

# 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



**We're hiring!**

Max 4 yrs, PD & senior researchers  
logic + automata + categories +  
machine learning + SE → CPS

## Approximating Reachability Probabilities by (Super-)Martingales

**NII**



**Ichiro Hasuo**

National Institute of Informatics  
Tokyo, Japan

# First Question

- \* Each of Alice, Bob and Charlie has some apples.
- \* On average one has  $\leq 2.5$  apples.
- \* How many can Alice have, at most?

# Overview

- \* Reachability in **probabilistic programs**
  - \* Need of “parameters”
- \* **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)
- \* Automated Synthesis

# 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.  
**Supermartingales for Refuting Reachability of Probabilistic Programs: Completeness.**  
In preparation

# Probabilistic Programs

- \* Programs with

- \* random assignment

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

- \* probabilistic branching

```
if prob(0.2)
```

- \* (also nondet. assignment & branching)

- \* Example: right (random walk)

- \* We disregard the Bayesian aspects

- \* observations, conditioning, priors/posteriors, etc.

- \* See e.g. [Gordon+, FOSE'14])

```
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  $p = 0.2$ )
```

# Probabilistic Programs

```
1  $x := m$ 
2 while  $x > 0$  do
3   if  $\text{prob}(p)$  do
4      $x := x - 1$ 
5   else
6      $x := x + 1$ 
7   fi
8 od
```

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

```
int goats, tigers;
double c1, c2, c3, curTime;
// initialize populations
goats = 100; tigers = 4;
// initialize reaction rates
c1 = 1; c2 = 5; c3 = 1;
//initialize time
curTime = 0;

while (curTime < TIMELIMIT)
{
  if (goats > 0 && tigers > 0)
  {
    double rate1, rate2, rate3,
           rate;
    rate1 = c1 * goats;
    rate2 = c2 * goats * tigers;
    rate3 = c3 * tigers;
    rate = rate1 + rate2 + rate3;

    double dwellTime =
      Exponential(rate);
    int discrete =
      Disc3(rate1/rate,rate2/rate);
    curTime += dwellTime;
    switch (discrete)
    {
      case 0: goats++; break;
      case 1: goats--; tigers++;
              break;
      case 2: tigers--; break;
    }
  }
}
```

```
else if (goats > 0)
{
  double rate;
  rate = c1 * goats;
  double dwellTime =
    Exponential(rate);
  curTime += dwellTime;
  goats++;
}
else if (tigers > 0)
{
  double rate;
  rate = c3 * tigers;
  double dwellTime =
    Exponential(rate);
  curTime += dwellTime;
  tigers--;
}
} //end while loop
return(goats,tigers);
}
```

[Gordon+, FOSE'14]

Figure 10: Lotka-Volterra Population Model.

# Reachability Probabilities in PP

\* **Question** What is  $\Pr(\text{the program terminates})$ ?

```
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
```

\* How do we define it?

\* Configuration graph

\* A state is a pair (program location, valuation)

\* Transition by small-step operations

\*  $\rightarrow$  MDP (Markov decision processes)  $M$

real-valued variables

$\rightarrow$  infinite states

$\rightarrow$  not for automated analysis

\*  $\Pr(\text{Term}) = \sup_{\sigma: \text{scheduler}} (M^\sigma \text{ reaches } \odot)$

If nondet. is  
angelic...

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

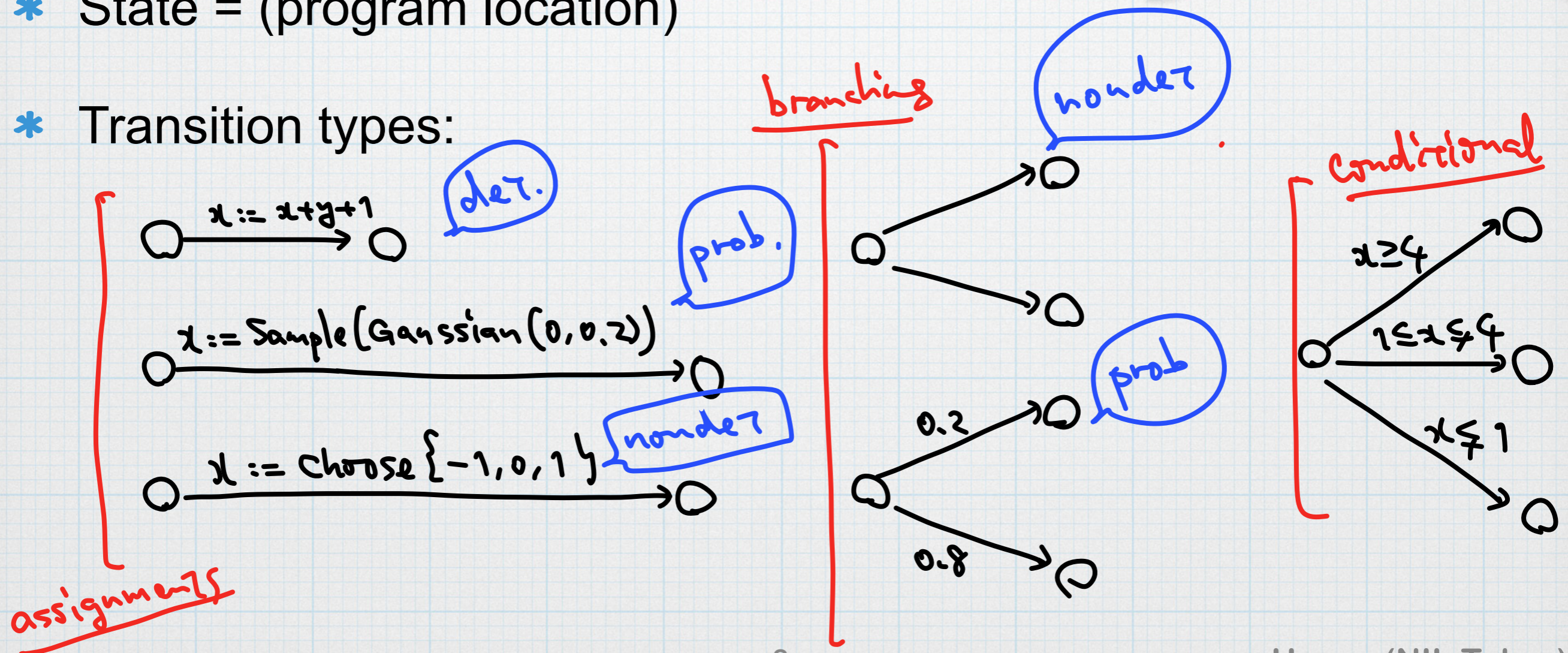
- \* Finite graph,  
“parametric” in memory states
  - \* (... justifies my presence here!)

```
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  $p = 0.2$ )

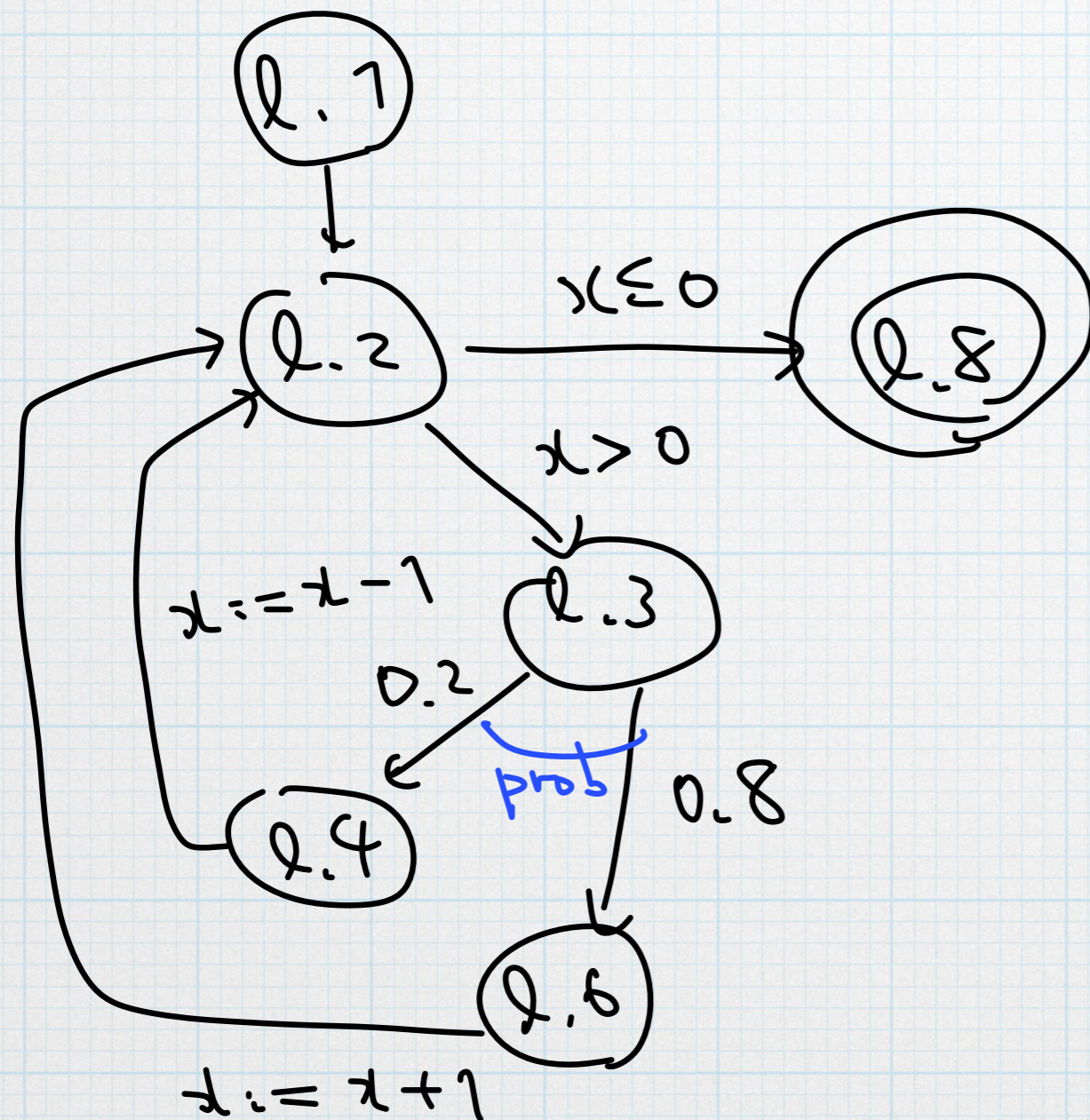
- \* State = (program location)

- \* 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  $p = 0.2$ )

# Our 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

$\Pr(\text{Reach}c)$

# Our Approach

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

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

to give *approximate* answers. Template-based synthesis

- \* Qualitative questions

- \*  $\Pr(\text{Reach}_C) \stackrel{?}{=} 1$  (almost sure reachability)

- \*  $\Pr(\text{Reach}_C) \stackrel{?}{\geq} \alpha$  (threshold reachability)

- \* Quantitative questions

- \*  $\Pr(\text{Reach}_C) \geq ??$  (lowerbound, “verification”)

- \*  $\Pr(\text{Reach}_C) \leq ??$  (upperbound, “refutation”)

- \*  $\mathbf{Exp}(\text{StepsToReach}_C)$ , upperbound, lowerbound, ...

- \* “Concentration” [Chatterjee+, POPL’16]

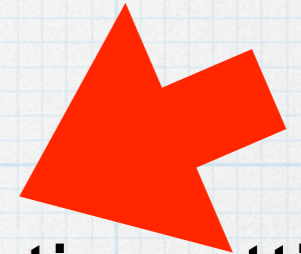
Find  $B$  s.t.  $(x > B \rightarrow \Pr(\text{StepsToReach}_C > x) < a e^{-bx})$

# Why Overapproximation?

- \*  $\Pr(\text{Reach}c) \leq \alpha$   
if and only if  
 $\Pr(\text{NotReach}c) \geq 1 - \alpha$
- \* Refutation of reachability  
is  
verification of safety

# Overview

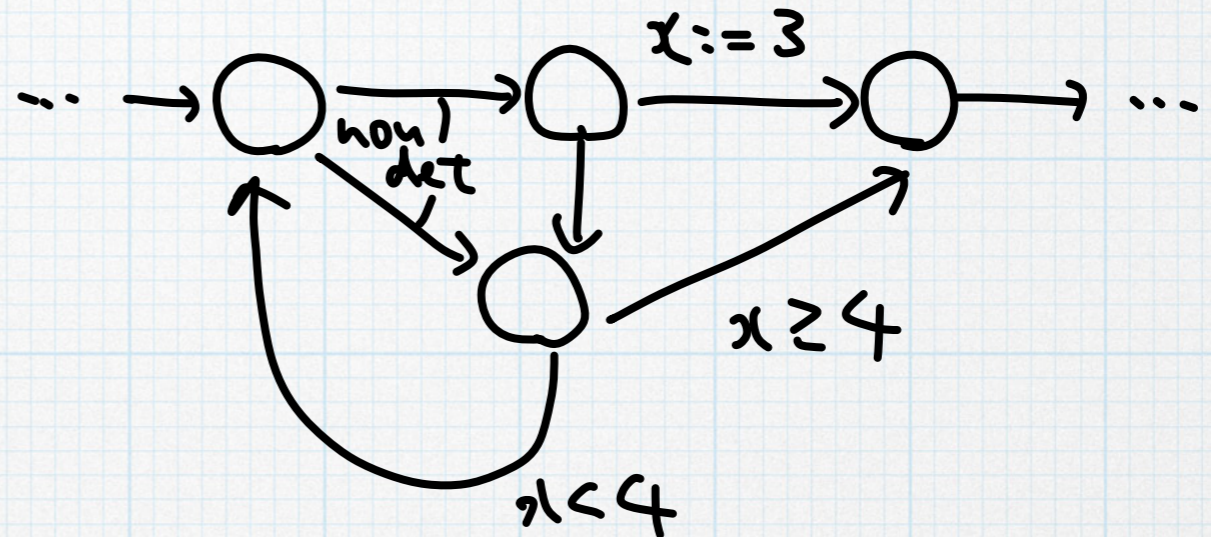
- \* Reachability in **probabilistic programs**
  - \* Need of “parameters”
- \* **Foundation of fixed points**, in the non-probabilistic setting
  - \* Ranking functions, invariants
  - \* Foundation: Knaster-Tarski, Cousot-Cousot
- \* **Known supermartingale** methods
  - \* Roles of concentration lemmas
- \* Something **new** (from our recent results)
- \* Automated Synthesis



# In Case of No Probabilities...

- \* pCFG

- \* 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

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

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

such that

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

Thm.

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

- \*  $\eta$  overapproximates #(steps to  $C$ )
- \* Note: {natural numbers} is well-founded
- \* Discrete analogue of (certain) **Lyapunov functions...**

# Invariants

$(S, \rightarrow \subseteq S \times S)$ : 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

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

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

such that

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

Thm.

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

$(S, \rightarrow \subseteq S \times S)$ : 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?

$$\text{Reach}_C = \mu C \cup \diamond \text{Reach}_C$$

\* NB:

$$\text{NotReach}_C = \nu (S \setminus C) \cap \Box \text{NotReach}_C$$

# Lattice-Theoretic Foundation

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

Thm. (Knaster-Tarski)

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

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

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

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

Thm. (Cousot-Cousot)

$\perp \sqsubseteq f(\perp) \sqsubseteq \dots \sqsubseteq f^\omega(\perp) \sqsubseteq \dots$   
stabilizes, and converges to  $\mu f$

$$\implies f^\alpha(\perp) \sqsubseteq \mu f \quad (\forall \alpha \in \text{Ord})$$

$\top \supseteq f(\top) \supseteq \dots \supseteq f^\omega(\top) \supseteq \dots$   
stabilizes, and converges to  $\nu f$

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

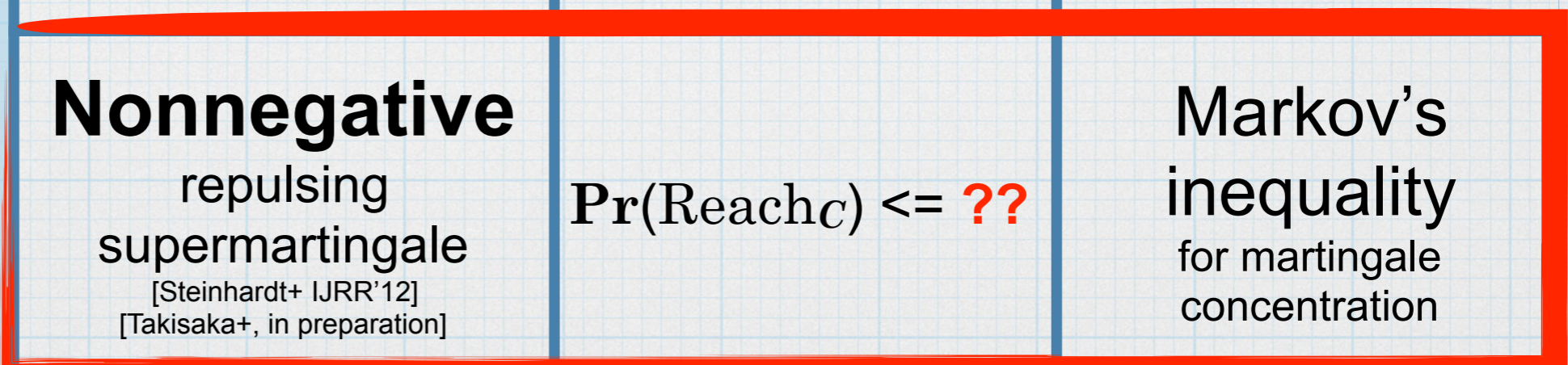
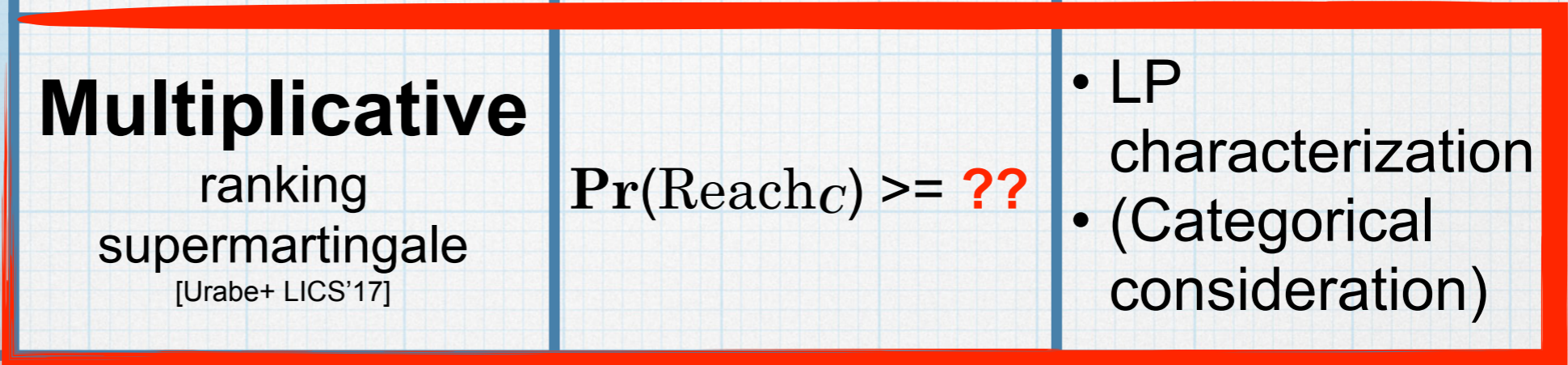
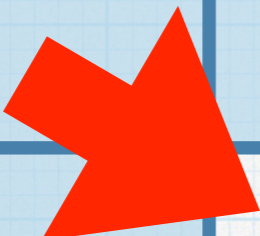
**Sound approx. from below**

# Overview

- \* Reachability in **probabilistic**
  - \* Need of “parameters”
- \* **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)
- \* Automated Synthesis

	KT	CC
lfp	<b>overapprox.</b>	underapprox.
gfp	underapprox.	<b>overapprox.</b>

		Answers what question?	Underlying math
<b>ranking</b> supermartingale ( <b>lower</b> bd)	<b>Additive</b> ranking supermartingale <small>[McIver+ PSSE'04] [Chakarov+ CAV'13]</small>	$\Pr(\text{Reach}_C) = ? 1$ $\text{Exp}(\text{Steps}_C) \leq ??$	(elementary)
	<b>Multiplicative</b> ranking supermartingale <small>[Urabe+ LICS'17]</small>	$\Pr(\text{Reach}_C) \geq ??$	<ul style="list-style-type: none"> <li>• LP characterization</li> <li>• (Categorical consideration)</li> </ul>
<b>repulsing</b> supermartingale ( <b>upper</b> bd)	<b><math>\epsilon</math>-decreasing</b> repulsing supermartingale <small>[Chatterjee+ POPL'17]</small>	$\Pr(\text{Reach}_C) \leq ??$	Azuma's inequality for martingale concentration
	<b>Nonnegative</b> repulsing supermartingale <small>[Steinhardt+ IJRR'12]            [Takisaka+, in preparation]</small>	$\Pr(\text{Reach}_C) \leq ??$	Markov's inequality for martingale concentration



# Disclaimer

- \* From now on:  
no nondeterminism, no parametrization
- \* Our setting is therefore:  
A Markov chain  $(S, S \xrightarrow{\text{tr}} \mathcal{D}S)$ , and  $C \subseteq S$

# Additive Ranking Supermartingale

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

## Def.

Let  $(S, S \xrightarrow{\text{tr}} \mathcal{D}S)$  be a MC,  
 $\eta: S \rightarrow \mathbb{R}$  be a function.

$\mathbb{X}\eta: S \rightarrow \mathbb{R}$  is defined by

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

\* Overapprox.  
**Exp(Steps to C)**

## Def.

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

$\eta: S \rightarrow \mathbb{R}_{\geq 0}$  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  $(S, S \xrightarrow{\text{tr}} \mathcal{D}S)$  be a MC,  
 $\eta: S \rightarrow \mathbb{R}$  be a function.

$\mathbb{X}\eta: S \rightarrow \mathbb{R}$  is defined by

$$\begin{aligned}(\mathbb{X}\eta)(s) &= \sum_{s'} \text{tr}(s) \\ &= \sum_{s'} \text{Pr}(s \rightarrow s') \\ &= \text{Exp}(\eta(s))\end{aligned}$$

\* Overapprox.  
**Exp(Steps to  $C$ )**

## Def.

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

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

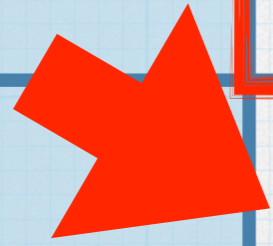
- $\forall s \in S \setminus C. \eta(s) \geq (\mathbb{X}\eta)(s) + 1.$
- $\eta(s) = 0$  implies  $s \in C$

## Thm.

Let  $\eta$  be a ranking supermartingale for  $C$ . Then:

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

		Answers what question?	Underlying math
<b>ranking</b> supermartingale ( <b>lower</b> bd)	<b>Additive</b> ranking supermartingale <small>[McIver+ PSSE'04] [Chakarov+ CAV'13]</small>	$\Pr(\text{Reach}_C) \stackrel{?}{=} 1$ $\text{Exp}(\text{Steps}_C) \leq ??$	(elementary)
	<b>Multiplicative</b> ranking supermartingale <small>[Urabe+ LICS'17]</small>	$\Pr(\text{Reach}_C) \geq ??$	<ul style="list-style-type: none"> <li>• LP characterization</li> <li>• (Categorical consideration)</li> </ul>
<b>repulsing</b> supermartingale ( <b>upper</b> bd)	<b><math>\epsilon</math>-decreasing</b> repulsing supermartingale <small>[Chatterjee+ POPL'17]</small>	$\Pr(\text{Reach}_C) \leq ??$	Azuma's inequality for martingale concentration
	<b>Nonnegative</b> repulsing supermartingale <small>[Steinhardt+ IJRR'12]            [Takisaka+, in preparation]</small>	$\Pr(\text{Reach}_C) \leq ??$	Markov's inequality for martingale concentration





# $\epsilon$ -Decreasing Repulsing Supermartingale

[Chatterjee+ POPL'17]

## Def.

Let  $(S, S \xrightarrow{\text{tr}} \mathcal{DS})$  be a MC,  $C \subseteq S$ ,  $\epsilon > 0$ ,  $\kappa > 0$ .

$\eta: S \rightarrow \mathbb{R}$  is an  $\epsilon$ -decreasing repulsing supermartingale for  $C$  with  $\kappa$ -b'dd difference if

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

## Thm.

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

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

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

# $\epsilon$ -Decreasing Repulsing Supermartingale

[Chatterjee+ POPL'17]

## Def.

Let  $(S, S \xrightarrow{\text{tr}} \mathcal{DS})$  be a MC,  $C \subseteq S$ ,  $\epsilon > 0$ ,  $\kappa > 0$ .

$\eta: S \rightarrow \mathbb{R}$  is an  $\epsilon$ -decreasing repulsing supermartingale for  $C$  with  $\kappa$ -b'dd difference if

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

## Thm.

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

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

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



# $\epsilon$ -Decreasing Repulsing Supermartingale

[Chatterjee+ POPL'17]

## Def.

Let  $(S, S \xrightarrow{\text{tr}} \mathcal{DS})$  be a MC,  $C \subseteq S$ ,  $\epsilon > 0$ ,  $\kappa > 0$ .

$\eta: S \rightarrow \mathbb{R}$  is an  $\epsilon$ -decreasing repulsing supermartingale for  $C$  with  $\kappa$ -b'dd difference if

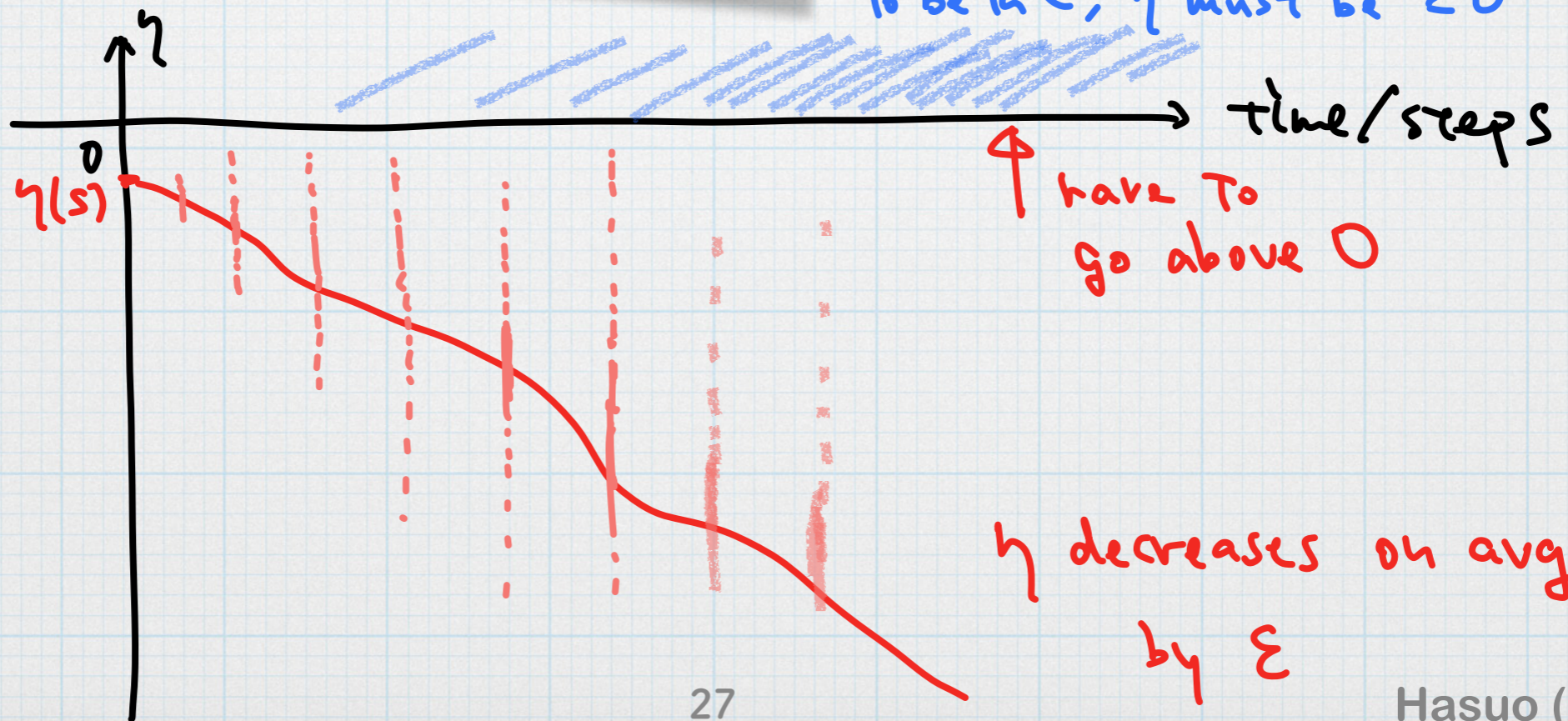
- $\forall s \in S \setminus C. \eta(s) \geq (\mathbb{X}\eta)(s) + \epsilon.$
- $\forall c \in C. \eta(c) \geq 0.$
- $\forall s \in S. \forall s' \in \text{supp}(\text{tr}(s)).$   
 $|\eta(s) - \eta(s')| \leq \kappa.$

## Thm.

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

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

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



# $\epsilon$ -Decreasing Repulsing Supermartingale

[Chatterjee+ POPL'17]

## Def.

Let  $(S, S \xrightarrow{\text{tr}} \mathcal{DS})$  be a MC,  $C \subseteq S$ ,  $\epsilon > 0$ ,  $\kappa > 0$ .

$\eta: S \rightarrow \mathbb{R}$  is an  $\epsilon$ -decreasing repulsing supermartingale for  $C$  with  $\kappa$ -b'dd difference if

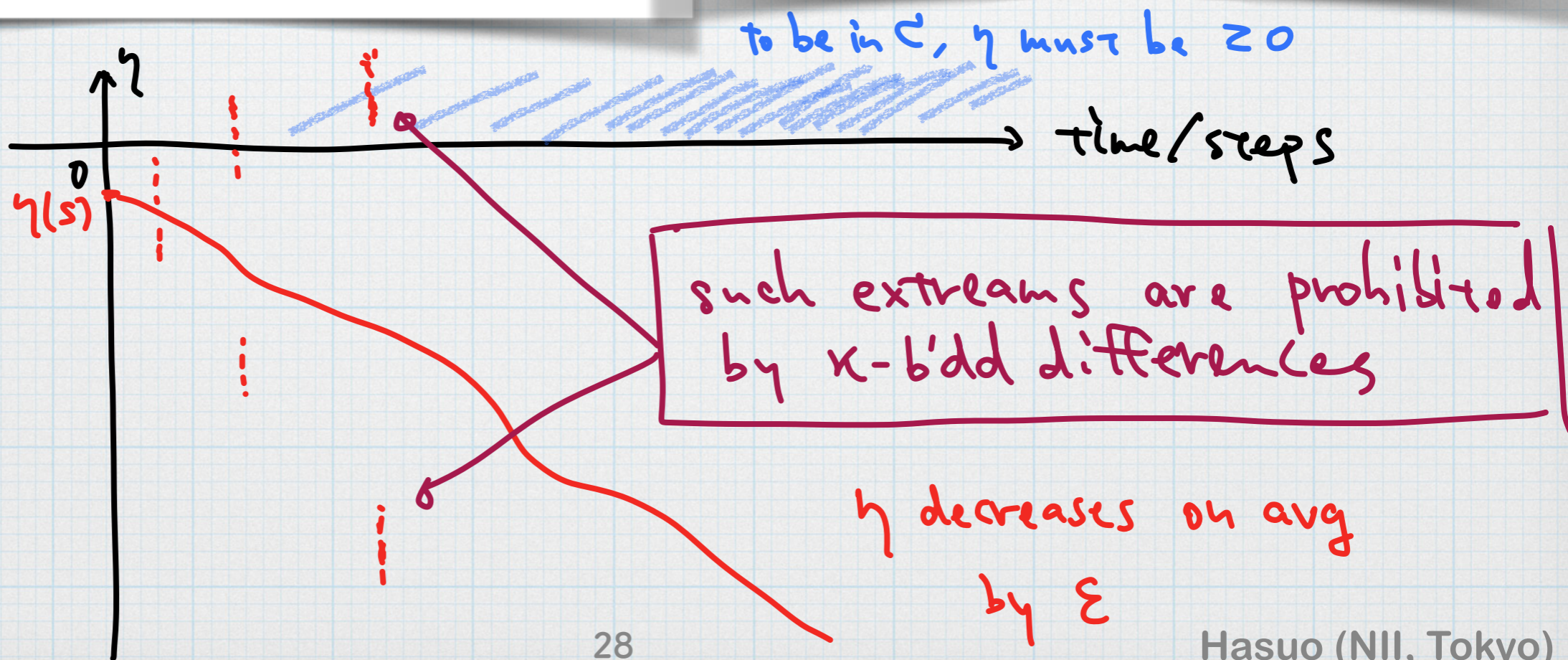
- $\forall s \in S \setminus C. \eta(s) \geq (\mathbb{X}\eta)(s) + \epsilon.$
- $\forall c \in C. \eta(c) \geq 0.$
- $\forall s \in S. \forall s' \in \text{supp}(\text{tr}(s)).$   
 $|\eta(s) - \eta(s')| \leq \kappa.$

## Thm.

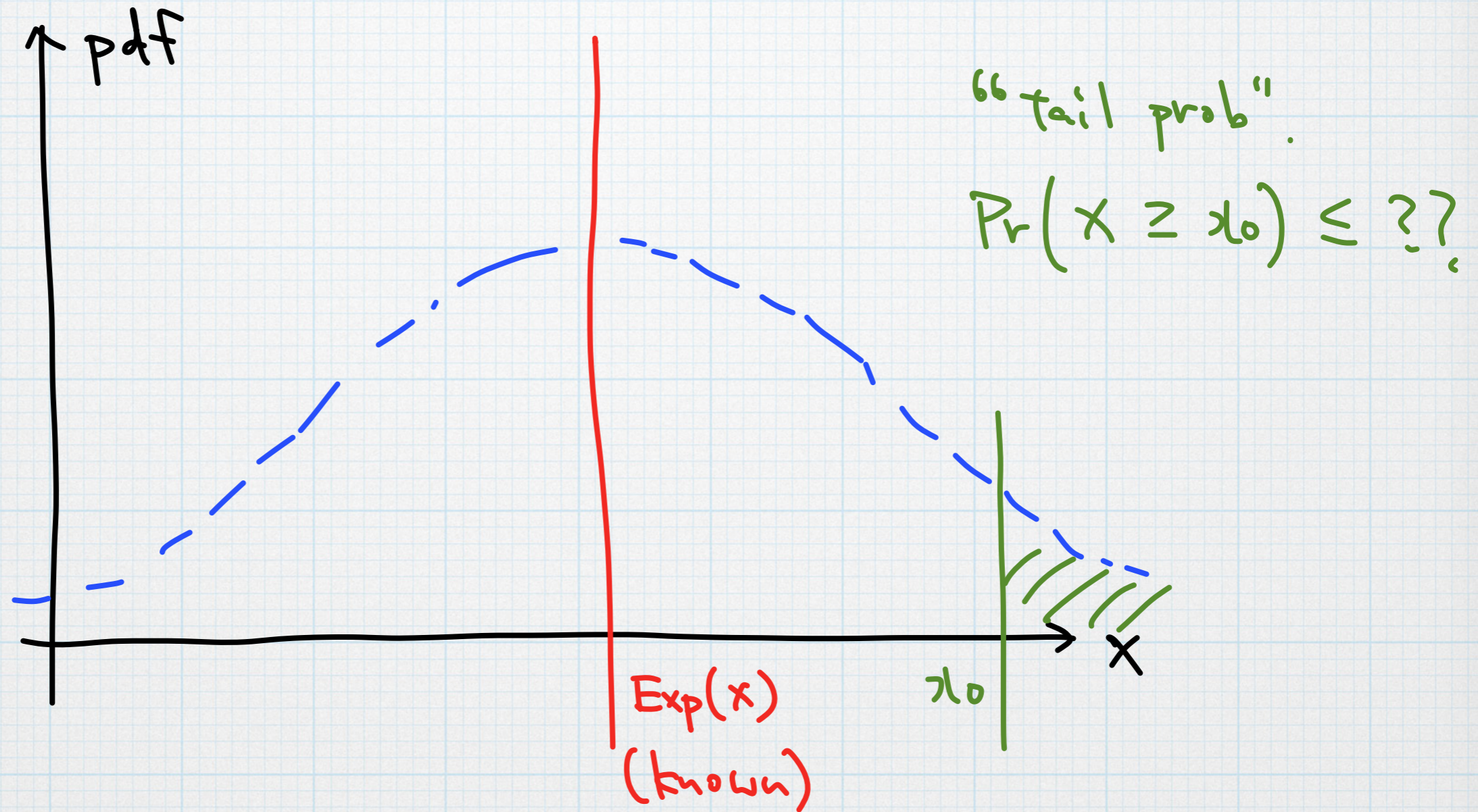
Let  $\eta$  be such a repulsing supermartingale for  $C$ . Assume  $\eta(s) < 0$ . Then

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

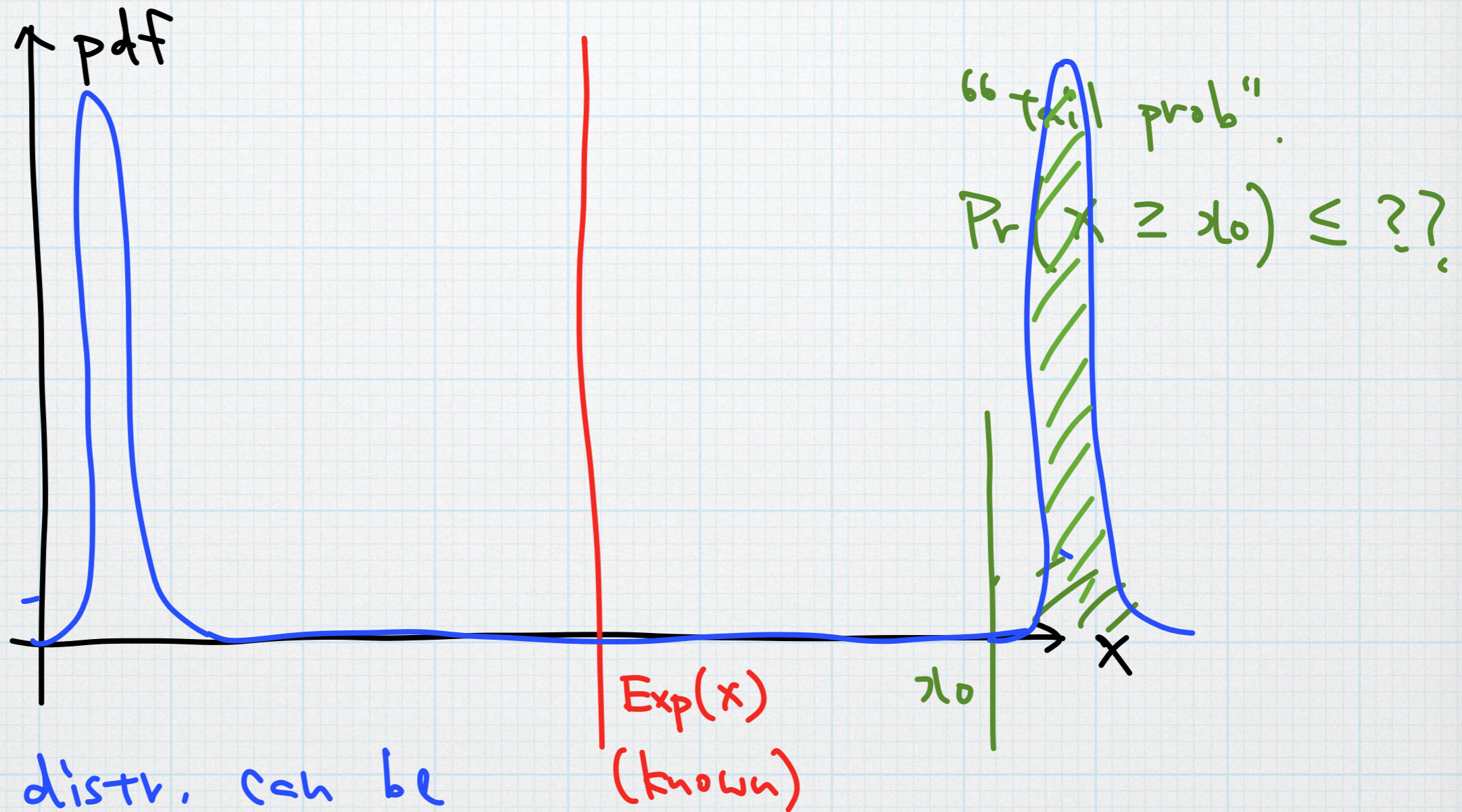
where  $\alpha = e^{\frac{\epsilon \cdot \eta(s)}{(\kappa + \epsilon)^2}}$ ,  $\gamma = e^{-\frac{\epsilon^2}{2(\kappa + \epsilon)^2}}$ .



# 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  $(S, S \xrightarrow{\text{tr}} \mathcal{D}S)$  be a MC.  
A *supermartingale* is  $\eta: S \rightarrow \mathbb{R}$  such that

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

If one-step  
difference is  
bounded...

Rem. Let  $s_0 \rightarrow s_1 \rightarrow \dots$  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  $\eta$  have  $\kappa$ -bdd difference. For each  $\lambda > 0$   
and  $n \in \mathbb{N}$ ,

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

# 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  $\mu$  and variance  $\sigma^2$ . 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  $\eta$  be a supermartingale, where

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

$$\text{Var}(\eta(s') \mid s \rightarrow s') \leq \sigma^2$$

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

$$|\eta(s_i) - \text{Exp}(\eta(s_i))| \leq M$$

Then

$$\Pr(\eta(s_n) - \eta(s_0) \geq \lambda) \leq \exp\left(\frac{-\lambda^2}{2n\sigma^2 + \frac{2}{3}M\lambda}\right)$$

		Answers what question?	Underlying math
<b>ranking</b> supermartingale ( <b>lower</b> bd)	<b>Additive</b> ranking supermartingale [Mclver+ PSSE'04] [Chakarov+ CAV'13]	$\Pr(\text{Reach}_C) \stackrel{?}{=} 1$ $\text{Exp}(\text{Steps}_C) \leq ??$	(elementary)
	<b>Multiplicative</b> ranking supermartingale [Urabe+ LICS'17]	$\Pr(\text{Reach}_C) \geq ??$	<ul style="list-style-type: none"> <li>• LP characterization</li> <li>• (Categorical consideration)</li> </ul>
<b>repulsing</b> supermartingale ( <b>upper</b> bd)	<b><math>\epsilon</math>-decreasing</b> repulsing supermartingale [Chatterjee+ POPL'17]	$\Pr(\text{Reach}_C) \leq ??$	Azuma's inequality for martingale concentration
	<b>Nonnegative</b> repulsing supermartingale [Steinhardt+ IJRR'12] [Takisaka+, in preparation]	$\Pr(\text{Reach}_C) \leq ??$	Markov's inequality for martingale concentration

# Overview

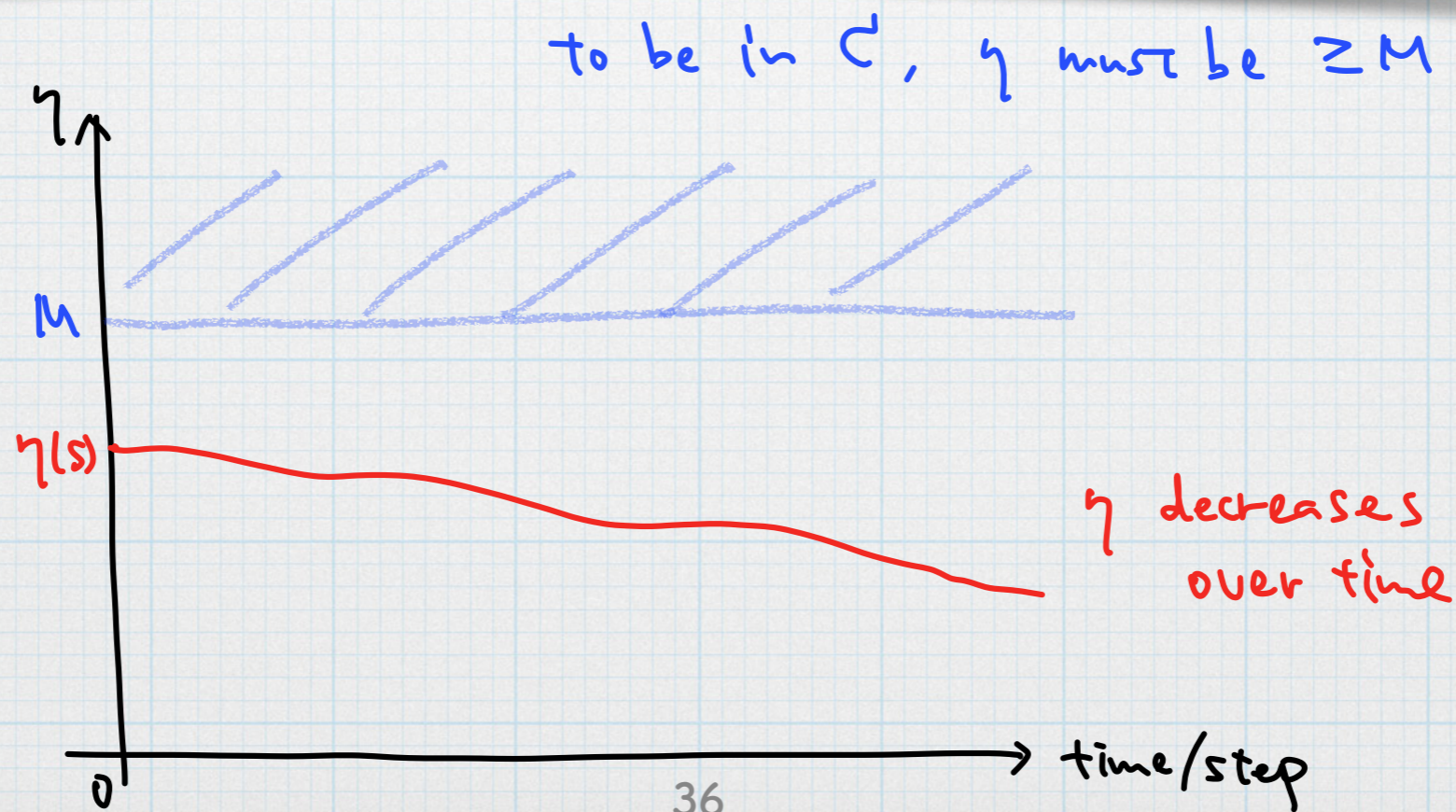
- \* Reachability in **probabilistic programs**
  - \* Need of “parameters”
- \* **Foundation of fixed points**, in the non-probabilistic setting
  - \* Ranking functions, invariants
  - \* Foundation: Knaster-Tarski, Cousot-Cousot
- \* **Known supermartingale** methods
  - \* Roles of concentration lemmas
- \* Something **new** (from our recent results)
- \* Automated Synthesis

# Nonnegative Repulsing Supermartingale

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

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

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

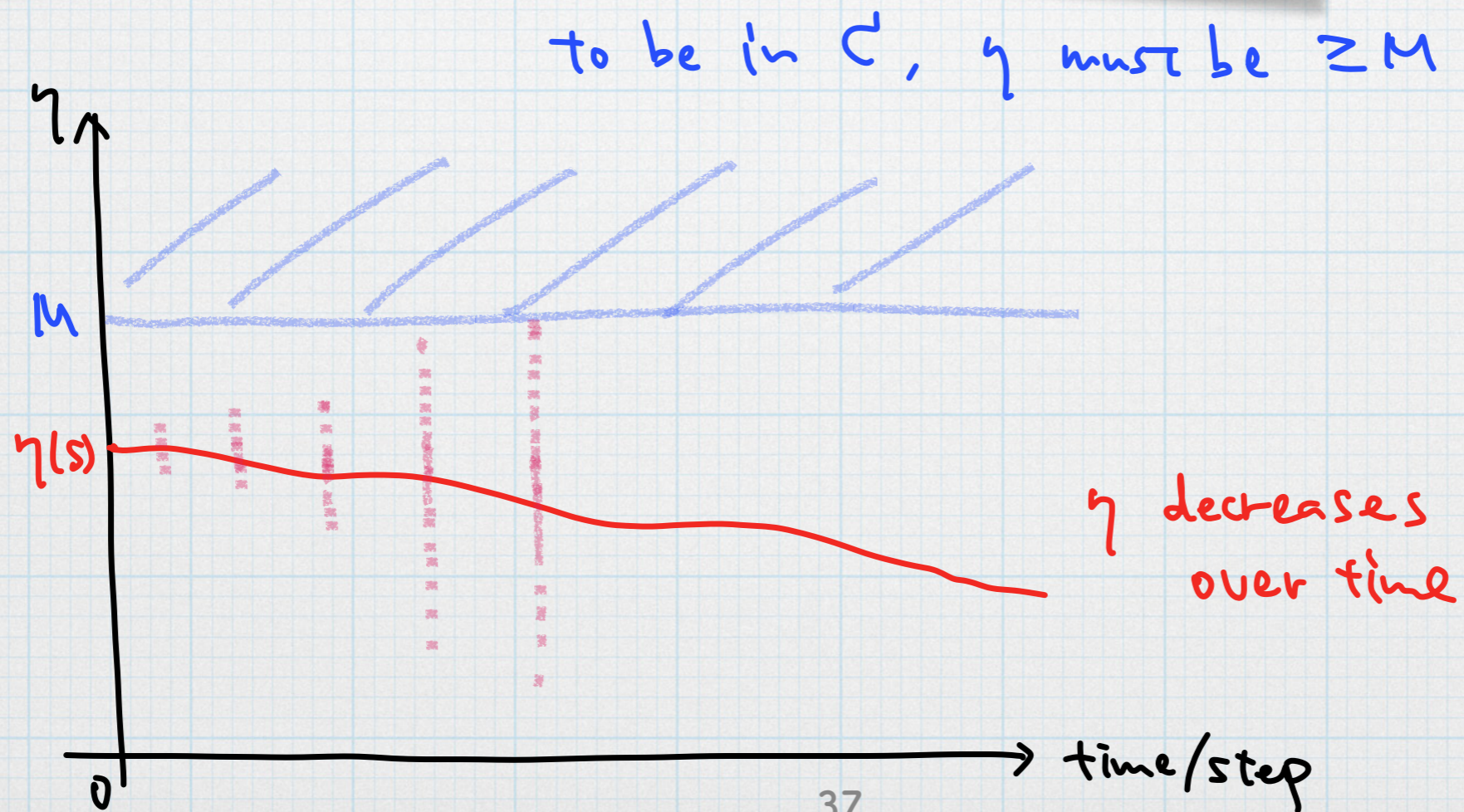


# Nonnegative Repulsing Supermartingale

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

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

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

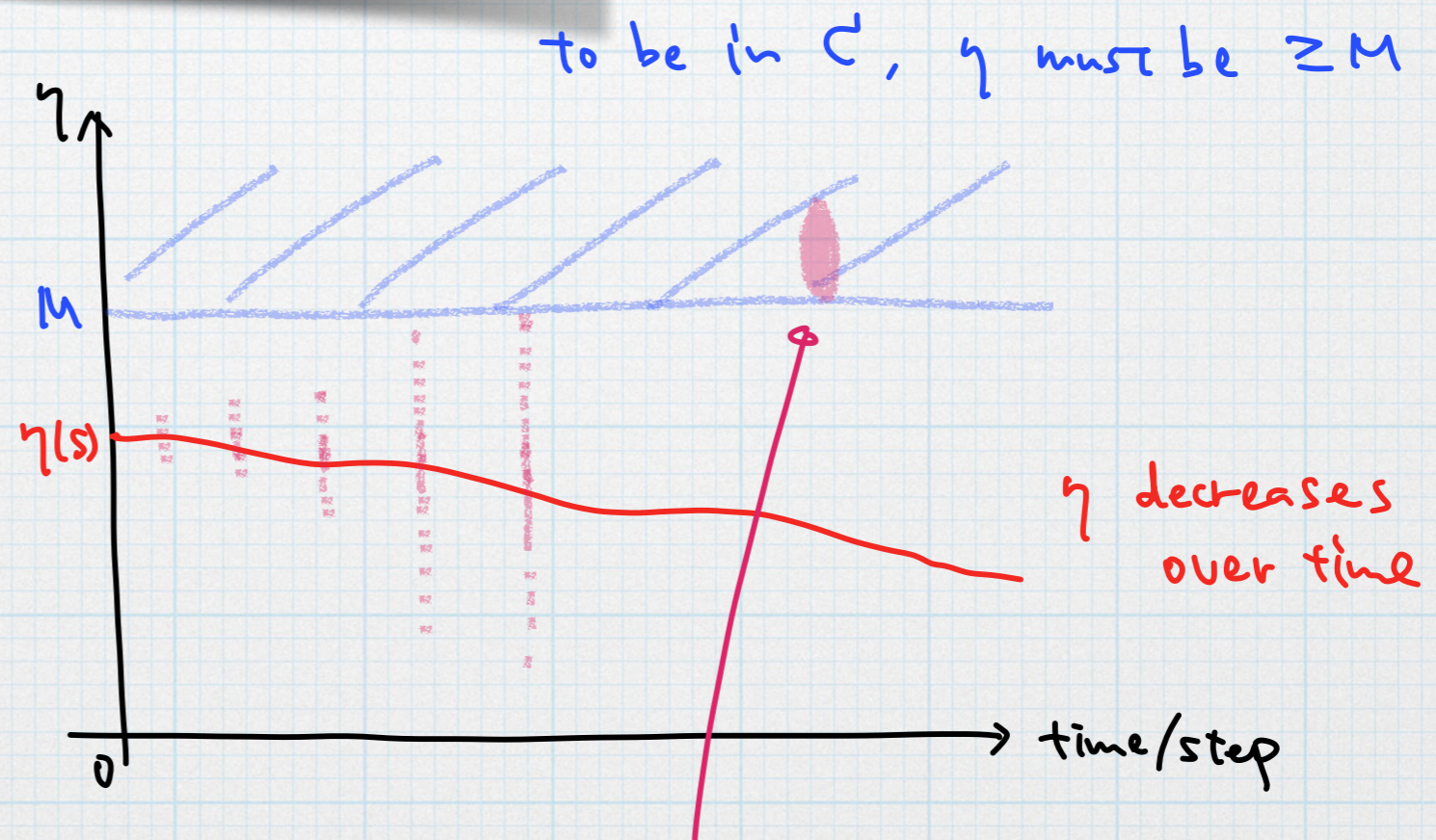


# Nonnegative Repulsing Supermartingale

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

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

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



# First Question, Again

- \* Each of Alice, Bob and Charlie has some apples.
- \* On average one has  $\leq 2.5$  apples.
- \* How many can Alice have, at most?

# Nonnegative Repulsing Supermartingale

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

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

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

**Thm. (upper bound)**

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

**Thm. (completeness)** There exists a nonnegative repulsing supermartingale  $\eta$  for  $C$  at  $M$  such that

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

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



		Answers what question?	Underlying math
<b>ranking</b> supermartingale ( <b>lower</b> bd)	<b>Additive</b> ranking supermartingale <small>[McIver+ PSSE'04] [Chakarov+ CAV'13]</small>	$\Pr(\text{Reach}_C) \stackrel{?}{=} 1$ $\text{Exp}(\text{Steps}_C) \leq ??$	(elementary)
	<b>Multiplicative</b> ranking supermartingale <small>[Urabe+ LICS'17]</small>	$\Pr(\text{Reach}_C) \geq ??$	<ul style="list-style-type: none"> <li>• LP characterization</li> <li>• (Categorical consideration)</li> </ul>
<b>repulsing</b> supermartingale ( <b>upper</b> bd)	<b><math>\epsilon</math>-decreasing</b> repulsing supermartingale <small>[Chatterjee+ POPL'17]</small>	$\Pr(\text{Reach}_C) \leq ??$	Azuma's inequality for martingale concentration
	<b>Nonnegative</b> repulsing supermartingale <small>[Steinhardt+ IJRR'12]            [Takisaka+, in preparation]</small>	$\Pr(\text{Reach}_C) \leq ??$	<b>Knaster-Tarski!</b>

# Concentration of Measure: No Need!

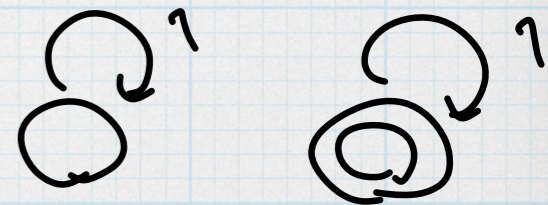
Def. Let  $(S, S \xrightarrow{\text{tr}} \mathcal{D}S)$  be a MC,  $C \subseteq S$ .  
Let  $\mathbb{X}_C : [0, 1]^S \rightarrow [0, 1]^S$  be defined by

$$\left( \eta : S \rightarrow [0, 1] \right) \xrightarrow{\mathbb{X}_C} \left( \begin{array}{l} \mathbb{X}_C \eta : S \rightarrow [0, 1] \\ s \mapsto \begin{cases} 1 & \text{if } s \in C \\ (\mathbb{X}\eta)(s) & \text{if } s \notin C \end{cases} \end{array} \right)$$

Thm. (upper bound)

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

(Easy from the Cousot-Cousot characterization of lfp)



Rem.

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

# Lattice-Theoretic Foundation

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

Thm. (Knaster-Tarski)

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

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

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

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

Thm. (Cousot-Cousot)

$\perp \sqsubseteq f(\perp) \sqsubseteq \dots \sqsubseteq f^\omega(\perp) \sqsubseteq \dots$   
stabilizes, and converges to  $\mu f$

$$\implies f^\alpha(\perp) \sqsubseteq \mu f \quad (\forall \alpha \in \text{Ord})$$

$\top \supseteq f(\top) \supseteq \dots \supseteq f^\omega(\top) \supseteq \dots$   
stabilizes, and converges to  $\nu f$

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

# Concentration of Measure: No Need!

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

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

that is,

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

Then, for each  $s \in S$ ,

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

- \* Derivation of nonnegative repulsing supermartingale from the Knaster-Tarski theorem
- \* Soundness and completeness follow easily

		Answers what question?	Underlying math
<b>ranking</b> supermartingale ( <b>lower</b> bd)	<b>Additive</b> ranking supermartingale <small>[McIver+ PSSE'04] [Chakarov+ CAV'13]</small>	$\Pr(\text{Reach}_C) \stackrel{?}{=} 1$ $\text{Exp}(\text{Steps}_C) \leq ??$	(elementary)
	<b>Multiplicative</b> ranking supermartingale <small>[Urabe+ LICS'17]</small>	$\Pr(\text{Reach}_C) \geq ??$	<ul style="list-style-type: none"> <li>• LP characterization</li> <li>• (Categorical consideration)</li> </ul>
<b>repulsing</b> supermartingale ( <b>upper</b> bd)	<b><math>\epsilon</math>-decreasing</b> repulsing supermartingale <small>[Chatterjee+ POPL'17]</small>	$\Pr(\text{Reach}_C) \leq ??$	Azuma's inequality for martingale concentration
	<b>Nonnegative</b> repulsing supermartingale <small>[Steinhardt+ IJRR'12]            [Takisaka+, in preparation]</small>	$\Pr(\text{Reach}_C) \leq ??$	<b>Knaster-Tarski!</b>

# Methodology

$$\begin{array}{ccc}
 FX & \xrightarrow{F\text{beh}_c} & FZ \\
 c\uparrow & & \uparrow^{\text{final}} \\
 X & \xrightarrow{\text{beh}_c} & Z
 \end{array}
 \qquad
 \begin{array}{ccc}
 FX & \xrightarrow{Ff} & FY \\
 c\uparrow & \sqsupseteq & \uparrow^d \\
 X & \xrightarrow{f} & Y
 \end{array}$$

system behavior
simulation

**“categorical ranking function”  
&  
soundness theorem**

**generalization**

**concretization**

**categorically  
generalized system**

**ranking function  
&  
soundness theorem**

**“probabilistic  
ranking  
function”?**

**nondeterministic  
system**

**probabilistic  
automaton**

# Categorical Ranking Function

**Def:**

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

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

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

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

$$\begin{array}{ccccc}
 FX & \xrightarrow{\quad} & FR & \xrightarrow{\quad} & F\Omega \\
 \uparrow c & & \downarrow r & & \downarrow \sigma \\
 & \xrightarrow{Fb} & & \xrightarrow{Fq} & \\
 & \sqcup & & \sqsubseteq & \\
 X & \xrightarrow{b} & R & \xrightarrow{q} & \Omega
 \end{array}$$

47

# Corecursive Algebra

**Def:**

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

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

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



# Scaled Multiplicative Ranking Supermartingale

**Def:**

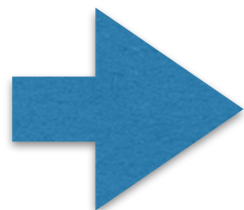
For  $\gamma \in (0, 1)$ , a function  $b : X \rightarrow [0, 1]$  is a  $\gamma$ -scaled multiplicative ranking supermartingale if:

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

By soundness of (categorical) ranking arrows,

**Thm:**

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



**Quantitative reasoning**

# Some Afterthoughts...

- \* LP characterization of reachability probabilities (e.g. [Baier & Katoen])
  - \* Minimize  $\mathbf{x}$
  - \* subject to  $\mathbf{x} = \mathbf{Ax} + \mathbf{b}$
  - \* Here  $\mathbf{A}$  is the transition matrix, and  $\mathbf{b}$  is the membership of  $\mathbf{C}$
- \* Our scaled multiplicative ranking supermartingale
  - \* Scale the constraint to  $\mathbf{x} = \gamma(\mathbf{Ax} + \mathbf{b})$  with  $0 < \gamma < 1$ 
    - Makes the solution  $\mathbf{x}_0$  **unique**. It is an lfp and a **gfp**
  - \* Once we find  $\mathbf{x}$  such that  $\mathbf{x} \preceq \gamma(\mathbf{Ax} + \mathbf{b})$ , we have  $\mathbf{x} \preceq \mathbf{x}_0$  by Knaster-Tarski
- \* (Still the categorical axiomatics gives a nice clue, I believe)

# Methodology

$$\begin{array}{ccc}
 FX & \xrightarrow{F\text{beh}_c} & FZ \\
 c\uparrow & & \uparrow^{\text{final}} \\
 X & \xrightarrow{\text{beh}_c} & Z
 \end{array}
 \qquad
 \begin{array}{ccc}
 FX & \xrightarrow{Ff} & FY \\
 c\uparrow & \sqsupseteq & \uparrow^d \\
 X & \xrightarrow{f} & Y
 \end{array}$$

system behavior
simulation

**“categorical ranking function”  
&  
soundness theorem**

**generalization**

**concretization**

**categorically  
generalized system**

**ranking function  
&  
soundness theorem**

**“probabilistic  
ranking  
function”?**

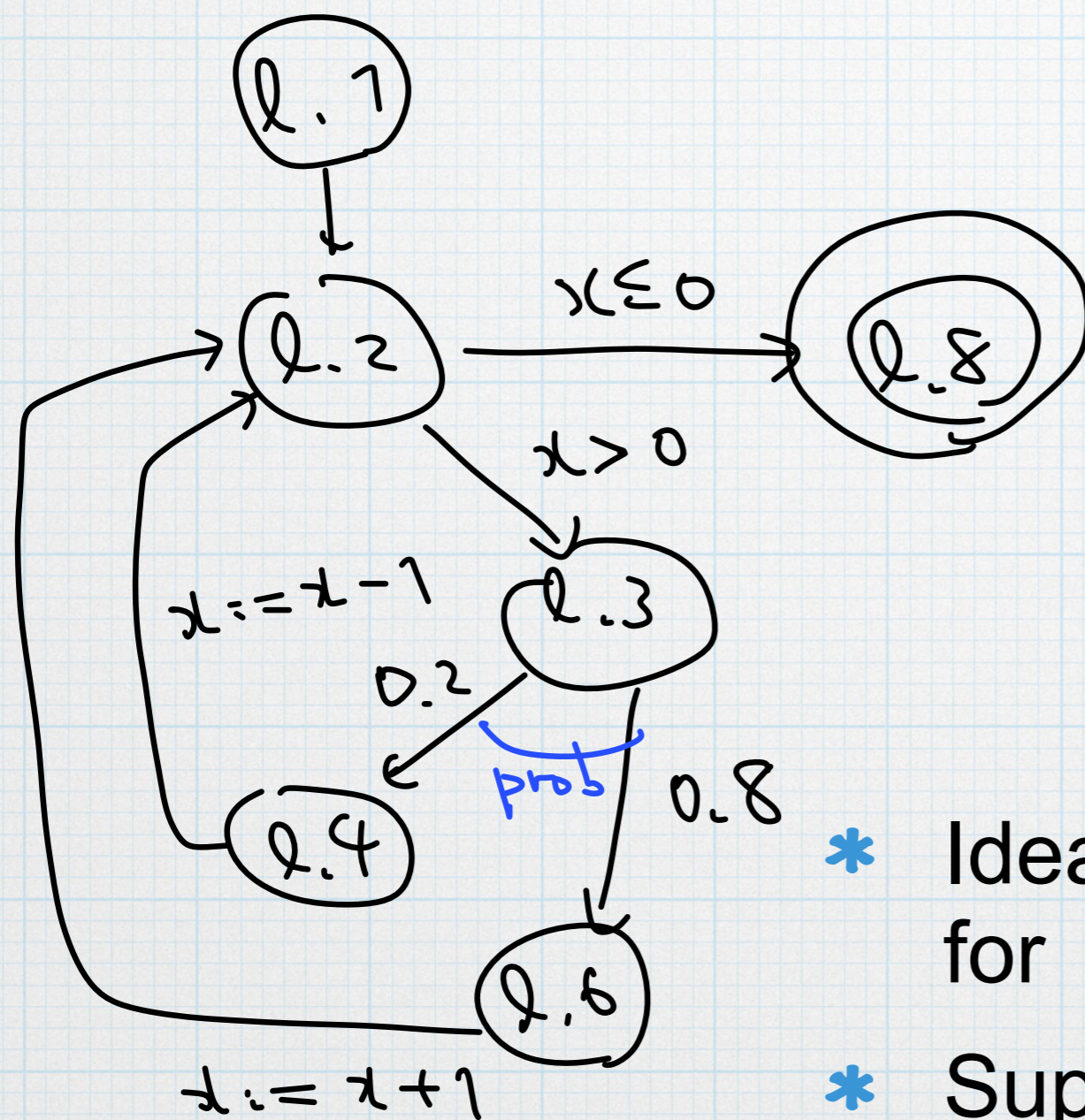
**nondeterministic  
system**

**probabilistic  
automaton**

# Overview

- \* Reachability in **probabilistic programs**
  - \* Need of “parameters”
- \* **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)
- \* Automated Synthesis

# 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  $\eta_l : \mathbb{R}^{\{x\}} \rightarrow \mathbb{R}, \quad i = 1, \dots, 8$

# Template-Based Synthesis

\* Let's use linear templates, for example

\* Meaning:  $\eta_l : \mathbb{R}\{x\} \rightarrow \mathbb{R}, \quad i = 1, \dots, 8$   
 $\eta_l(r) \equiv a_l r + b_l$

\*  $a_l, b_l$ : undetermined parameters

\* They are determined so that supermartingale constraints are satisfied, e.g.

\* Constraint solving  
by LP, SDP, QE,  
...

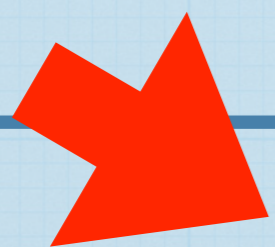
## Def.

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

$\eta : S \rightarrow \mathbb{R}_{\geq 0}$  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
<b>ranking</b> supermartingale ( <b>lower</b> bd)	<b>Additive</b> ranking supermartingale <small>[McIver+ PSSE'04] [Chakarov+ CAV'13]</small>	$\Pr(\text{Reach}_C) \stackrel{?}{=} 1$ $\text{Exp}(\text{Steps}_C) \leq ??$	(elementary)
	<b>Multiplicative</b> ranking supermartingale <small>[Urabe+ LICS'17]</small>	$\Pr(\text{Reach}_C) \geq ??$	<ul style="list-style-type: none"> <li>LP characterization</li> <li>(Categorical consideration)</li> </ul>
<b>repulsing</b> supermartingale ( <b>upper</b> bd)	<b><math>\epsilon</math>-decreasing</b> repulsing supermartingale <small>[Chatterjee+ POPL'17]</small>	$\Pr(\text{Reach}_C) \leq ??$	Azuma's inequality for martingale concentration
	<b>Nonnegative</b> repulsing supermartingale <small>[Steinhardt+ IJRR'12]            [Takisaka+, in preparation]</small>	$\Pr(\text{Reach}_C) \leq ??$	Markov's inequality for martingale concentration



# Preliminary Experimental Results

```
1   $x := m$ 
2  while  $x > 0$  do
3    if  $x < N$  do
4      if  $\text{prob}(p)$  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   $x := \text{Geometric}(0.5)$ 
2  while  $x \geq 1$  do
3     $x := x - 1$ 
4  od
5  if  $\text{prob}(0.5)$  do
6    while  $x \leq 0$  do
7       $x := x - 1$ 
8    od
9  else
10   skip
11 od
```

Fig. 2. APP corresponding to Example 2

```
1   $x := \text{Uniform}[0, 1]$ 
2  while  $x < 1$  do
3    if  $\text{prob}(p)$  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  $\text{prob}(p)$  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)	$\epsilon$ -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	$\int_0^1 \left(\frac{0.25}{0.75}\right)^{\lceil \log_2(1/x) \rceil} dx \approx 0.2$	0.5	—
4	$\left(\frac{0.25}{0.75}\right)^1 \approx 0.333333$	—	< 1

# Summary

- \* Reachability in probabilistic programs is **rich**
- \* **Martingale** methods for (over-/under-) approximations
  - \* Role of **concentration lemmas**
  - \* Knaster-Tarski foundation is still useful
- \* Automated synthesis by constraint solving, numeric optimization
- \* Also showcased use of categorical/coalgebraic methods

**We're hiring!**

Max 4 yrs, PD & senior researchers  
logic + automata + categories +  
machine learning + SE → CPS

**Thank you for your attention!**

Ichiro Hasuo (NII, Tokyo)

<http://group-mmm.org/~ichiro/>