\sigma : F\Omega \to \Omega$ is $f : X \to \Omega$ s.t. $\sigma \circ Ff \circ c = f$

$$\begin{array}{ccc} FX & \xrightarrow{Ff} & F\Omega \\ {\scriptstyle c}\uparrow & = & \downarrow{\scriptstyle \sigma} \\ X & \xrightarrow{f} & \Omega \end{array}$$

- Especially, the **least coalgebra-algebra homomorphism** $[\![\mu\sigma]\!]_c : X \to \Omega$ captures **reachability**

Coalgebra-Algebra Homomorphism

Def:

A ***coalgebra-algebra homomorphism*** from $c : X \to FX$ to $\sigma : F\Omega \to \Omega$ is $f : X \to \Omega$ s.t. $\sigma \circ Ff \circ c = f$

$$\begin{array}{ccc} FX & \xrightarrow{Ff} & F\Omega \\ {\scriptstyle c}\uparrow & = & \downarrow{\scriptstyle \sigma} \\ X & \xrightarrow{f} & \Omega \end{array}$$

- Especially, the **least coalgebra-algebra homomorphism** $[\![\mu\sigma]\!]_c : X \to \Omega$ captures **reachability**

Example:

- For nondeterministic systems, $^\exists\sigma : F\{0,1\} \to \{0,1\}$ s.t. $[\![\mu\sigma]\!]_c(x) = 1 \iff \text{an accepting state is reachable from } x$
- For probabilistic systems, $^\exists\sigma : F[0,1] \to [0,1]$ s.t. $[\![\mu\sigma]\!]_c(x) = \mathbf{Prob}(\text{reach an accepting state from } x)$

Remark: Coalgebra-Algebra Homomorphism is Fixed Point

(see e.g. [Jacobs, LMCS 2015])

Def:

$$\Phi_{c,\sigma} : \left(X \xrightarrow{f} \Omega \right) \mapsto \left(X \xrightarrow{c} FX \xrightarrow{Ff} F\Omega \xrightarrow{\sigma} \Omega \right)$$

(predicate lifting + precomposing c => weakest precondition)

Remark: Coalgebra-Algebra Homomorphism is Fixed Point

(see e.g. [Jacobs, LMCS 2015])

Def:

$$\Phi_{c,\sigma} : \; X \xrightarrow{f} \Omega \;\longmapsto\; \begin{array}{ccc} FX & \xrightarrow{Ff} & F\Omega \\ {\scriptstyle c}\uparrow & & \downarrow{\scriptstyle \sigma} \\ X & & \Omega \end{array}$$

(predicate lifting + precomposing c => weakest precondition)

Prop:

$$\begin{array}{ccc} FX & \xrightarrow{Ff} & F\Omega \\ {\scriptstyle c}\uparrow & = & \downarrow{\scriptstyle \sigma} \\ X & \xrightarrow{f} & \Omega \end{array} \quad \Leftrightarrow \quad f \text{ is a fixed point of } \Phi_{c,\sigma}$$

Remark: Coalgebra-Algebra Homomorphism is Fixed Point

(see e.g. [Jacobs, LMCS 2015])

Def:

$$\Phi_{c,\sigma} : \; X \xrightarrow{f} \Omega \;\longmapsto\; \begin{array}{ccc} FX & \xrightarrow{Ff} & F\Omega \\ {\scriptstyle c}\uparrow & & \downarrow{\scriptstyle \sigma} \\ X & & \Omega \end{array}$$

(predicate lifting + precomposing c => weakest precondition)

Prop:

$$\begin{array}{ccc} FX & \xrightarrow{Ff} & F\Omega \\ {\scriptstyle c}\uparrow & = & \downarrow{\scriptstyle \sigma} \\ X & \xrightarrow{f} & \Omega \end{array} \quad \Leftrightarrow \quad f \text{ is a fixed point of } \Phi_{c,\sigma}$$

- Reachability as the **least fixed point** (see e.g. [Baier & Katoen])

reachability as the
least coalgebra-algebra homomorphism

Outline

- Preliminary
  - Ranking Function
  - Coalgebra and Coalgebra-Algebra Homomorphism
- Contribution
  - Coalgebraic Ranking Function
  - Probabilistic Ranking Function
- Conclusion and Future Work

Categorical Ranking Function

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 ($\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$)

Categorical Ranking Function

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, $\bot$-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:

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

Categorical Ranking Function

Def:

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

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

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

Def:

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

$$\boldsymbol{b \sqsubseteq_{R} r \circ Fb \circ c}$$

Categorical Ranking Function

Def:

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

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

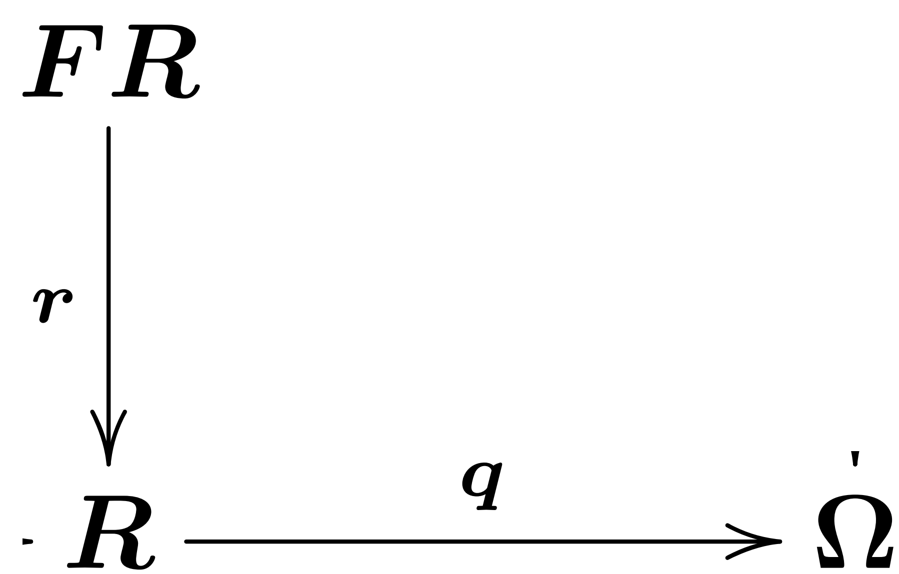
1. R is a complete lattice and $\Phi_{c,r}$ is monotone
2. q is monotone, $\bot$-preserving and continuous
3. $q \circ r \sqsubseteq \sigma \circ Fq$ 4. r is corecursive

Def:

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

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

16



Categorical Ranking Function

Def:

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

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

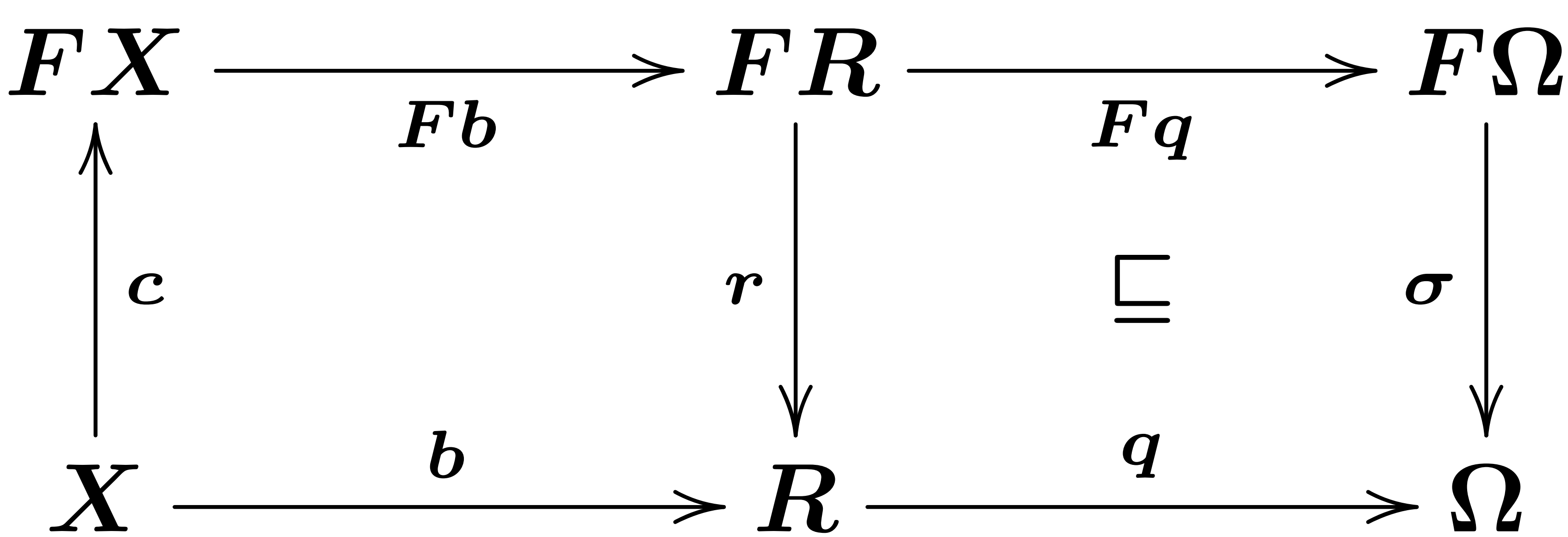
1. $\boldsymbol{R}$ is a complete lattice and $\boldsymbol{\Phi_{c,r}}$ is monotone
2. $\boldsymbol{q}$ is monotone, $\perp$-preserving and continuous
3. $\boldsymbol{q \circ r \sqsubseteq \sigma \circ Fq}$ 4. $\boldsymbol{r}$ is corecursive

Def:

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

$$\boldsymbol{b \sqsubseteq_R r \circ Fb \circ c}$$

16



Categorical Ranking Function

Def:

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

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

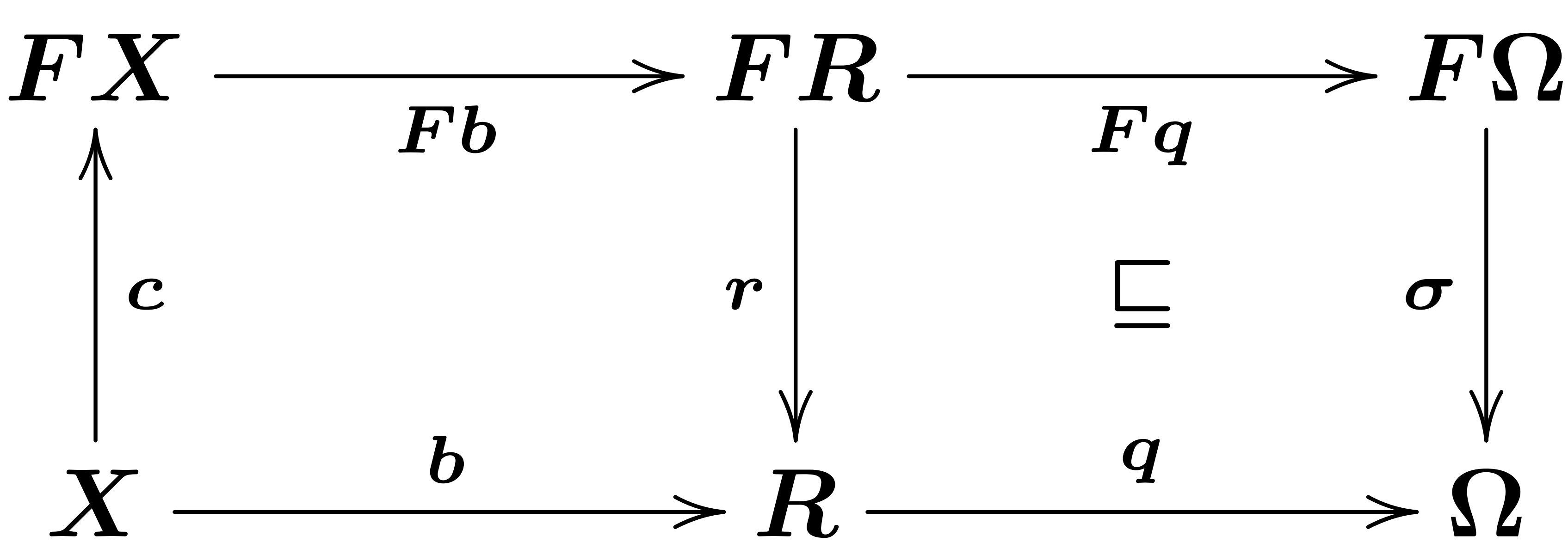
1. $\boldsymbol{R}$ is a complete lattice and $\boldsymbol{\Phi_{c,r}}$ is monotone
2. $\boldsymbol{q}$ is monotone, $\bot$-preserving and continuous
3. $\boldsymbol{q} \circ \boldsymbol{r} \sqsubseteq \boldsymbol{\sigma} \circ \boldsymbol{Fq}$ 4. $\boldsymbol{r}$ is corecursive

Def:

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

$$\boldsymbol{b} \sqsubseteq_{\boldsymbol{R}} \boldsymbol{r} \circ \boldsymbol{Fb} \circ \boldsymbol{c}$$

16



Corecursive Algebra

Def:

An algebra $r : FR \to R$ is **corecursive** if for all coalgebra $c : X \to FX$, a coalgebra-algebra homomorphism from c to r uniquely exists.

$$\begin{array}{ccc} FX & \xrightarrow{F(\!|r|\!)_c} & FR \\ c \uparrow & = & \downarrow r \\ X & \xrightarrow{(\!|r|\!)_c} & R \end{array}$$

- It has been used to ensure **productivity** of general structured corecursion [Capretta et al., SBMF '09]
- We use it to ensure **reachability** (termination)

Categorical Ranking Function

Def:

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

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

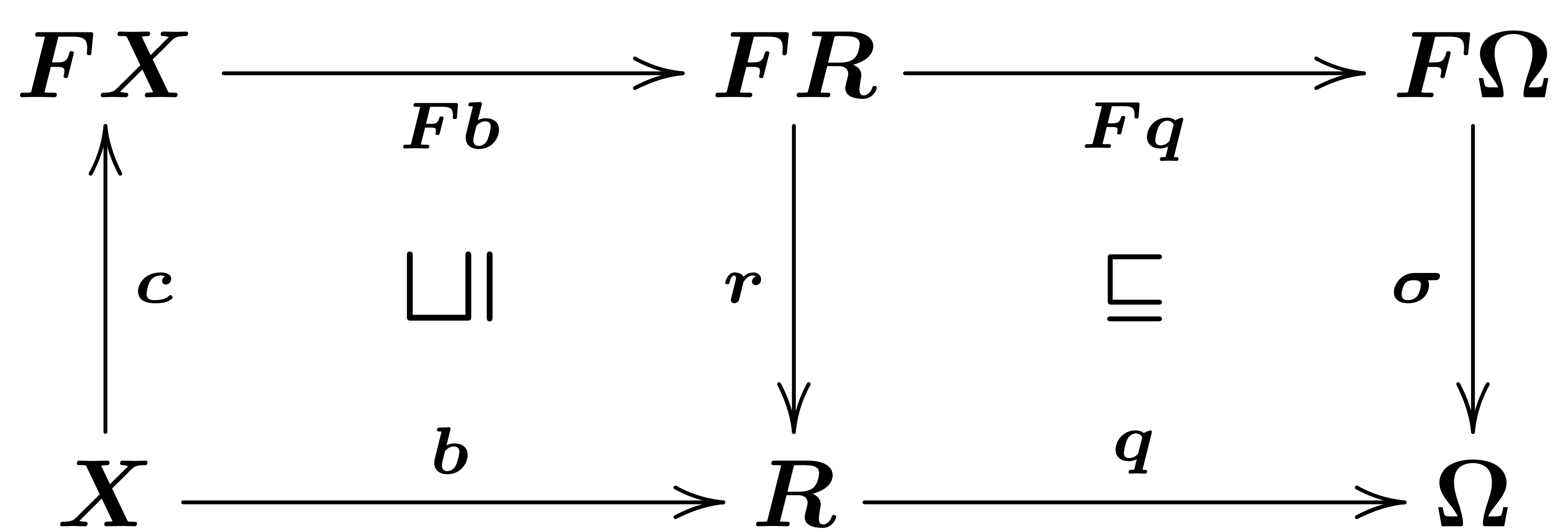
1. $\boldsymbol{R}$ is a complete lattice and $\boldsymbol{\Phi_{c,r}}$ is monotone
2. $\boldsymbol{q}$ is monotone, $\bot$-preserving and continuous
3. $\boldsymbol{q \circ r \sqsubseteq \sigma \circ Fq}$ 4. $\boldsymbol{r}$ is corecursive

Def:

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

$$\boldsymbol{b \sqsubseteq_R r \circ Fb \circ c}$$

18



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:

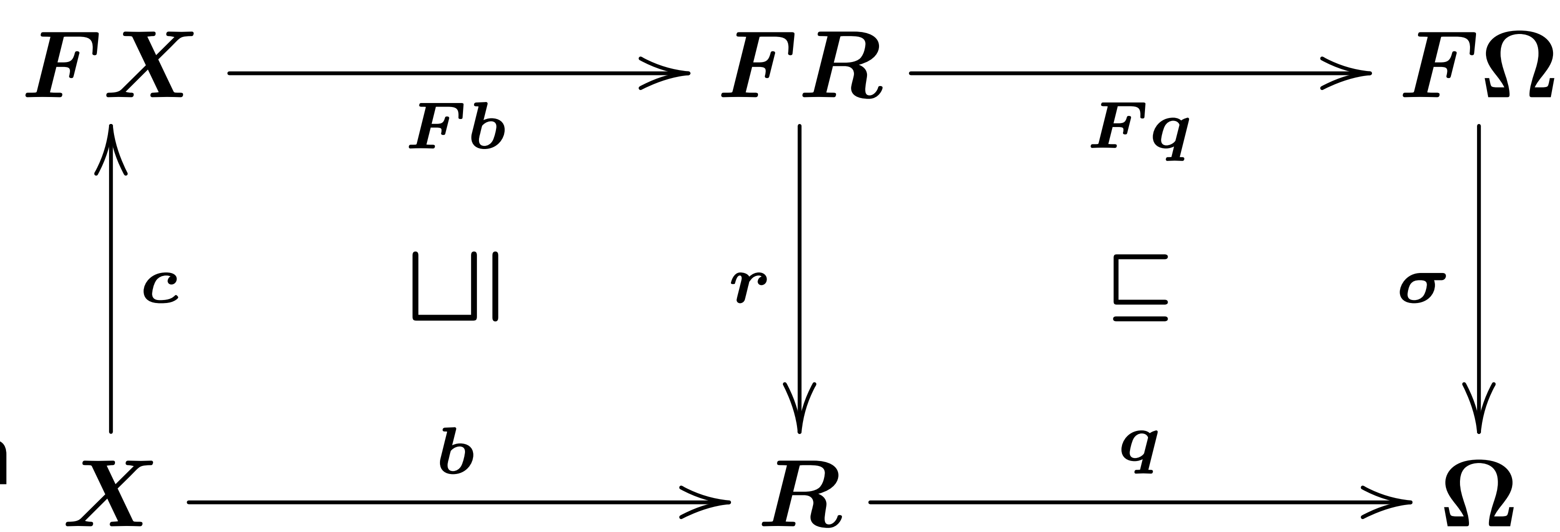
$$b \sqsubseteq_R r \circ Fb \circ c$$

18

fix a ranking domain

⬇

notion of ranking function



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 Soundness Theorem

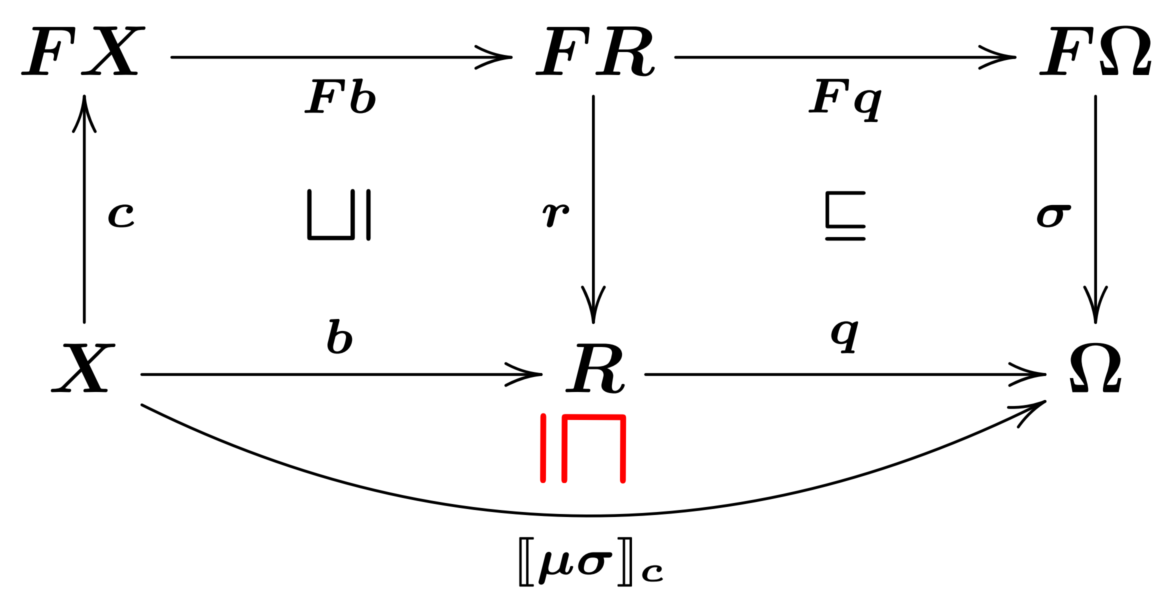
Thm: (see e.g. [Floyd, PSAM '67])

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

Categorical Soundness Theorem

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

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



Thm (soundness):

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

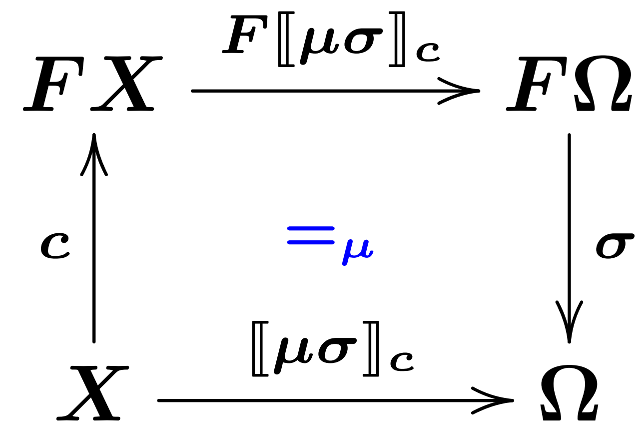
Intuition behind Corecursiveness

$$\begin{array}{ccc} FX & \xrightarrow{F[\![\mu\sigma]\!]_c} & F\Omega \\ {\scriptstyle c}\uparrow & =_\mu & \downarrow{\scriptstyle \sigma} \\ X & \xrightarrow{[\![\mu\sigma]\!]_c} & \Omega \end{array}$$

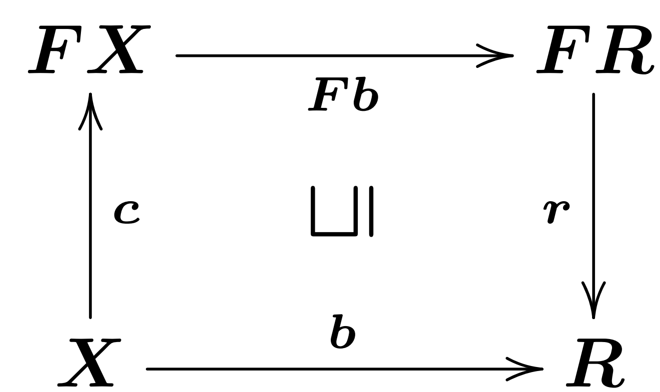
- Aim of ranking function:
  under-approximate the **least** **fixed point**

Intuition behind Corecursiveness

- Aim of ranking function:
  under-approximate the **least** **fixed point**

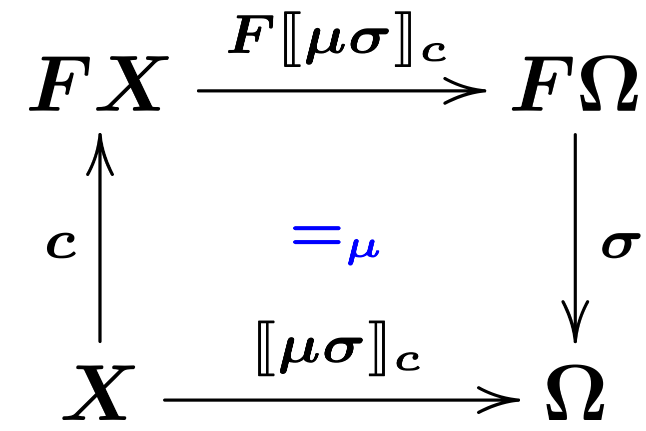


- Ranking arrow is a **post-fixed point**

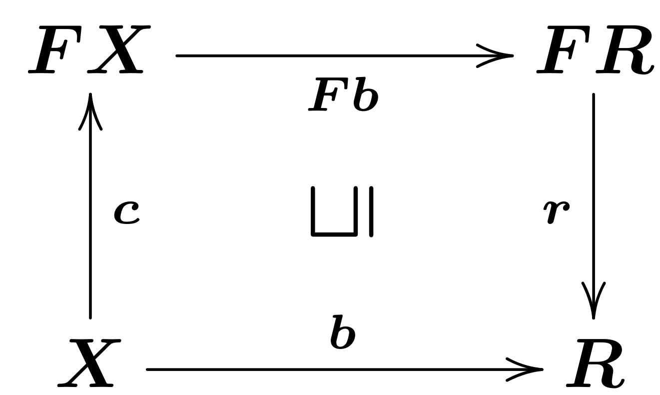


Intuition behind Corecursiveness

- Aim of ranking function:
  under-approximate the **least fixed point**

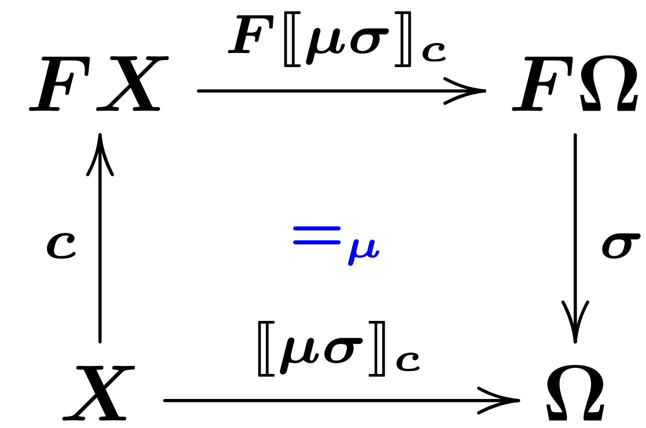


- Ranking arrow is a **post-fixed point**

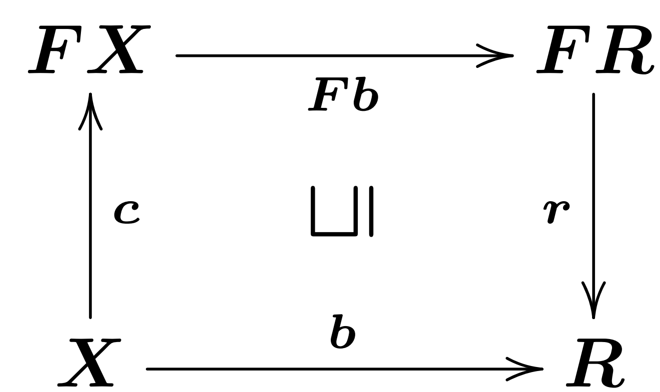


It under-approximates the **greatest** fixed point
(the Knaster-Tarski theorem)

Intuition behind Corecursiveness



- Aim of ranking function:
  under-approximate the **least** **fixed point**



- Ranking arrow is a **post-fixed point**

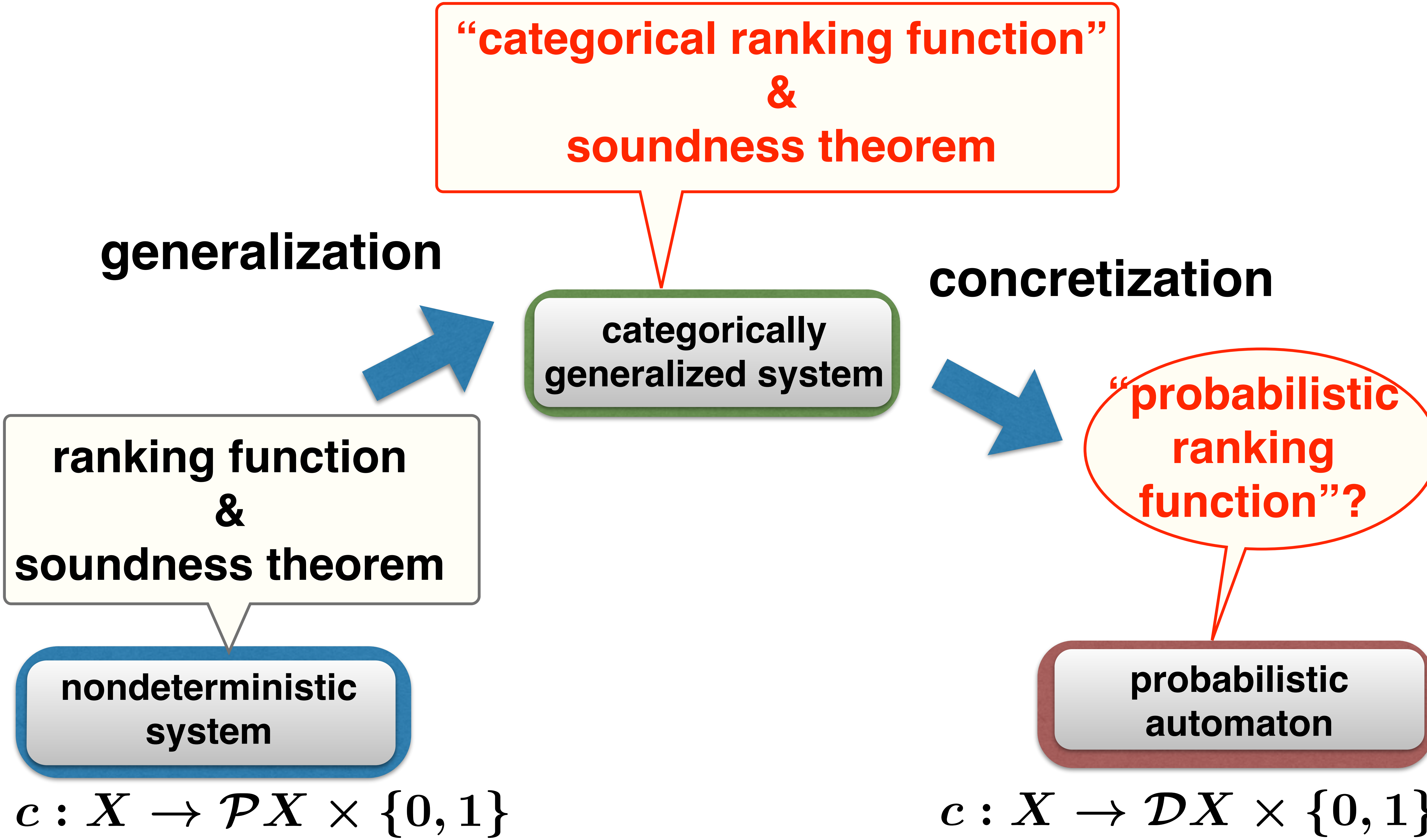
It under-approximates the **greatest** fixed point
(the Knaster-Tarski theorem)

we collapse the least and the greatest fixed points
(i.e. unique coalgebra-algebra homomorphism)

Outline

- Preliminary
  - Ranking Function
  - Coalgebra and Coalgebra-Algebra Homomorphism
- Contribution
  - Coalgebraic Ranking Function
  - Probabilistic Ranking Function
- Conclusion and Future Work

Concretization



Ranking Supermartingale [Chakarov et al., '13]

- A method for checking almost-sure reachability on probabilistic systems

Def:

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

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

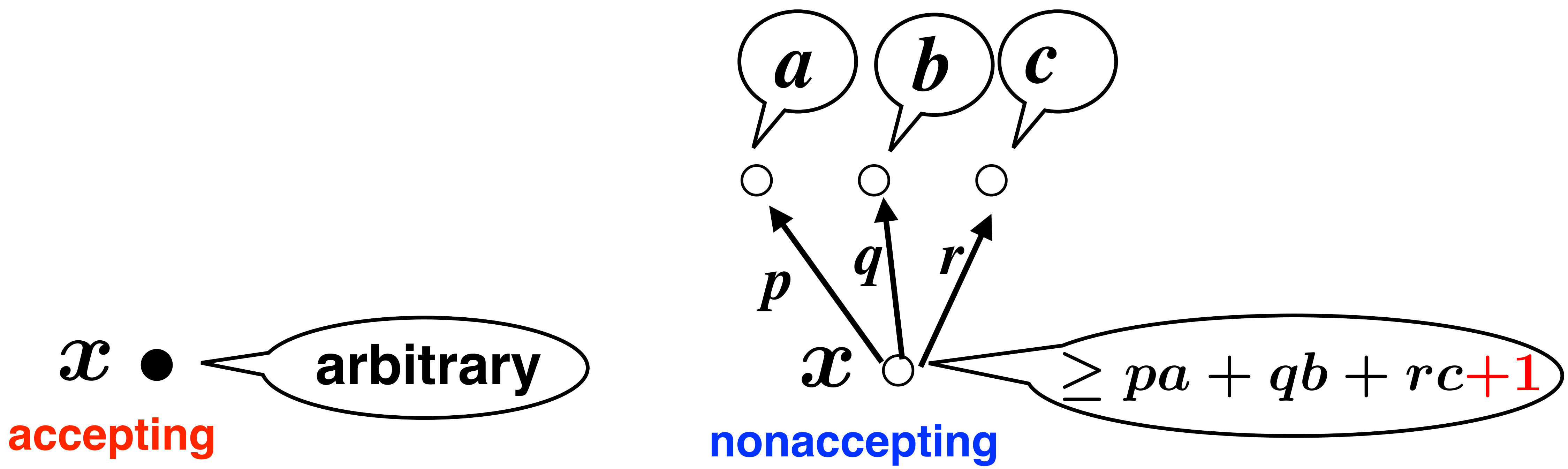
Ranking Supermartingale [Chakarov et al., '13]

- A method for checking almost-sure reachability on probabilistic systems

Def:

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

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



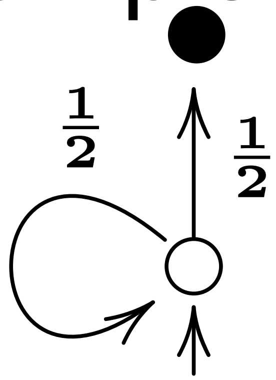
Soundness Theorem

Def:

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

$$\sum_{x' \in X} \mathbf{Prob}(x \to x') \cdot b(x') +1 \quad \leq \quad b(x)$$

- Example



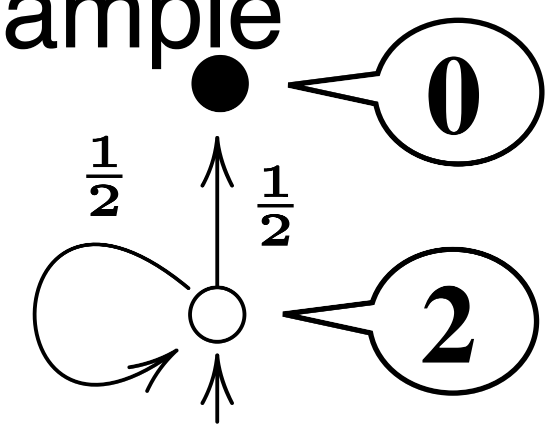
Soundness Theorem

Def:

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

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

- Example



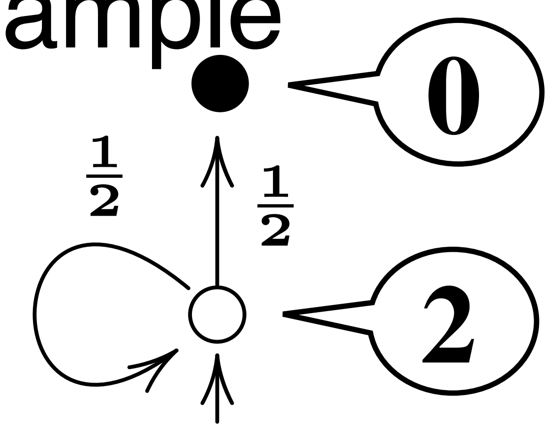
Soundness Theorem

Def:

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

$$\sum_{x' \in X} \mathbf{Prob}(x \to x') \cdot b(x') + 1 \quad \leq \quad b(x)$$

- Example



$$b(x) \geq \mathbb{E}\left(\begin{array}{l} \text{number of steps to an} \\ \text{accepting state from } x \end{array} \right)$$

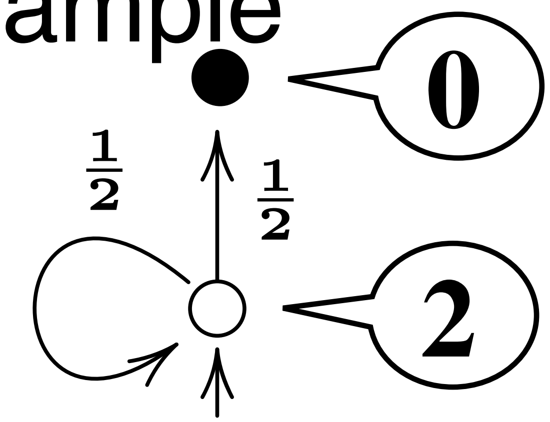
Soundness Theorem

Def:

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

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

- Example



$$b(x) \geq \mathbb{E}\left(\begin{array}{l}\text{number of steps to an} \\ \text{accepting state from } x\end{array}\right)$$

Thm:

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

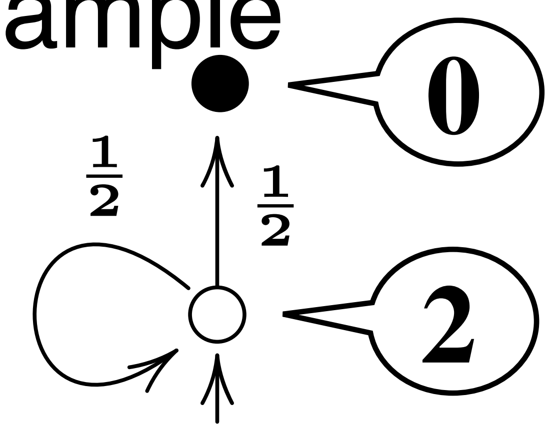
Soundness Theorem

Def:

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

$$\sum_{x' \in X} \mathrm{Prob}(x \to x') \cdot b(x') + 1 \quad \leq \quad b(x)$$

- Example



$$b(x) \geq \mathbb{E}\left(\begin{array}{l}\text{number of steps to an} \\ \text{accepting state from } x\end{array}\right)$$

Thm:

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

- Ranking supermartingale resembles to ranking function

  ➡ a ranking domain for ranking supermartingale exists?

Problem and Next Step

- We couldn't find a ranking domain $(\boldsymbol{r}, \boldsymbol{q}, \sqsubseteq_{\boldsymbol{R}})$ s.t.

$$\boldsymbol{b} \text{ is a ranking supermartingale} \iff \begin{array}{l}\boldsymbol{b} \text{ is a ranking arrow} \\ \text{wrt. } (\boldsymbol{r}, \boldsymbol{q}, \sqsubseteq_{\boldsymbol{R}})\end{array}$$

Problem and Next Step

- We couldn't find a ranking domain $(\boldsymbol{r}, \boldsymbol{q}, \sqsubseteq_{\boldsymbol{R}})$ s.t.

$$\boldsymbol{b} \text{ is a ranking supermartingale} \iff \begin{array}{l}\boldsymbol{b} \text{ is a ranking arrow} \\ \text{wrt. } (\boldsymbol{r}, \boldsymbol{q}, \sqsubseteq_{\boldsymbol{R}})\end{array}$$

➡ We decided to **give up** describing ranking supermartingales

Problem and Next Step

- We couldn't find a ranking domain $(\boldsymbol{r}, \boldsymbol{q}, \sqsubseteq_{\boldsymbol{R}})$ s.t.

$$\boldsymbol{b} \text{ is a ranking supermartingale} \iff \begin{array}{l}\boldsymbol{b} \text{ is a ranking arrow} \\ \text{wrt. } (\boldsymbol{r}, \boldsymbol{q}, \sqsubseteq_{\boldsymbol{R}})\end{array}$$

➡ We decided to **give up** describing ranking supermartingales

- Instead, we found **two ranking domains** for probabilistic systems

➡ They induces **new** definitions of ranking function (to the best of our knowledge)

Distribution-valued Ranking Supermartingale

Def:

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

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

By soundness of (categorical) ranking arrows,

Thm:

$$\boldsymbol{b}(\boldsymbol{x}) \big([\mathbf{0}, \infty) \big) \;\leq\; \mathbf{Pr} \left(\begin{array}{c} \text{an accepting state} \\ \text{is reached from } \boldsymbol{x} \end{array} \right)$$

Distribution-valued Ranking Supermartingale

Def:

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

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

By soundness of (categorical) ranking arrows,

Thm:

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

→ **Quantitative reasoning**

Scaled Noncounting Ranking Supermartingale

Def:

For $\gamma \in (0,1)$, a function $b : X \to [0,1]$ is a γ **-scaled noncounting ranking function** if:

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

By soundness of (categorical) ranking arrows,

Thm:

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

→ **Quantitative reasoning**

Outline

- Preliminary
  - Ranking Function
  - Coalgebra and Coalgebra-Algebra Homomorphism
- Contribution
  - Coalgebraic Ranking Function
  - Probabilistic Ranking Function
- Conclusion and Future Work

Conclusion

- Categorical generalization of **ranking function**
  - **Post-fixed point + corecursive algebra**
  - (Categorical) soundness theorem

- Concretization for probabilistic systems:
  - failed to describe ranking supermartingale
  - induced two new notions for liveness checking

Future Work

- Extension to Büchi/parity systems
- Implementation