Martingale-Based Methods for Reachability Probabilities

Excitements and Afterthoughts ~~about~~ in Coalgebras

Ichiro Hasuo

National Institute of Informatics

Tokyo, Japan

Supported by ERATO HASUO Metamathematics for Systems Design Project (No. JPMJER1603), JST; Grants-in-Aid No. 15KT0012 & 15K11984, JSPS; and JSPS-Inria Bilateral Joint Research Project “CRECOGI”

Overview

- Reachability in **probabilistic programs**
- **Foundation of fixed points,** in the non-probabilistic setting
  - Ranking functions, invariants
  - Foundation: Knaster-Tarski, Cousot-Cousot
- Known **supermartingale** methods
  - Roles of concentration lemmas
- Something new (from **fixed points** and **coalgebras**)
- Coalgebras: excitements, afterthoughts, our project

Based on Joint Works:

* Natsuki Urabe, Masaki Hara and Ichiro Hasuo.
  Categorical Liveness Checking by Corecursive Algebras.
  LICS 2017

* Toru Takisaka, Yuichiro Oyabu, Natsuki Urabe and Ichiro Hasuo.
  Ranking and Repulsing Supermartingales for Approximating Reachability in Probabilistic Programs.
  ATVA 2018

Probabilistic Programs

- Programs with
  - random assignment

$$x := \mathbf{Gaussian}(0, 0.2)$$

  - probabilistic branching

$$\mathbf{if}\ \mathbf{prob}(0.2)$$

    - (also nondet. assignment & branching)

```
1  x := m
2  while x > 0 do
3     if prob(p) do
4        x := x − 1
5     else
6        x := x + 1
7     fi
8  od
```

(say, $m = 16$ and $p = 0.2$)

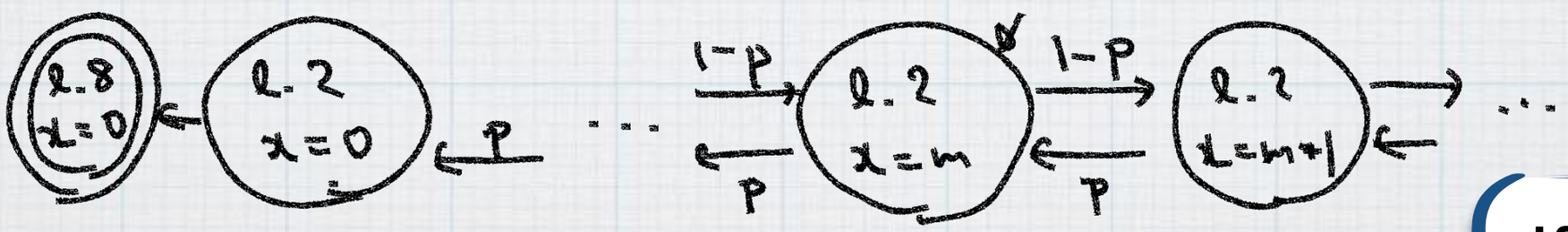
- Example: right (random walk)
- We disregard the Bayesian aspects
  - observations, conditioning, priors/posteriors, etc.
  - See e.g. [Gordon+, FOSE'14]

Reachability Probabilities in PP

```
1  x := m
2  while x > 0 do
3     if prob(p) do
4        x := x − 1
5     else
6        x := x + 1
7     fi
```

real-valued variables
➜ infinite states
➜ not for automated analysis

- **Question** What is $\mathbf{Pr}(\text{the program terminates})$?
- How do we define it?
  - Configuration graph
    - A state is a pair (program locat
    - Transition by small-step operati
    - ➜ MDP (Markov decision processes) M



- $$\mathbf{Pr}(\mathbf{Term}) = \sup_{\sigma:\ \text{scheduler}} (M^\sigma \text{ reaches } \circledcirc)$$

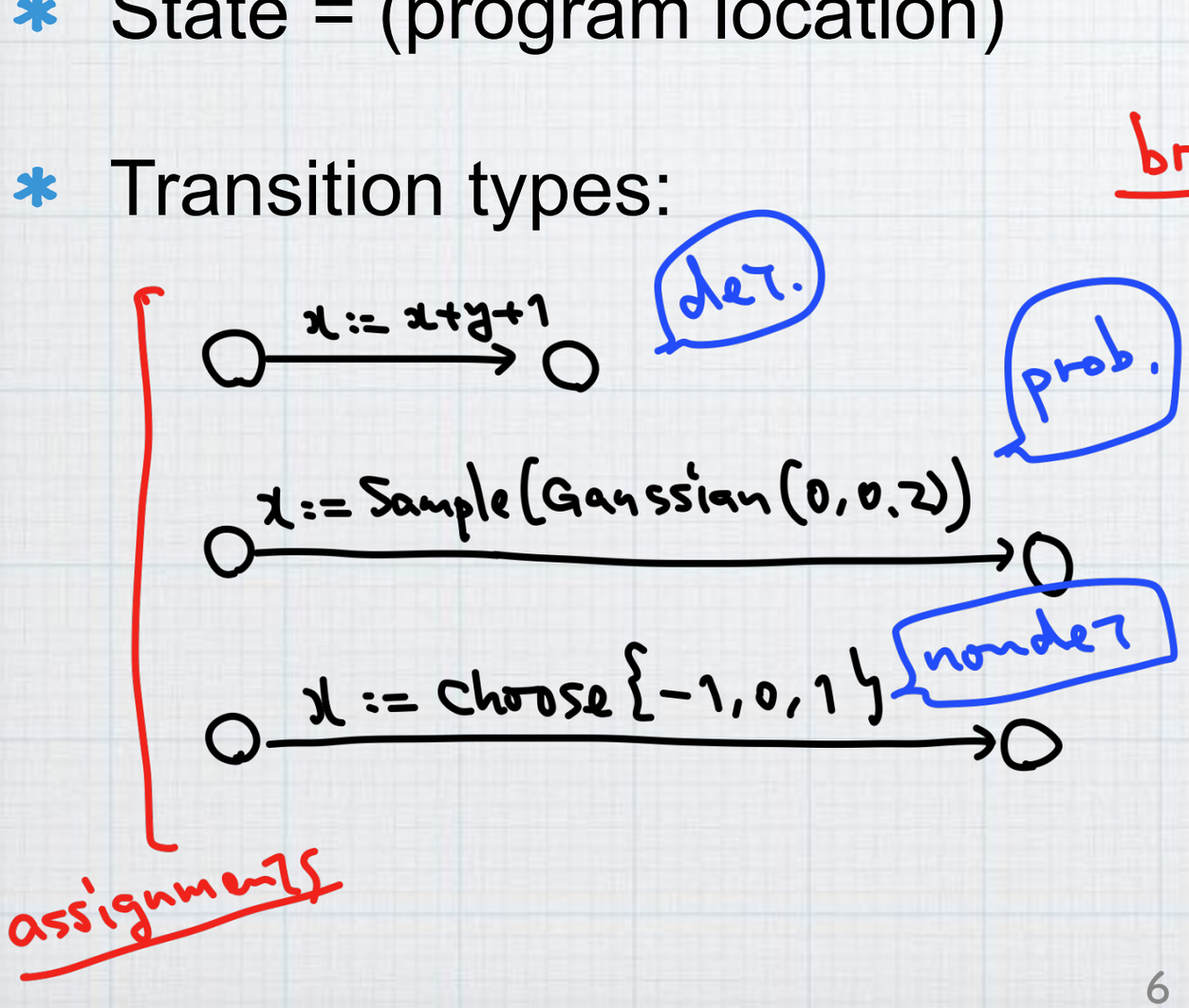
If nondet. is angelic…

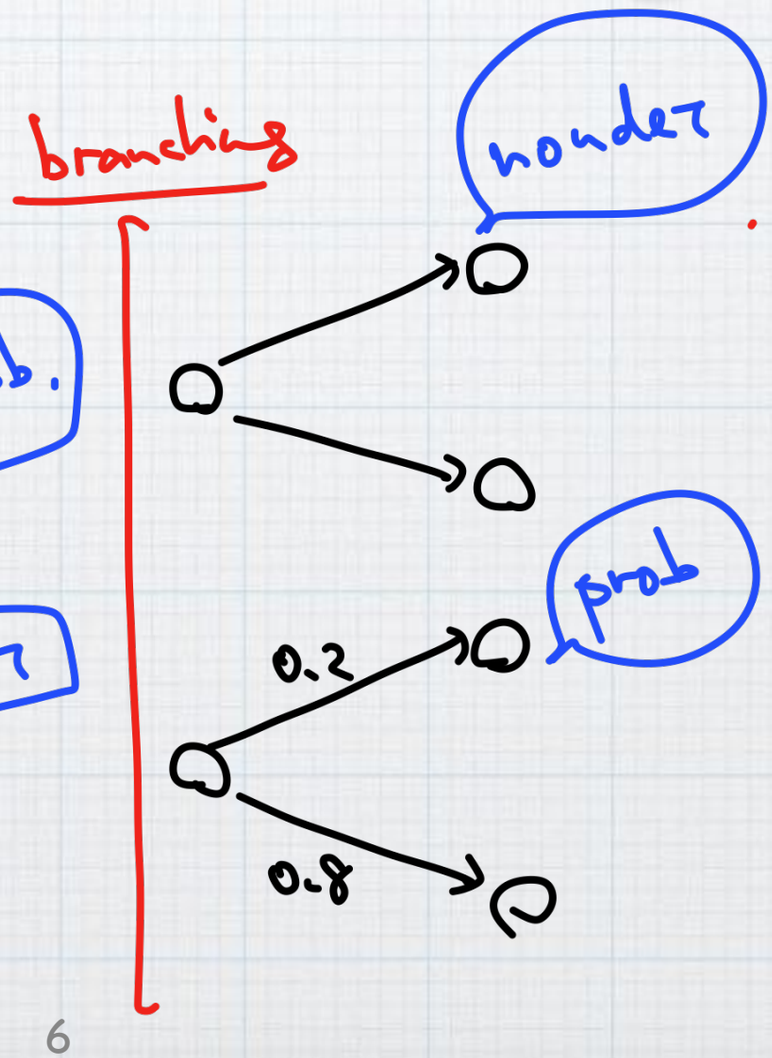
Probabilistic Control Flow Graph (pCFG) See e.g. [Chatterjee+, POPL'17]

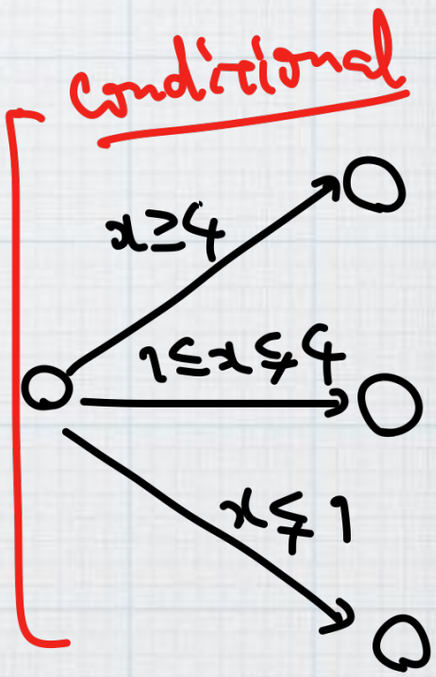
```
1  x := m
2  while x > 0 do
3     if prob(p) do
4        x := x − 1
5     else
6        x := x + 1
7     fi
8  od
```

(say, $m = 16$ and $p = 0.2$)

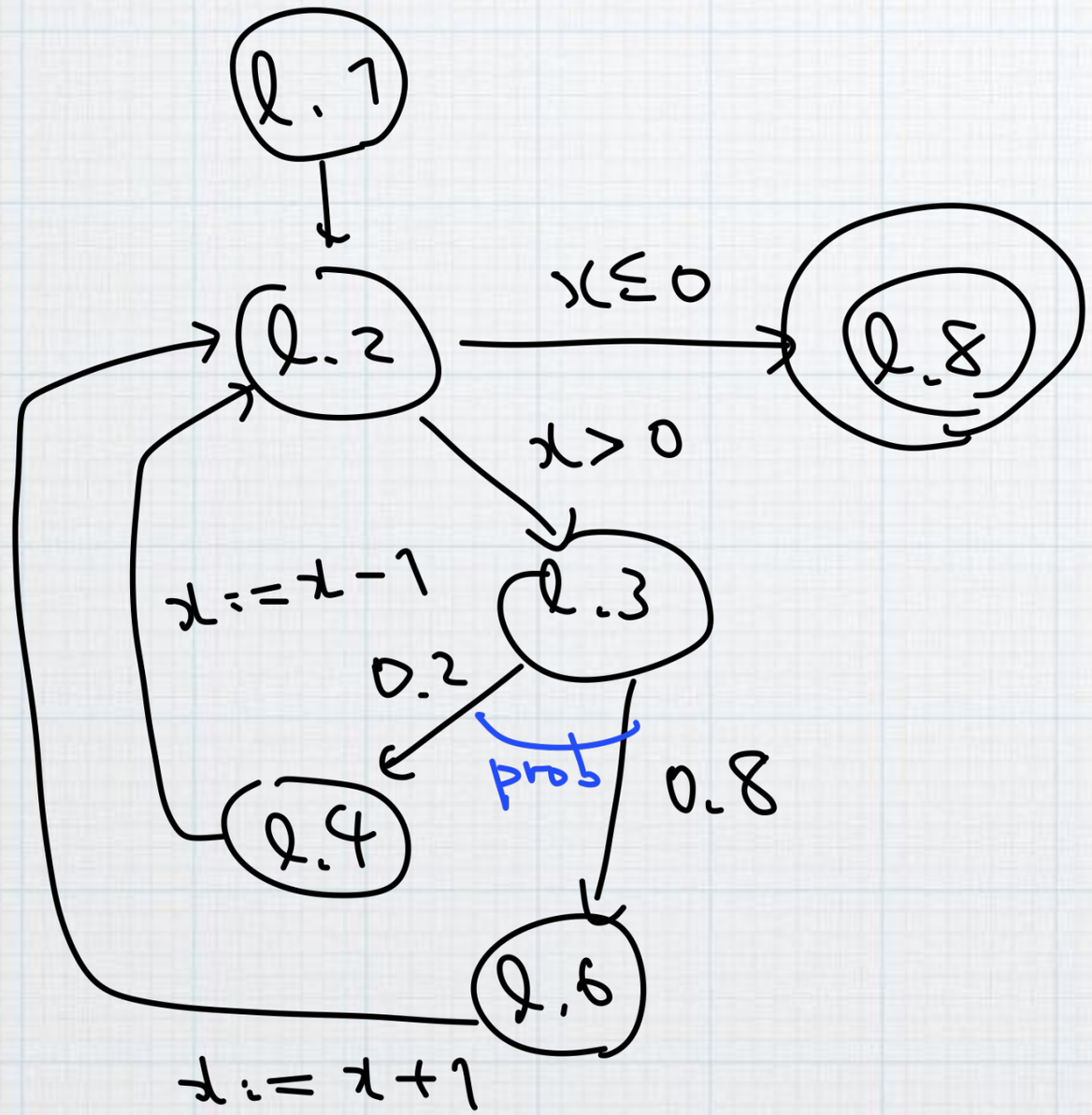
* Finite graph, "**parametric**" in memory states
  * (… justifies my presence here!)
* State = (program location)
* Transition types:







Probabilistic Control Flow Graph (pCFG) See e.g. [Chatterjee+, POPL'17]




```
1  x := m
2  while x > 0 do
3     if prob(p) do
4        x := x − 1
5     else
6        x := x + 1
7     fi
8  od
```

(say, $m = 16$ and $p = 0.2$)

The Problem

* **Given**
  * a pCFG. n variables, state set L
  * $C \subseteq L \times \mathbb{R}^n$
    (Lebesgue measurable) target region
  * $l_0 \in L,\ \vec{x}_0 \in \mathbb{R}^n$
    initial configuration

* **Answer**
  $\mathbf{Pr}(\mathrm{Reach}_C)$

Approach

- Use **parametric certificates**, i.e. functions

$$\left(f_l : \mathbb{R}^n \to \mathbb{R} \right)_{l \in L}$$

  to give *approximate* answers. Template-based synthesis

- Qualitative questions
  - $\mathbf{Pr}(\mathrm{Reach}_C) =^{?} 1$ (almost sure reachability)
  - $\mathbf{Pr}(\mathrm{Reach}_C) >=^{?} \alpha$ (threshold reachability)
- Quantitative questions
  - $\mathbf{Pr}(\mathrm{Reach}_C)$ >= ?? (lowerbound, “verification”)
  - $\mathbf{Pr}(\mathrm{Reach}_C)$ <= ?? (upperbound, “refutation”)
  - $\mathbf{Exp}(\mathrm{StepsToReach}_C)$, upperbound, lowerbound, …
  - “Concentration” [Chaterjee+, POPL’16]
    Find B s.t. $(x > B \rightarrow \exists\ a, b.\ \mathbf{Pr}(\mathrm{StepsToReach}_C > x) < ae^{-bx})$

Why Overapproximation?

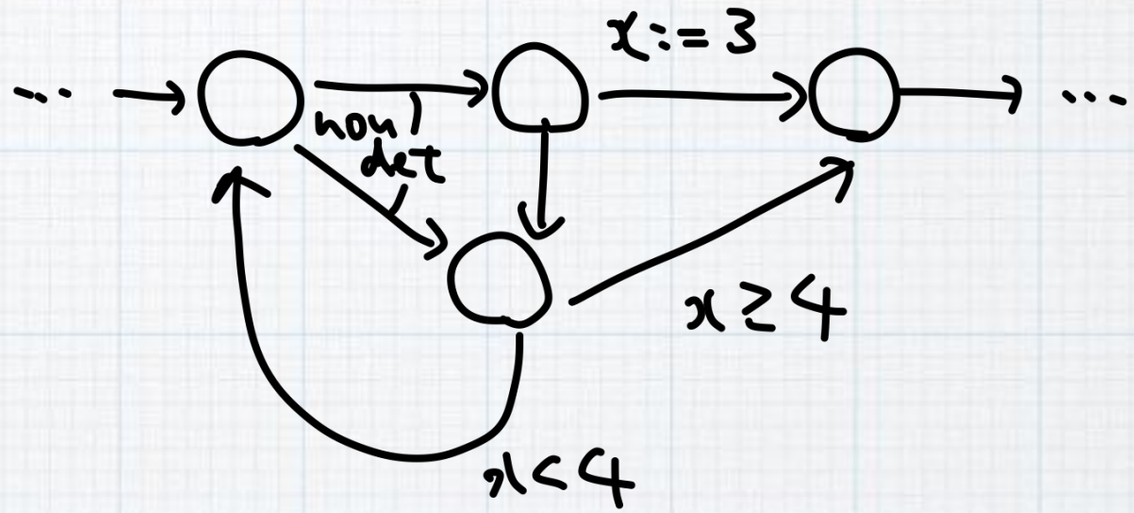
* $\mathbf{Pr}(\mathrm{Reach}_C)$ <= α
  if and only if
  $\mathbf{Pr}(\mathrm{NotReach}_C)$ >= 1- α
* Refutation of reachability
  is
  verification of safety

Overview

* Reachability in **probabilistic programs**
* **Foundation of fixed points,** in the non-probabilistic setting
  * Ranking functions, invariants
  * Foundation: Knaster-Tarski, Cousot-Cousot
* Known **supermartingale** methods
  * Roles of concentration lemmas
* Something new (from **fixed points** and **coalgebras**)
* Coalgebras: excitements, afterthoughts, our project

In Case of No Probabilities…

* ~~p~~CFG



* **Reachability question**: is there a scheduler that leads to C?

* **Verify** reachability by **ranking functions**,
  refute reachability (= verify safety) by **invariants**

* From now on, our theory is not parametrized for simplicity
  * **Kripke frames** instead of CFGs
  * MDPs (or even **MCs**) instead of pCFGs

Ranking Functions

$(S, \to \subseteq S \times S)$: Kripke frame, $C \subseteq S$.
A *ranking function* is

$$\eta : S \to \mathbb{N} \cup \{\infty\}$$

such that

- $\forall s \in S \setminus C.\ \exists s' \in S.$
  $\left(s \to s' \text{ and } \eta(s) \geq \eta(s') + 1 \right)$
- $\eta(s) = 0$ implies $s \in C$

Thm.
$\eta(s) \neq \infty$ implies C is reachable from s.

- η overapproximates #(steps to C)
- Note: $\mathbf{N}$ = {natural numbers} is well-founded
- Discrete analogue of (certain) **Lyapunov functions**…

Invariants

$(S, \to \subseteq S \times S)$: Kripke frame, $C \subseteq S$.
An *invariant* for $S \setminus C$ is

$$I \subseteq S$$

such that

- $I \subseteq \Box I$, where
  $\Box I = \{s \mid \forall s' \leftarrow s.\, s' \in I\}$
- $I \subseteq S \setminus C$

Thm.
$s \in I$ implies C is *not* reachable from s.

* Get trapped in I
* Discrete analogue of **barrier certificates**…

Ranking Functions & Invariants

$(S, \to \subseteq S \times S)$: Kripke frame, $C \subseteq S$.
A *ranking function* is

$$\eta : S \to \mathbb{N} \cup \{\infty\}$$

such that

- $\forall s \in S \setminus C.\ \exists s' \in S.$
  $(\ s \to s' \text{ and } \eta(s) \geq \eta(s') + 1\ )$
- $\eta(s) = 0$ implies $s \in C$

Thm.
$\eta(s) \neq \infty$ implies C is reachable from s.

$(S, \to \subseteq S \times S)$: Kripke frame, $C \subseteq S$.
An *invariant* for $S \setminus C$ is

$$I \subseteq S$$

such that

- $I \subseteq \Box I$, where
  $\Box I = \{s \mid \forall s' \leftarrow s.\ s' \in I\}$
- $I \subseteq S \setminus C$

Thm.
$s \in I$ implies C is *not* reachable from s.

* How come the difference?
* NB:

$$\mathbf{Reach}_C =_{\mu} C \cup \Diamond \mathbf{Reach}_C$$
$$\mathbf{NotReach}_C =_{\nu} (S \setminus C) \cap \Box \mathbf{NotReach}_C$$

Lattice-Theoretic Foundation

L: complete lattice, $f : L \to L$ monotone

Thm. (Knaster-Tarski)

- $\mu f = \mathbf{min}\{l \in L \mid f(l) \sqsubseteq l\}$

$$\Longrightarrow \quad \frac{f(l) \sqsubseteq l}{\mu f \sqsubseteq l}$$

- $\nu f = \mathbf{max}\{l \in L \mid l \sqsubseteq f(l)\}$

$$\Longrightarrow \quad \frac{l \sqsubseteq f(l)}{l \sqsubseteq \nu f}$$

Thm. (Cousot-Cousot)

$\bot \sqsubseteq f(\bot) \sqsubseteq \cdots \sqsubseteq f^{\omega}(\bot) \sqsubseteq \cdots$
stabilizes, and converges to μf

$$\Longrightarrow \quad f^{\alpha}(\bot) \sqsubseteq \mu f \quad (\forall \alpha \in \mathbf{Ord})$$

$\top \sqsupseteq f(\top) \sqsupseteq \cdots \sqsupseteq f^{\omega}(\top) \sqsupseteq \cdots$
stabilizes, and converges to νf

$$\Longrightarrow \quad \nu f \sqsubseteq f^{\alpha}(\top) \quad (\forall \alpha \in \mathbf{Ord})$$

Sound approx. from below

Overview

- **Categorically**:
  initial algebra, final coalgebra, Lambek lemma, initial/final sequence, …

	KT	CC
lfp	**overapprox.**	underapprox.
gfp	underapprox.	**overapprox.**

- **Foundation of fixed points**, in the non-probabilistic setting
  - Ranking functions, invariants
  - Foundation: Knaster-Tarski, Cousot-Cousot
- Known **supermartingale** methods
  - Roles of concentration lemmas
- Something new (from our recent results)
- Coalgebras: excitements, afterthoughts, our project

		Answers what question?	Underlying math
ranking martingale-like methods (**lower** bd)	**Additive** ranking supermartingale [McIver+ PSSE'04] [Chakarov+ CAV'13]	$\mathbf{Pr}(\mathrm{Reach}\,c) =^{?} 1$ $\mathbf{Exp}(\mathrm{Steps}\,c) <= ??$	(elementary)
	γ-scaling ranking submartingale [Urabe+ LICS'17] [Takisaka+, ATVA'18]	$\mathbf{Pr}(\mathrm{Reach}\,c) >= ??$	• Coalgebra! • (?)
repulsing martingale-like methods (**upper** bd)	**ε-decreasing** repulsing supermartingale [Chatterjee+ POPL'17]	$\mathbf{Pr}(\mathrm{Reach}\,c) <= ??$	Azuma's inequality for martingale concentration
	Nonnegative repulsing supermartingale [Steinhardt+ IJRR'12] [Takisaka+, ATVA'18]	$\mathbf{Pr}(\mathrm{Reach}\,c) <= ??$	Markov's inequality for martingale concentration

New

New

Disclaimer

* From now on:
  no nondeterminism,
  no parametrization/variables

* Our setting is therefore:

$$\text{A Markov chain } (\boldsymbol{S}, \boldsymbol{S} \xrightarrow{\mathbf{tr}} \boldsymbol{\mathcal{D}S}), \text{ and } \boldsymbol{C} \subseteq \boldsymbol{S}$$

* Variables are fine.
  Nondeterminism is fine, too, but intricate (measure theory). See [Takisaka+, ATVA'18]

Additive Ranking Supermartingale

[McIver+ PSSE'04] [Chakarov+ CAV'13]

Def.

Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC,
$\eta\colon S \to \mathbb{R}$ be a function.

$\mathbb{X}\eta\colon S \to \mathbb{R}$ is defined by

$$\begin{aligned}(\mathbb{X}\eta)(s) &= \sum_{s'} \mathbf{tr}(s)(s') \cdot \eta(s') \\ &= \sum_{s'} \mathbf{Pr}(s \to s') \cdot \eta(s') \\ &= \mathbf{Exp}(\eta(s') \mid s \to s').\end{aligned}$$

* Overapprox.
  $\mathbf{Exp}(\text{Steps to } C)$

Def.

Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC, $C \subseteq S$.

$\eta\colon S \to \mathbb{R}_{\geq 0}$ is a *ranking supermartingale* for C if

- $\forall s \in S \setminus C. \quad \eta(s) \geq (\mathbb{X}\eta)(s) + 1.$
- $\eta(s) = 0$ implies $s \in C$

Additive Ranking Supermartingale

[McIver+ PSSE'04] [Chakarov+ CAV'13]

Def.

Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC,
$\eta\colon S \to \mathbb{R}$ be a function.

$\mathbb{X}\eta\colon S \to \mathbb{R}$ is defined by

$$(\mathbb{X}\eta)(s) = \sum_{s'} \mathbf{tr}(s)$$
$$= \sum_{s'} \mathbf{Pr}(s$$
$$= \mathbf{Exp}(\eta(s$$

* Overapprox.
  $\mathbf{Exp}(\text{Steps to } C)$

Def.

Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC, $C \subseteq S$.

$\eta\colon S \to \mathbb{R}_{\geq \mathbf{0}}$ is a *ranking supermartingale* for C if

- $\forall s \in S \setminus C.\quad \eta(s) \geq (\mathbb{X}\eta)(s) + \mathbf{1}.$
- $\eta(s) = \mathbf{0}$ implies $s \in C$

Thm.

Let η be a ranking supermartingale for C. Then:

- $\mathbf{Pr}(\mathbf{Reach}_C) = \mathbf{1}$ (almost sure reachability)
- $\mathbf{Exp}(\text{Steps from } s \text{ to } C) \leq \eta(s)$

		Answers what question?	Underlying math
ranking martingale-like methods (**lower** bd)	**Additive** ranking supermartingale [McIver+ PSSE'04] [Chakarov+ CAV'13]	$\mathbf{Pr}(\mathrm{Reach}\,c) =^{?} 1$ $\mathbf{Exp}(\mathrm{Steps}\,c)$ <= ??	(elementary)
	γ-scaling ranking submartingale [Urabe+ LICS'17] [Takisaka+, ATVA'18]	$\mathbf{Pr}(\mathrm{Reach}\,c)$ >= ??	• Coalgebra! • (?)
repulsing martingale-like methods (**upper** bd)	**ε-decreasing** repulsing supermartingale [Chatterjee+ POPL'17]	$\mathbf{Pr}(\mathrm{Reach}\,c)$ <= ??	Azuma's inequality for martingale concentration
	Nonnegative repulsing supermartingale [Steinhardt+ IJRR'12] [Takisaka+, ATVA'18]	$\mathbf{Pr}(\mathrm{Reach}\,c)$ <= ??	Markov's inequality for martingale concentration

New

New

ε-Decreasing Repulsing Supermartingale

[Chatterjee+ POPL'17]

Def.

Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC, $C \subseteq S$, $\varepsilon > 0$, $\kappa > 0$.

$\eta : S \to \mathbb{R}$ is an *ε-decreasing repulsing supermartingale* for C with κ-b'dd difference if

- $\forall s \in S \setminus C. \quad \eta(s) \geq (\mathbb{X}\eta)(s) + \varepsilon.$
- $\forall c \in C. \quad \eta(c) \geq 0.$
- $\forall s \in S. \forall s' \in \mathbf{supp}(\mathbf{tr}(s)).$
  $|\eta(s) - \eta(s')| \leq \kappa.$

Thm.

Let η be such a repulsing supermartingale for C. Assume $\eta(s) < 0$. Then

$$\mathbf{Pr}(\mathbf{Reach}_{s,C}) \leq \alpha \frac{\gamma^{\lceil |\eta s|/\kappa \rceil}}{1-\gamma}$$

where $\alpha = e^{\frac{\varepsilon \cdot \eta(s)}{(\kappa+\varepsilon)^2}}$, $\gamma = e^{-\frac{\varepsilon^2}{2(\kappa+\varepsilon)^2}}$.

ε-Decreasing Repulsing Supermartingale

[Chatterjee+ POPL'17]

Def.

Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC, $C \subseteq S$, $\varepsilon > 0$, $\kappa > 0$.

$\eta\colon S \to \mathbb{R}$ is an *ε-decreasing repulsing supermartingale* for C with κ-b'dd difference if

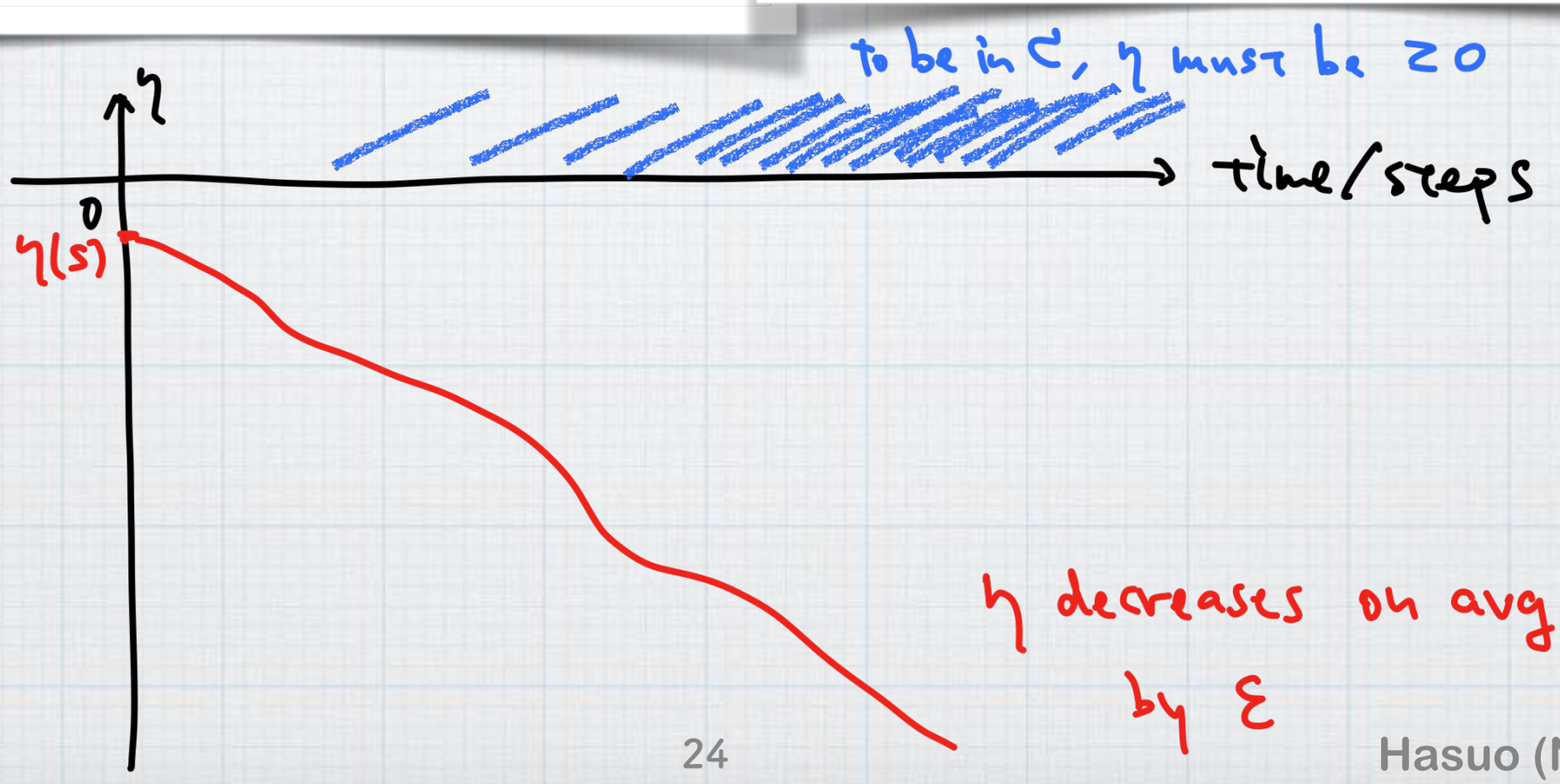
- $\forall s \in S \setminus C.\quad \eta(s) \geq (\mathbb{X}\eta)(s) + \varepsilon$.
- $\forall c \in C.\quad \eta(c) \geq 0$.
- $\forall s \in S.\, \forall s' \in \mathbf{supp}(\mathbf{tr}(s)).$ $|\eta(s) - \eta(s')| \leq \kappa$.

Thm.

Let η be such a repulsing supermartingale for C. Assume $\eta(s) < 0$. Then

$$\Pr(\mathbf{Reach}_{s,C}) \leq \alpha \frac{\gamma^{\lceil |\eta s|/\kappa \rceil}}{1-\gamma}$$

where $\alpha = e^{\frac{\varepsilon \cdot \eta(s)}{(\kappa+\varepsilon)^2}}$, $\gamma = e^{-\frac{\varepsilon^2}{2(\kappa+\varepsilon)^2}}$.



ε-Decreasing Repulsing Supermartingale

[Chatterjee+ POPL'17]

Def.

Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC, $C \subseteq S$, $\varepsilon > 0$, $\kappa > 0$.

$\eta\colon S \to \mathbb{R}$ is an *ε-decreasing repulsing supermartingale* for C with κ-b'dd difference if

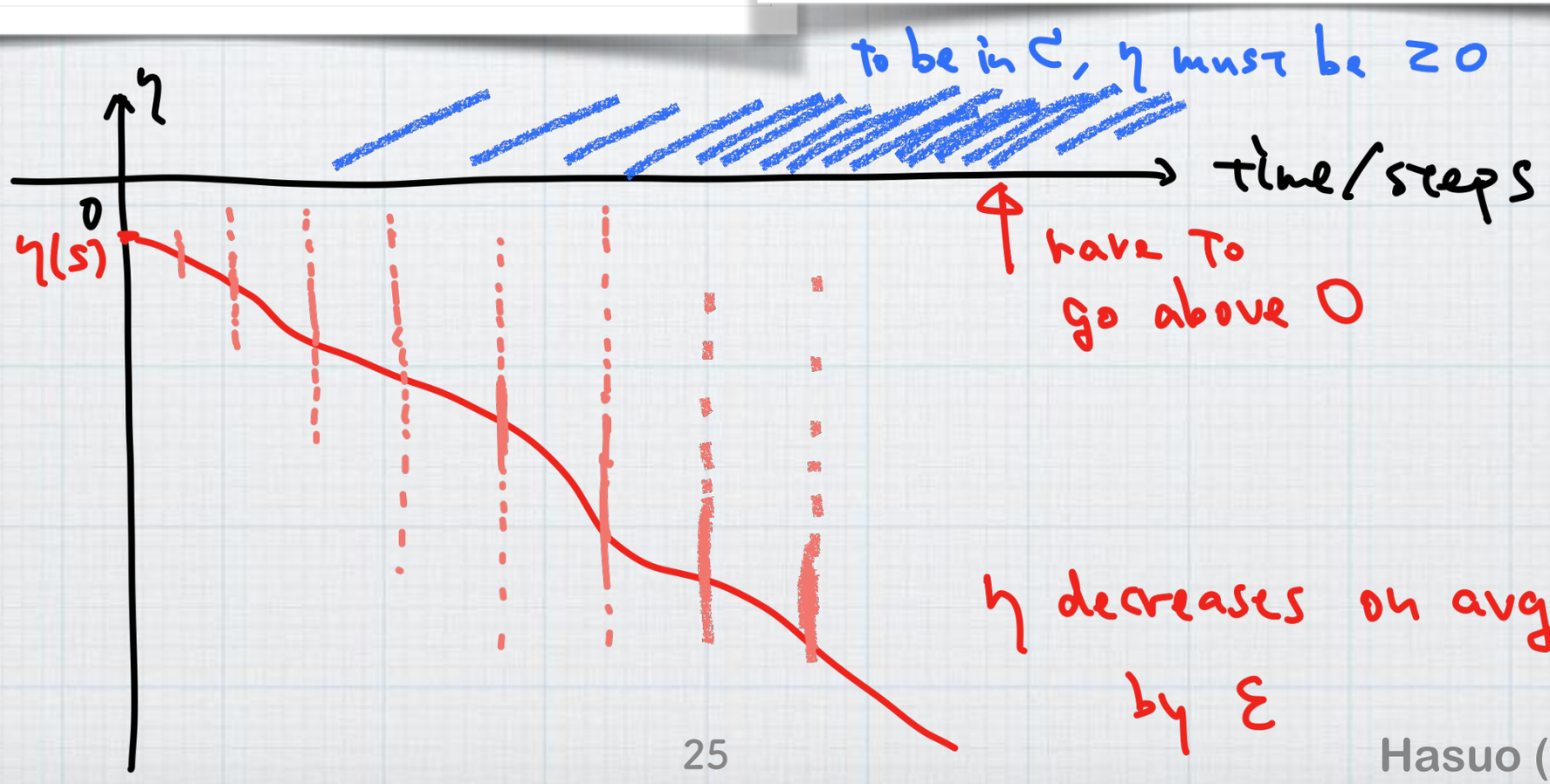
- $\forall s \in S \setminus C.\quad \eta(s) \geq (\mathbb{X}\eta)(s) + \varepsilon.$
- $\forall c \in C.\quad \eta(c) \geq 0.$
- $\forall s \in S.\, \forall s' \in \mathbf{supp}(\mathbf{tr}(s)).$
  $|\eta(s) - \eta(s')| \leq \kappa.$

Thm.

Let η be such a repulsing supermartingale for C. Assume $\eta(s) < 0$. Then

$$\Pr(\mathbf{Reach}_{s,C}) \leq \alpha \frac{\gamma^{\lceil |\eta s|/\kappa \rceil}}{1-\gamma}$$

where $\alpha = e^{\frac{\varepsilon \cdot \eta(s)}{(\kappa+\varepsilon)^2}}$, $\gamma = e^{-\frac{\varepsilon^2}{2(\kappa+\varepsilon)^2}}$.



ε-Decreasing Repulsing Supermartingale

[Chatterjee+ POPL'17]

Def.

Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC, $C \subseteq S$, $\varepsilon > 0$, $\kappa > 0$.

$\eta\colon S \to \mathbb{R}$ is an *ε-decreasing repulsing supermartingale* for C with κ-b'dd difference if

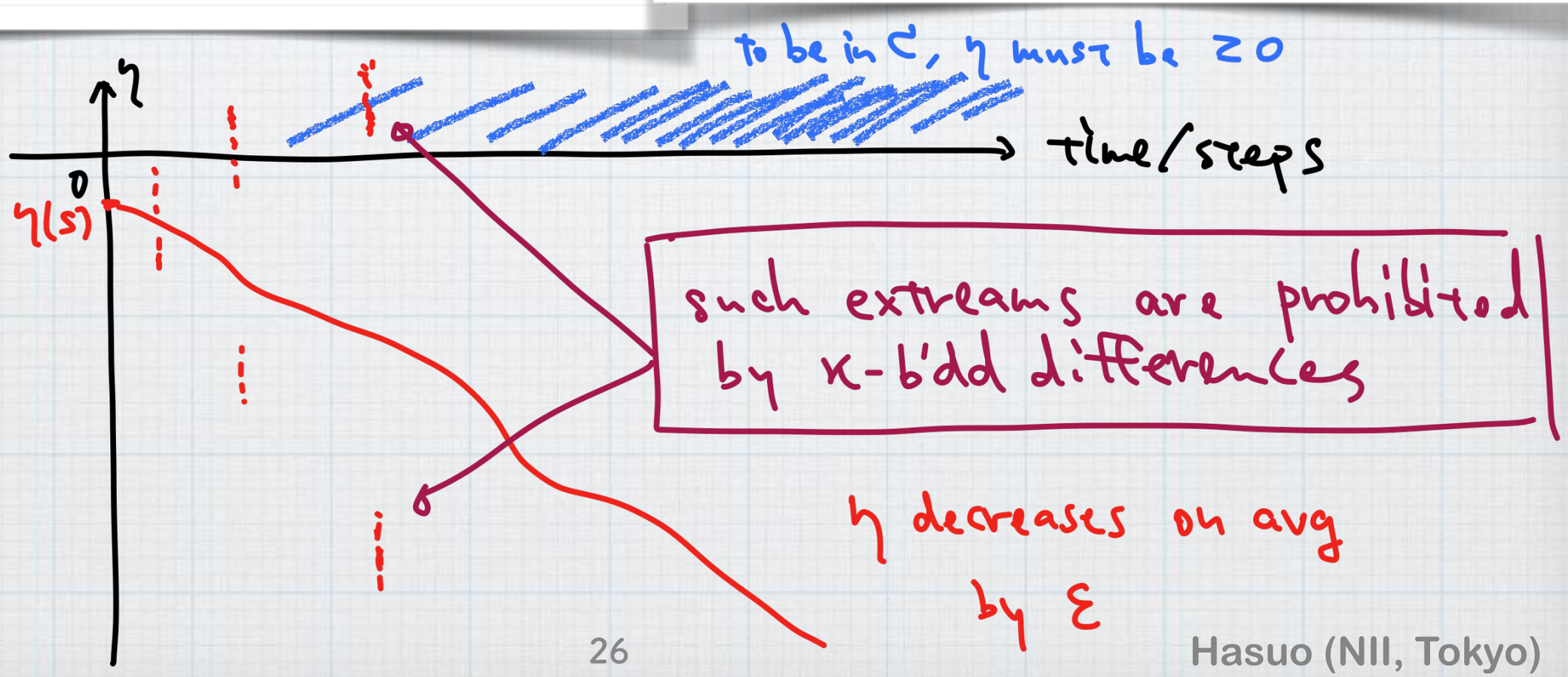
- $\forall s \in S \setminus C.\quad \eta(s) \geq (\mathbb{X}\eta)(s) + \varepsilon.$
- $\forall c \in C.\quad \eta(c) \geq 0.$
- $\forall s \in S.\, \forall s' \in \mathbf{supp}(\mathbf{tr}(s)).$
  $|\eta(s) - \eta(s')| \leq \kappa.$

Thm.

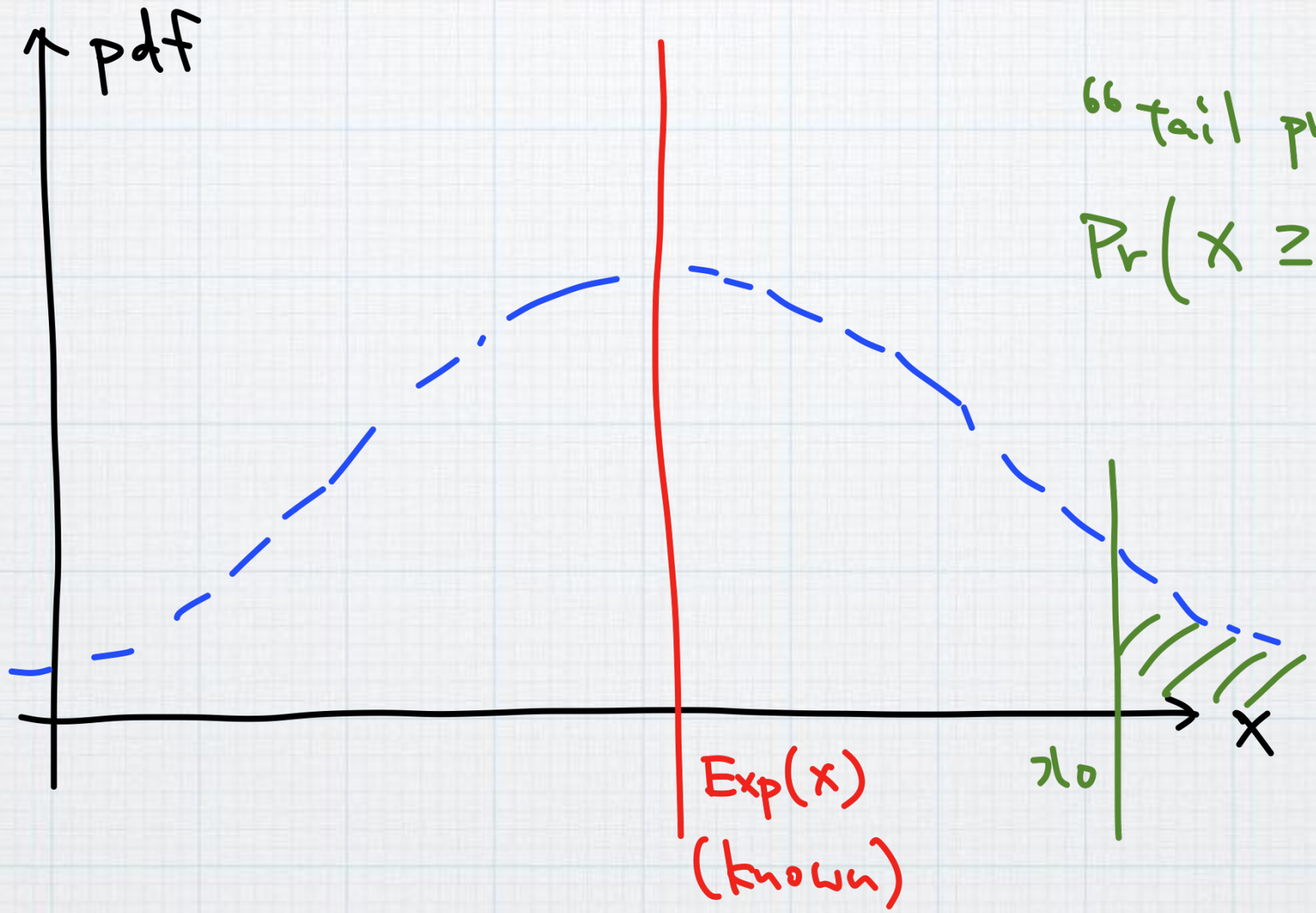
Let η be such a repulsing supermartingale for C. Assume $\eta(s) < 0$. Then

$$\mathbf{Pr}(\mathbf{Reach}_{s,C}) \leq \alpha \frac{\gamma^{\lceil |\eta s|/\kappa \rceil}}{1-\gamma}$$

where $\alpha = e^{\frac{\varepsilon \cdot \eta(s)}{(\kappa+\varepsilon)^2}}$, $\gamma = e^{-\frac{\varepsilon^2}{2(\kappa+\varepsilon)^2}}$.



Concentration of Measure Inequalities



Concentration of Measure Inequalities

The distr. can be this extreme

⇒ knowing the avg. is not enough!

Concentration of Measure I: Azuma's Inequality Used in [Chatterjee+ POPL'17]

Def. Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC.
A *supermartingale* is $\eta : S \to \mathbb{R}$ such that

$$\forall s \in S. \quad \eta(s) \geq (\mathbb{X}\eta)(s)$$

When one-step difference is bounded…

Rem. Let $s_0 \to s_1 \to \cdots$ be a run of the MC, with s_0 fixed. Then s_n is a rand. var. in S for each n, and $\eta(s_n)$ is a rand. var. in $\mathbb{R}$.

Thm. (Azuma) Let η have κ-bdd difference. For each $\lambda > 0$ and $n \in \mathbb{N}$,

$$\mathbf{Pr}\big(\, \eta(s_n) - \eta(s_0) \geq \lambda \,\big) \;\leq\; e^{-\frac{\lambda^2}{2n\kappa^2}}$$

Concentration of Measure II: The Chebyshev-Cantelli Inequality

Used e.g.in [Bouissou+ TACAS'16]

Thm. (Chebyshev–Cantelli) Let X be a random variable with mean μ and variance σ^2. Then for each $k > 0$,

$$\Pr(X - \mu \geq k\sigma) \leq \frac{1}{1 + k^2}$$

If variance is known…

Concentration of Measure III: Bernstein's Inequality

Used e.g.in [Bouissou+ TACAS'16]

Thm. (Bernstein) Let η be a supermartingale, where

- conditional variance is bounded: $\exists \sigma$ such that

$$\mathbf{Var}\big(\,\eta(s') \,\big|\, s \to s'\,\big) \;\leq\; \sigma^2$$

- deviation from the mean is bounded: $\exists M$ such that, $\forall i \in [0, n]$,

$$\big|\,\eta(s_i) - \mathbf{Exp}(\eta(s_i))\,\big| \;\leq\; M$$

Then

$$\mathbf{Pr}\big(\,\eta(s_n) - \eta(s_0) \geq \lambda\,\big) \;\leq\; \exp\Big(\frac{-\lambda^2}{2n\sigma^2 + \frac{2}{3}M\lambda}\Big)$$

		Answers what question?	Underlying math
ranking martingale-like methods (**lower** bd)	**Additive** ranking supermartingale [McIver+ PSSE'04] [Chakarov+ CAV'13]	$\mathbf{Pr}(\mathrm{Reach}\,c) =^{?} 1$ $\mathbf{Exp}(\mathrm{Steps}\,c)$ <= ??	(elementary)
	γ-scaling ranking submartingale [Urabe+ LICS'17] [Takisaka+, ATVA'18]	$\mathbf{Pr}(\mathrm{Reach}\,c)$ >= ??	• Coalgebra! • (?)
repulsing martingale-like methods (**upper** bd)	**ε-decreasing** repulsing supermartingale [Chatterjee+ POPL'17]	$\mathbf{Pr}(\mathrm{Reach}\,c)$ <= ??	Azuma's inequality for martingale concentration
	Nonnegative repulsing supermartingale [Steinhardt+ IJRR'12] [Takisaka+, ATVA'18]	$\mathbf{Pr}(\mathrm{Reach}\,c)$ <= ??	Markov's inequality for martingale concentration

New

New

Overview

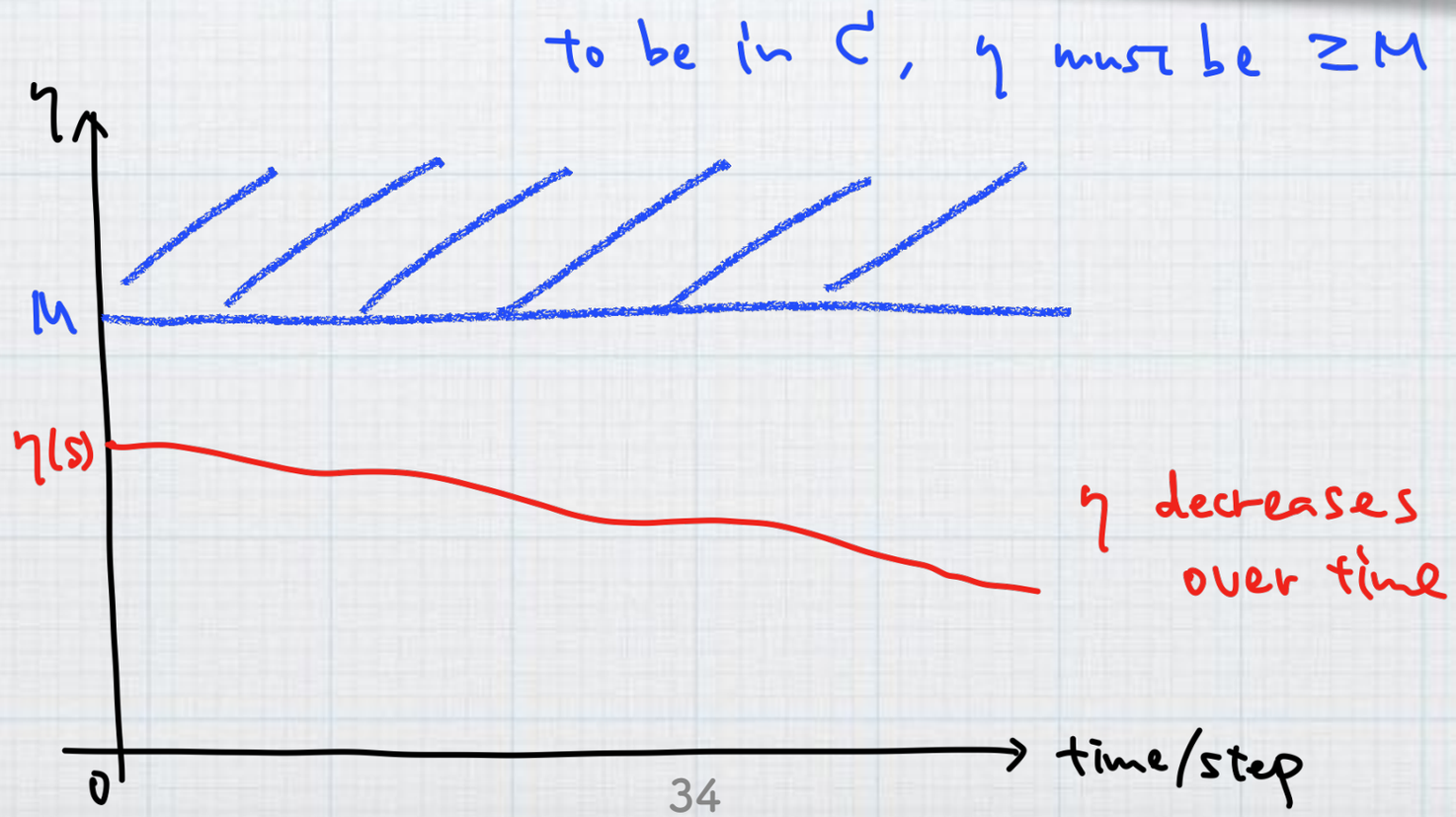
- Reachability in **probabilistic programs**
- **Foundation of fixed points,** in the non-probabilistic setting
  - Ranking functions, invariants
  - Foundation: Knaster-Tarski, Cousot-Cousot
- Known **supermartingale** methods
  - Roles of concentration lemmas
- Something new (from **fixed points** and **coalgebras**)
- Coalgebras: excitements, afterthoughts, our project

Nonnegative Repulsing Supermartingale

[Steinhardt+ IJRR'12] [Takisaka, Oyabu, Urabe, IH, in preparation]

Def. Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC, $C \subseteq S$ and $M > 0$. $\eta : S \to \mathbb{R}$ is a *nonnegative repulsing supermartingale* for C at M if

- $\forall s \in S.\quad \eta(s) \geq 0$
- $\forall s \in S \setminus C.\quad \eta(s) \geq (\mathbb{X}\eta)(s)$
- $\forall c \in C.\quad \eta(c) \geq M$

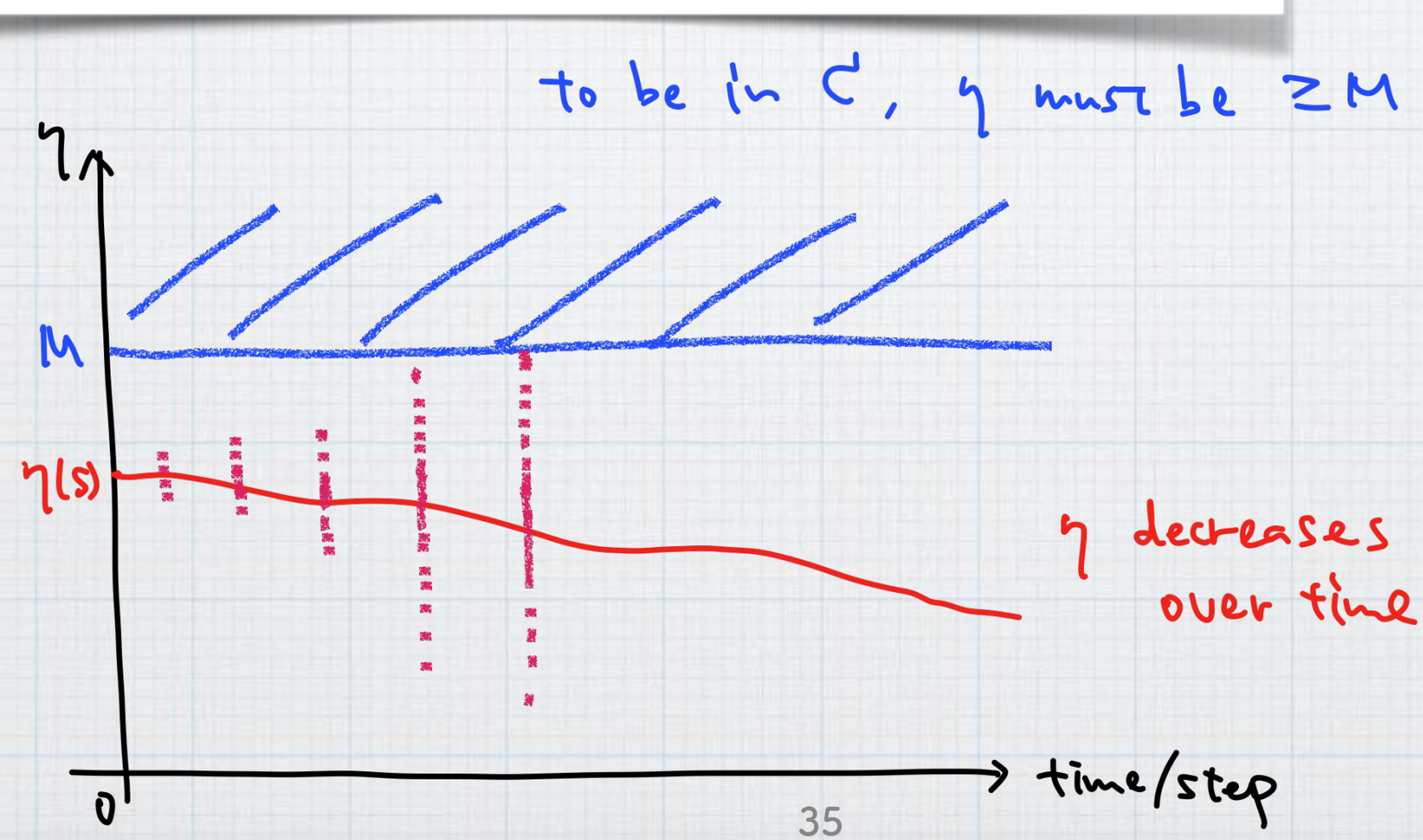


Nonnegative Repulsing Supermartingale

[Steinhardt+ IJRR'12] [Takisaka, Oyabu, Urabe, IH, in preparation]

Def. Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC, $C \subseteq S$ and $M > 0$. $\eta\colon S \to \mathbb{R}$ is a *nonnegative repulsing supermartingale* for C at M if

- $\forall s \in S.\quad \eta(s) \geq 0$
- $\forall s \in S \setminus C.\quad \eta(s) \geq (\mathbb{X}\eta)(s)$
- $\forall c \in C.\quad \eta(c) \geq M$

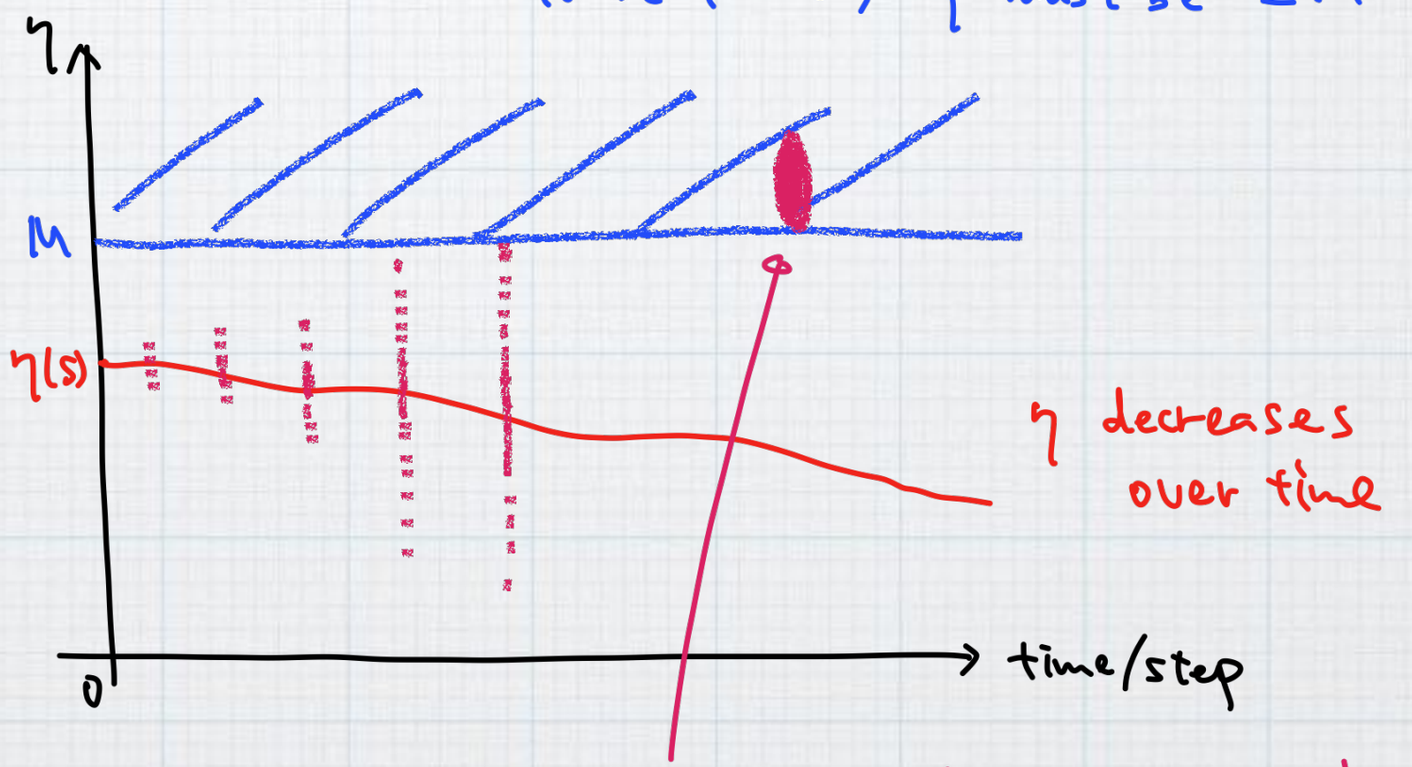


Nonnegative Repulsing Supermartingale

[Steinhardt+ IJRR'12] [Takisaka, Oyabu, Urabe, IH, in preparation]

Def. Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC, $C \subseteq S$ and $M > 0$. $\eta\colon S \to \mathbb{R}$ is a *nonnegative repulsing supermartingale* for C at M if

- $\forall s \in S.\quad \eta(s) \geq 0$
- $\forall s \in S \setminus C.\quad \eta(s) \geq (\mathbb{X}\eta)(s)$
- $\forall c \in C.\quad \eta(c) \geq M$



Nonnegative Repulsing Supermartingale

[Steinhardt+ IJRR'12]. With nondeterminism: [Takisaka, Oyabu, Urabe, IH, ATVA'18]

Def. Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC, $C \subseteq S$ and $M > 0$. $\eta : S \to \mathbb{R}$ is a *nonnegative repulsing supermartingale* for C at M if

- $\forall s \in S.\quad \eta(s) \geq 0$
- $\forall s \in S \setminus C.\quad \eta(s) \geq (\mathbb{X}\eta)(s)$
- $\forall c \in C.\quad \eta(c) \geq M$

Thm. (upper bound)

$$\mathbf{Pr}(\mathbf{Reach}_{s,C}) \leq \frac{1}{M}\eta_s$$

Thm. (completeness) There exists a nonnegative repulsing supermartingale η for C at M such that

$$\mathbf{Pr}(\mathbf{Reach}_{s,C}) = \frac{1}{M}\eta_s$$

Proof. Take $M = 1$, $\eta(s) = \mathbf{Pr}(\mathbf{Reach}_{s,C})$.

		Answers what question?	Underlying math
ranking martingale-like methods (**lower** bd)	**Additive** ranking supermartingale [McIver+ PSSE'04] [Chakarov+ CAV'13]	$\mathbf{Pr}(\mathrm{Reach}\,c) =^{?} 1$ $\mathbf{Exp}(\mathrm{Steps}\,c)$ <= ??	(elementary)
	γ-scaling ranking submartingale [Urabe+ LICS'17] [Takisaka+, ATVA'18]	$\mathbf{Pr}(\mathrm{Reach}\,c)$ >= ??	• **Coalgebra!** • (?)
repulsing martingale-like methods (**upper** bd)	**ε-decreasing** repulsing supermartingale [Chatterjee+ POPL'17]	$\mathbf{Pr}(\mathrm{Reach}\,c)$ <= ??	Azuma's inequality for martingale concentration
	Nonnegative repulsing supermartingale [Steinhardt+ IJRR'12] [Takisaka+, ATVA'18]	$\mathbf{Pr}(\mathrm{Reach}\,c)$ <= ??	Knaster-Tarski!

New

New

Concentration of Measure: No Need!

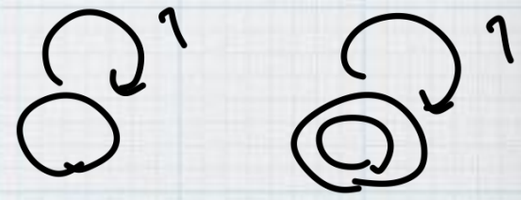
Def. Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC, $C \subseteq S$.
Let $\mathbb{X}_C : [0,1]^S \longrightarrow [0,1]^S$ be defined by

$$\Big(\, \eta : S \to [0,1] \,\Big) \xmapsto{\mathbb{X}_C} \left(\begin{array}{lcll} \mathbb{X}_C\eta : & S & \longrightarrow & [0,1] \\ & s & \longmapsto & \begin{cases} 1 & \text{if } s \in C \\ (\mathbb{X}\eta)(s) & \text{if } s \notin C \end{cases} \end{array} \right)$$

Thm. (upper bound)

$$\mathbf{Pr}(\mathbf{Reach}_C) =_{\mu} \mathbb{X}_C \mathbf{Pr}(\mathbf{Reach}_C)$$

(Easy from the Cousot-Cousot characterization of lfp)



Rem.

- The *least* fixed point
- In the complete lattice $[\mathbf{0}, \mathbf{1}]$, so that a sink state gets $\mathbf{0}$

Lattice-Theoretic Foundation

L: complete lattice, $f : L \to L$ monotone

Thm. (Knaster-Tarski)

- $\mu f = \mathbf{min}\{l \in L \mid f(l) \sqsubseteq l\}$

$$\Longrightarrow \frac{f(l) \sqsubseteq l}{\mu f \sqsubseteq l}$$

- $\nu f = \mathbf{max}\{l \in L \mid l \sqsubseteq f(l)\}$

$$\Longrightarrow \frac{l \sqsubseteq f(l)}{l \sqsubseteq \nu f}$$

Thm. (Cousot-Cousot)

$\bot \sqsubseteq f(\bot) \sqsubseteq \cdots \sqsubseteq f^{\omega}(\bot) \sqsubseteq \cdots$
stabilizes, and converges to μf

$$\Longrightarrow \quad f^{\alpha}(\bot) \sqsubseteq \mu f \quad (\forall \alpha \in \mathbf{Ord})$$

$\top \sqsupseteq f(\top) \sqsupseteq \cdots \sqsupseteq f^{\omega}(\top) \sqsupseteq \cdots$
stabilizes, and converges to νf

$$\Longrightarrow \quad \nu f \sqsubseteq f^{\alpha}(\top) \quad (\forall \alpha \in \mathbf{Ord})$$

Concentration of Measure: No Need!

Thm. Let $\eta : S \to [0,1]$ be such that

$$\mathbb{X}_C(\eta) \leq \eta \ ,$$

that is,

- $\forall s \in S \setminus C. \quad \eta(s) \geq (\mathbb{X}\eta)(s)$
- $\forall c \in C. \quad \eta(c) \geq 1$

Then, for each $s \in S$,

$$\mathbf{Pr}(\mathbf{Reach}_{s,C}) \ \leq \ \eta(s)$$

$$\begin{array}{ccc} \mathbb{X}_C\,\mathbf{Reach}_{s,C} & \dashrightarrow & \mathbb{X}_C\,\eta \\ \text{init}\downarrow \cong & & \downarrow \\ \mathbf{Reach}_{s,C} & \dashrightarrow & \eta \end{array} \qquad \text{in the poset } [0,1]^S$$

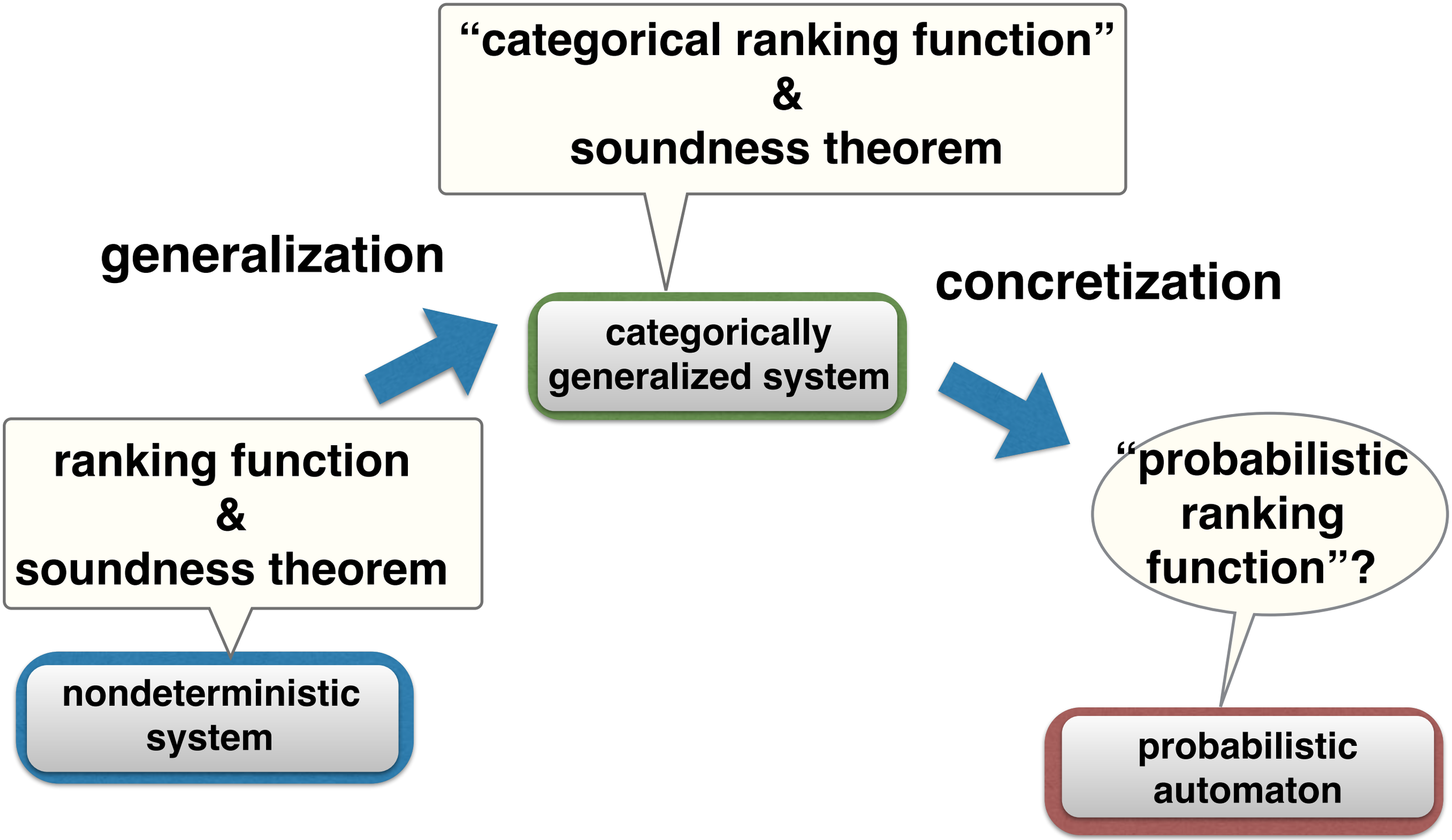
- Very simple, but not previously known
- Soundness and completeness follow easily
- Template-based synthesis:
  experimentally outperforms the known method [Chatterjee+ POPL'17]

		Answers what question?	Underlying math
ranki… martingale methods (**lower** bd)	**Additive** ranking supermartingale [McIver+ PSSE'04] [Chakarov+ CAV'13]	$\mathbf{Pr}(\mathrm{Reach}\,c) =^{?} 1$ $\mathbf{Exp}(\mathrm{Steps}\,c)$ <= ??	(elementary)
	γ-scaling ranking submartingale [Urabe+ LICS'17] [Takisaka+, ATVA'18]	$\mathbf{Pr}(\mathrm{Reach}\,c)$ >= ??	• LFP characterization • (Categorical consideration)
repulsing martingale-like methods (**upper** bd)	**ε-decreasing** repulsing supermartingale [Chatterjee+ POPL'17]	$\mathbf{Pr}(\mathrm{Reach}\,c)$ <= ??	Azuma's inequality for martingale concentration
	Nonnegative repulsing supermartingale [Steinhardt+ IJRR'12] [Takisaka+, ATVA'18]	$\mathbf{Pr}(\mathrm{Reach}\,c)$ <= ??	Knaster-Tarski!

New

New

Methodology [UrabeHH, LICS'17]



Categorical Ranking Function

Def:

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

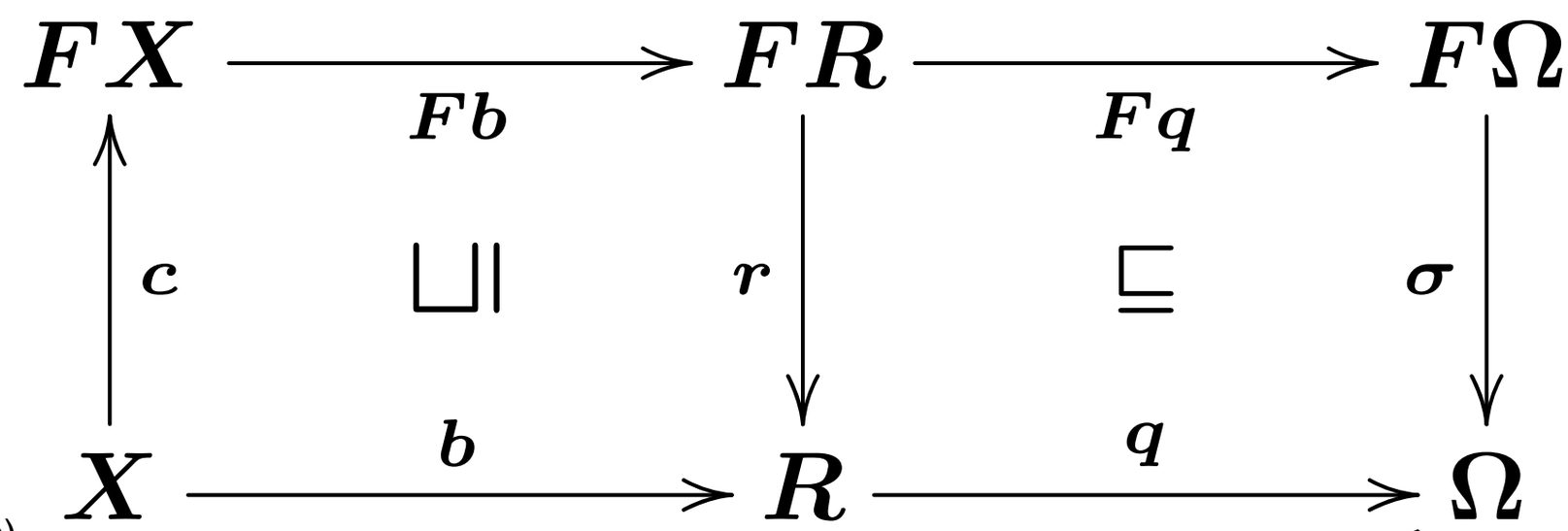
$$(\, \boldsymbol{r : FR \to R},\ \boldsymbol{q : R \to \Omega},\ \boldsymbol{\sqsubseteq_R} \,) \quad \text{s.t.}$$

1. $\boldsymbol{R}$ is a complete lattice and $\boldsymbol{\Phi_{c,r}}$ is monotone
2. $\boldsymbol{q}$ is monotone, $\bot$-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. $(r, q, \sqsubseteq_R)$ if:

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



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.

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

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

Scaled Multiplicative Ranking Submartingale

Def:

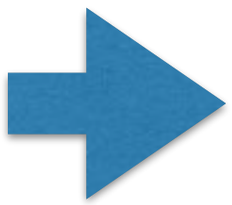
For $\gamma \in (0,1)$, a function $b : X \to [0,1]$ is a γ **-scaled multiplicative ranking submartingale** if:

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

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

Abstract Technique

$$T[\_]$$

$$\begin{array}{lll} A & ::= & \texttt{true} \mid \texttt{false} \mid A_1 \wedge A_2 \mid \neg A \mid a_1 < a_2 \mid \\ & & \forall x \in {}^*\mathbb{N}.\, A \mid \forall x \in {}^*\mathbb{R}.\, A \end{array}$$

$$\begin{array}{ccc} FX & \xrightarrow{F\mathsf{beh}_c} & FZ \\ {\scriptstyle c}\uparrow & & \uparrow{\scriptstyle \mathrm{final}} \\ X & \xrightarrow[\mathsf{beh}_c]{} & Z \end{array}$$

system behavior

$$\begin{array}{ccc} FX & \xrightarrow{Ff} & FY \\ {\scriptstyle c}\uparrow & \sqsupseteq & \uparrow{\scriptstyle d} \\ X & \xrightarrow[f]{} & Y \end{array}$$

simulation

Identify "mathematical essense"

Choose parameter e_1

Choose parameter e_2

Existing Technique

$$T_1 = T[e_1]$$

Novel Technique

$$T[e_2]$$

- Formal methods, from software to cyber-physical systems. "Metatheoretical transfer"
- Real-world application, exploiting abstraction and generality

Some Afterthoughts…

- LP characterization of reachability probabilities (e.g. [Baier & Katoen])
  - Minimize **x**
  - subject to **x** = **A**$\mathbf{x}$ + **b**
  - Here **A** is the transition matrix, and **b** is the membership of C
- Our scaled multiplicative ranking supermartingale
  - Scale the constraint to **x** = γ(**A**$\mathbf{x}$ + **b**) with $0 < \gamma < 1$
    ➜ Makes the solution $\mathbf{x_0}$ unique. It is an lfp and a **gfp**
  - Once we find **x** such that **x** ≦ γ(**A**$\mathbf{x}$ + **b**), we have **x** ≦ $\mathbf{x_0}$ by Knaster-Tarski
- (Still the categorical axiomatics gives a nice clue, I believe)

ERATO 蓮尾メタ数理システムデザインプロジェクト

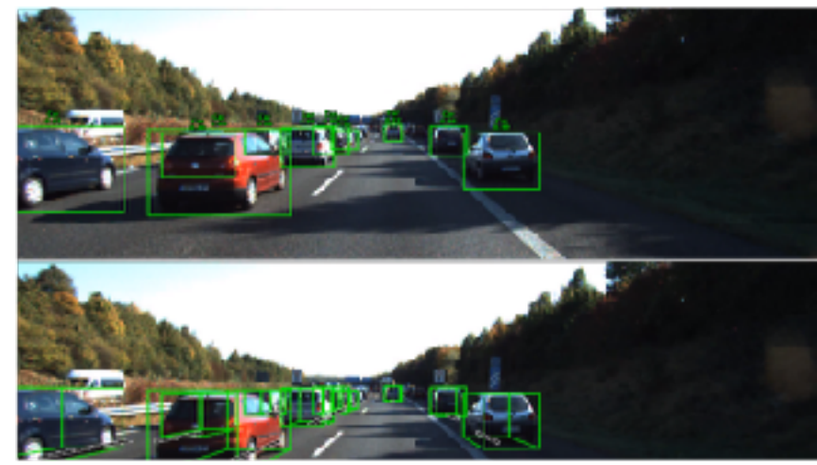
ERATO Metamathematics for Systems Design Project

国立情報学研究所 & 科学技術振興機構　National Institute of Informatics & Japan Science and Technology Agency

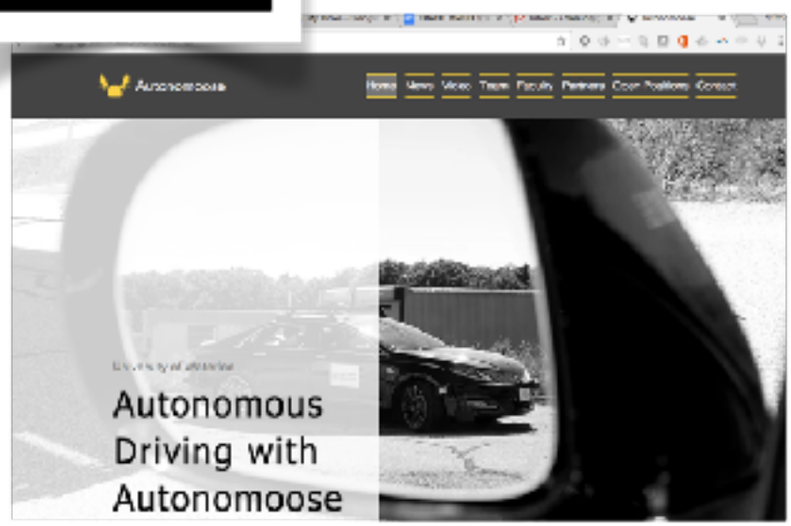
ERATO MMSD

* Our goal:
  Formal methods for cyber-physical systems (CPS)
  * Pursued by many…
    e.g. NSF's CPS initiative (computer science + control theory)

* Our uniqueness　position paper [Hasuo, New Gener. Comp. '17]
  * Theory: foundation and diversity
    * Algebraic, logical and categorical metatheory
      ➜
      "Mathematical transfer" from software to CPS
    * Logic/automata, control
      + category theory, software engineering,
      machine learning, probability theory, …
* Application:
  tackle real systems (≒ real automated driving cars)
  * Industrial collaboration
  * The autonomoose project at U. Waterloo
  * Cars ← efficient testing ← formal reasoning
    ← categories!



mazda



Overview

* Reachability in **probabilistic programs**
* **Foundation of fixed points,** in the non-probabilistic setting
  * Ranking functions, invariants
  * Foundation: Knaster-Tarski, Cousot-Cousot
* Known **supermartingale** methods
  * Roles of concentration lemmas
* Something new (from our recent results)
* Coalgebras: excitements, afterthoughts, our project

Summary

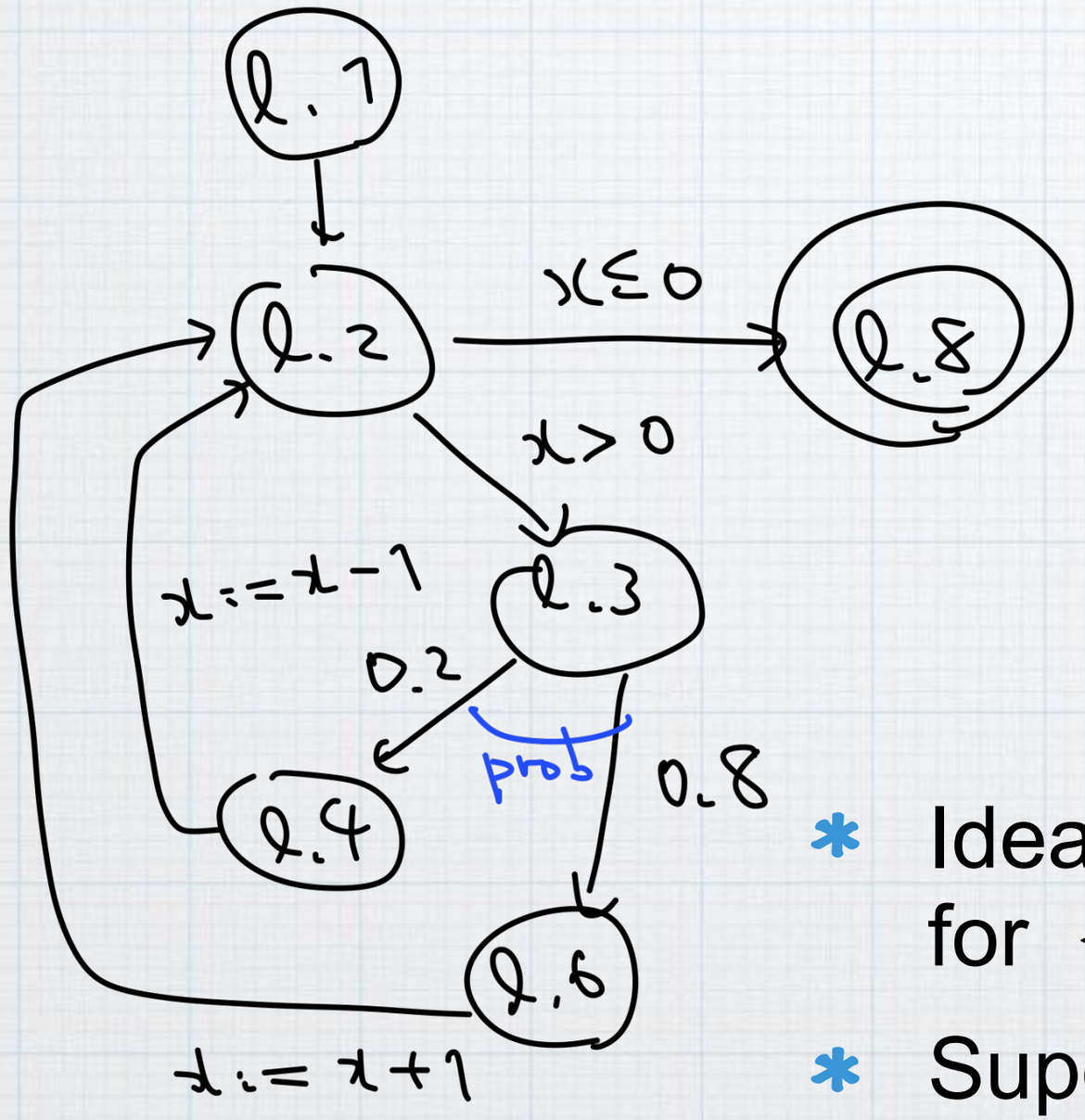
- **Coalgebras**: excitements, afterthoughts, … Still I love them!
  - Buechi and parity conditions
    [Urabe, Shimizu & IH, CONCUR'16] [Urabe & IH, CMCS'18]
    ➜ Tutorial at CONCUR'18
- Real-world application of categorical methods. Our approach
  - As a **metatheory**
    - for deriving object-level (accessible and automated) techniques
- Reachability in probabilistic programs is **rich**
  - **Martingale** methods for (over-/under-) approximations
    - Role of **concentration lemmas**
    - Knaster-Tarski foundation is still useful

We're hiring!
Max 3.5 yrs, PD & senior researchers
logic + automata + categories + machine learning + software engineering
➜ CPS, automated driving

Thank you for your attention!
Ichiro Hasuo (NII, Tokyo)
http://group-mmm.org/~ichiro/

Appendix

Probabilistic Control Flow Graph (pCFG) See e.g. [Chatterjee+, POPL'17]




```
1  x := m
2  while x > 0 do
3     if prob(p) do
4        x := x − 1
5     else
6        x := x + 1
7     fi
8  od
```

(say, $m = 16$ and $p = 0.2$)

* Idea: a state l in pCFG stands for $\{ (l, [x \mapsto r]) \mid r \in \mathbb{R} \}$
* Supermartingales are given by $\eta_l : \mathbb{R}^{\{x\}} \to \mathbb{R}, \qquad i = 1, \ldots, 8$

Template-Based Synthesis

- Let's use linear templates, for example
- Meaning: $\eta_l : \mathbb{R}^{\{x\}} \to \mathbb{R}, \qquad i = 1, \ldots, 8$

  $\eta_l(r) \equiv a_l r + b_l$
  - a_l, b_l: undetermined parameters
  - They are determined so that supermartingale constraints are satisfied, e.g.
- Constraint solving by LP, SDP, QE, …

Def.

Let $(S, S \xrightarrow{\mathbf{tr}} \mathcal{D}S)$ be a MC, $C \subseteq S$.

$\eta : S \to \mathbb{R}_{\geq 0}$ is a *ranking supermartingale* for C if

- $\forall s \in S \setminus C. \quad \eta(s) \geq (\mathbb{X}\eta)(s) + 1.$
- $\eta(s) = 0$ implies $s \in C$

		Answers what question?	Underlying math
ranking supermartingale (**lower** bd)	**Additive** ranking supermartingale [McIver+ PSSE'04] [Chakarov+ CAV'13]	$\mathbf{Pr}(\mathrm{Reach}c) =^{?} 1$ $\mathbf{Exp}(\mathrm{Steps}c)$ <= ??	(elementary)
	Multiplicative ranking supermartingale [Urabe+ LICS'17]	$\mathbf{Pr}(\mathrm{Reach}c)$ >= ??	• LP characterization • (Categorical consideration)
repulsing supermartingale (**upper** b	**ε-decreasing** repulsing supermartingale [Chatterjee+ POPL'17]	$\mathbf{Pr}(\mathrm{Reach}c)$ <= ??	Azuma's inequality for martingale concentration
	Nonnegative repulsing supermartingale [Steinhardt+ IJRR'12] [Takisaka+, in preparation]	$\mathbf{Pr}(\mathrm{Reach}c)$ <= ??	Markov's inequality for martingale concentration

Preliminary Experimental Results

```
1   x := m
2   while  x > 0  do
3      if  x < N  do
4         if  prob(p)  do
5            x := x − 1
6         else
7            x := x + 1
8         fi
9      else
10        x := x + 1
11     fi
12  od
```

Fig. 1. APP corresponding to Example 1

```
1   x := Geometric(0.5)
2   while  x ≥ 1  do
3      x := x − 1
4   od
5   if  prob(0.5)  do
6      while  x ≤ 0  do
7         x := x − 1
8      od
9   else
10     skip
11  od
```

Fig. 2. APP corresponding to Example 2

```
1   x := Uniform[0, 1]
2   while  x < 1  do
3      if  prob(p)  do
4         x := 2 ∗ x
5      else
6         x := 0.5 ∗ x
7      fi
8   od
```

Fig. 3. APP corresponding to Example 3

```
1   x := m
2   while  x > 0  do
3      if  prob(p)  do
4         x := x − 1
5      else
6         x := x + 1
7      fi
8   od
```

Fig. 4. APP corresponding to Example 4

Preliminary Experimental Results

```
1   x := m
2   while  x > 0  do
3      if  x < N  do
4         if  prob(p)  do
5            x := x − 1
6         else
7            x := x + 1
8         fi
9      else
10        x := x + 1
11     fi
12  od
```

Fig. 1. APP corresponding to Example 1

```
1   x := Geometric(0.5)
2   while  x ≥ 1  do
3      x := x − 1
4   od
5   if  prob(0.5)  do
6      while  x ≤ 0  do
7         x := x − 1
8      od
9   else
10     skip
11  od
```

Fig. 2. APP corresponding to Example 2

```
1   x := Uniform[0, 1]
2   while  x < 1  do
3      if  prob(p)  do
4         x := 2 ∗ x
5      else
6         x := 0.5 ∗ x
7      fi
8   od
```

Fig. 3. APP corresponding to Example 3

```
1   x := m
2   while  x > 0  do
3      if  prob(p)  do
4         x := x − 1
5      else
6         x := x + 1
7      fi
8   od
```

Fig. 4. APP corresponding to Example 4

example	true reachability probability	Nonnegative (ours)	ε-decreasing
1	$\frac{(0.4/0.6)^5-(0.4/0.6)^{10}}{1-(0.4/0.6)^{10}} \approx 0.116364$	0.5054945055	< 1
2	0.5	0.5	—
2a	0.5	0.5	—
2b	0.5	0.5	—
3	$\int_0^1 (\frac{0.25}{0.75})^{\lceil \log_2(1/x) \rceil} dx \approx 0.2$	0.5	—
4	$(\frac{0.25}{0.75})^1 \approx 0.333333$	—	< 1