Ranking and Repulsing Supermartingales for Reachability in Probabilistic Programs

Toru Takisaka[1], Yuichiro Oyabu[2,3], Natsuki Urabe[1], Ichiro Hasuo[2,3]

National Institute of Informatics, Japan[1]

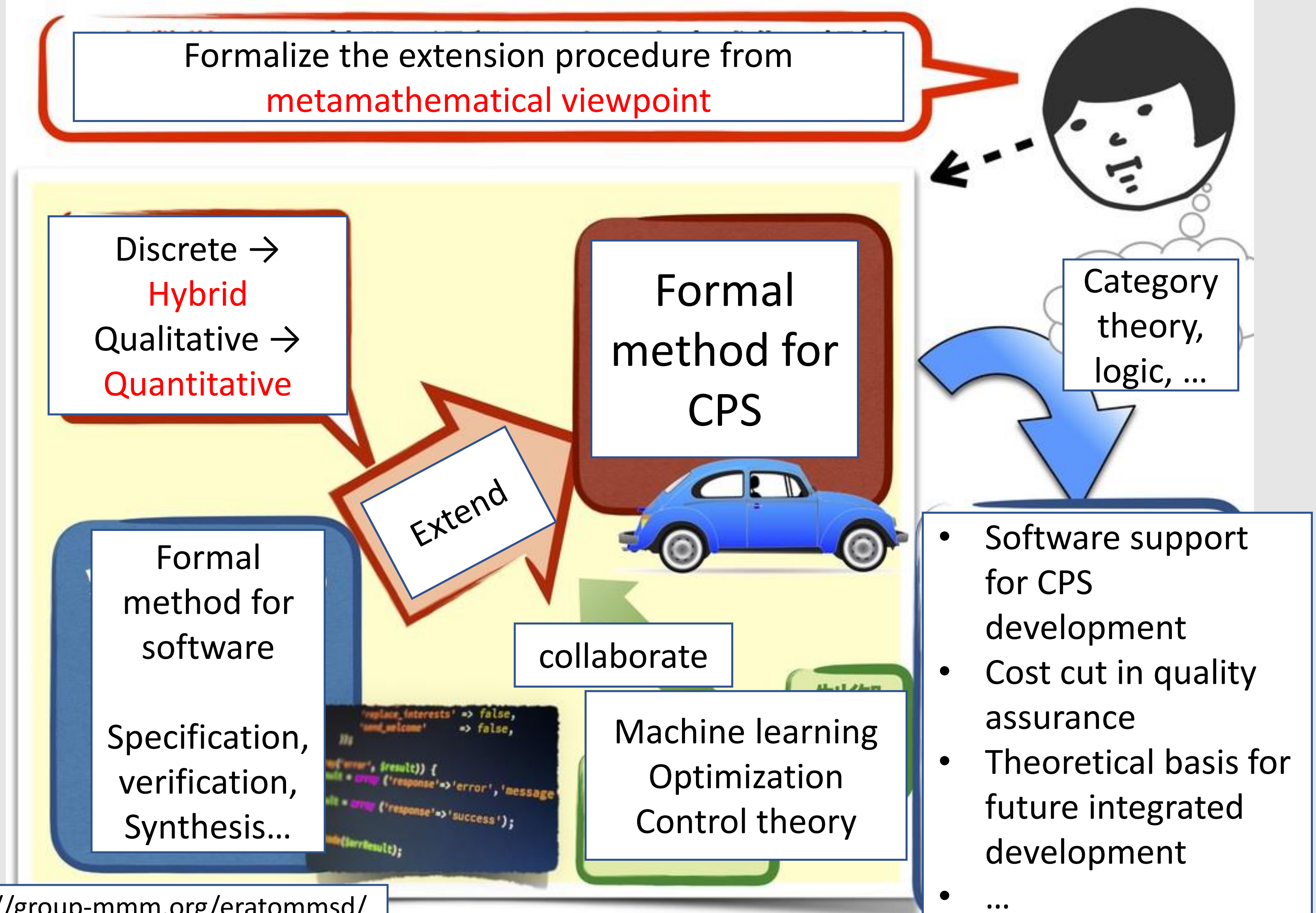
The Graduate University for Advanced Studies (SOKENDAI), Japan[2]

University of Tokyo, Japan[3]

ERATO 蓮尾メタ数理システムデザインプロジェクト

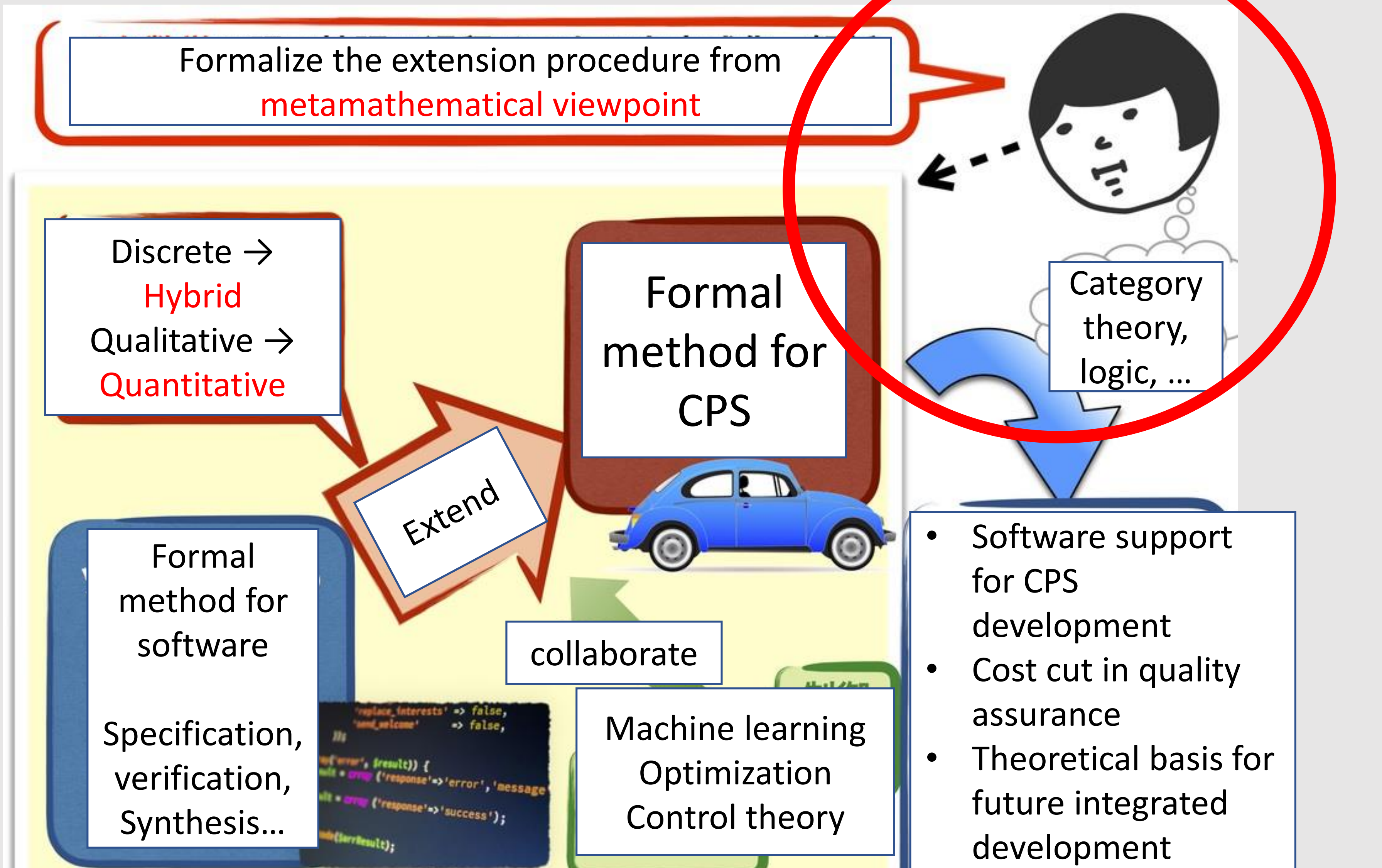
ERATO Metamathematics for Systems Design Project

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



https://group-mmm.org/eratommsd/

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



https://group-mmm.org/eratommsd/

Outline

- Introduction / preliminaries
  - Our topic: supermartingale for reachability analysis
  - What can supermartingale do?
  - What is supermartingale? / Why does it work?
  - Which property of SM techniques are we interested? - Soundness / completeness

- Our contribution
  - Theoretical part: characterization of SM techniques via KT theorem
  - Implementation and experiments

Problem formulation

Input: probabilistic program

```
x := 15; t := 0;
while x > 0 do
  if * then
    t := t + 2;
    x := x - 1
  else
   t := t + 1;
   p := Bernoulli(0.9);
   x := x - p
  fi
assert (t <= 20)
```

Problem formulation

Input: probabilistic program

```
x := 15; t := 0;
while x > 0 do
  if * then
    t := t + 2;
    x := x - 1
  else
    t := t + 1;
    p := Bernoulli(0.9);
    x := x - p
  fi
assert (t <= 20)
```

Nondet. / Prob. branching

Nondet. / Prob. assignment

Problem formulation

Input: probabilistic program

```
x := 15; t := 0;
while x > 0 do
  if * then
    t := t + 2;
    x := x − 1
  else
    t := t + 1;
    p := Bernoulli(0.9);
    x := x − p
  fi
assert (t <= 20)
```

Nondet. / Prob. branching

Nondet. / Prob. assignment

Problem

What is the probability that the program terminates?

(under angelic/demonic scheduler)

We admit continuous variables

⇒ Generally one can't compute probability efficiently

Problem formulation

Input: probabilistic program

```
x := 15; t := 0;
while x > 0 do
  if * then
    t := t + 2;
    x := x − 1
  else
    t := t + 1;
    p := Bernoulli(0.9);
    x := x − p
  fi
assert (t <= 20)
```

Nondet. / Prob. branching

Nondet. / Prob. assignment

Problem

What is the probability that the program terminates?

(under angelic/demonic scheduler)

We admit continuous variables

⇒ Generally one can't compute probability efficiently

⇒ Reachability analysis by supermartingale

Outline

- Introduction / preliminaries
  - Our topic: supermartingale for reachability analysis
  - What can supermartingale do?
  - What is supermartingale? / Why does it work?
  - Which property of SM techniques are we interested? - Soundness / completeness

- Our contribution
  - Theoretical part: characterization of SM techniques via KT theorem
  - Implementation and experiments

Ranking supermartingale for a.s. termination (Chakarov-Sankaranarayanan, CAV'13 etc.)

Probabilistic modification of real-world benchmarks
(in Alias+, SAS'10)

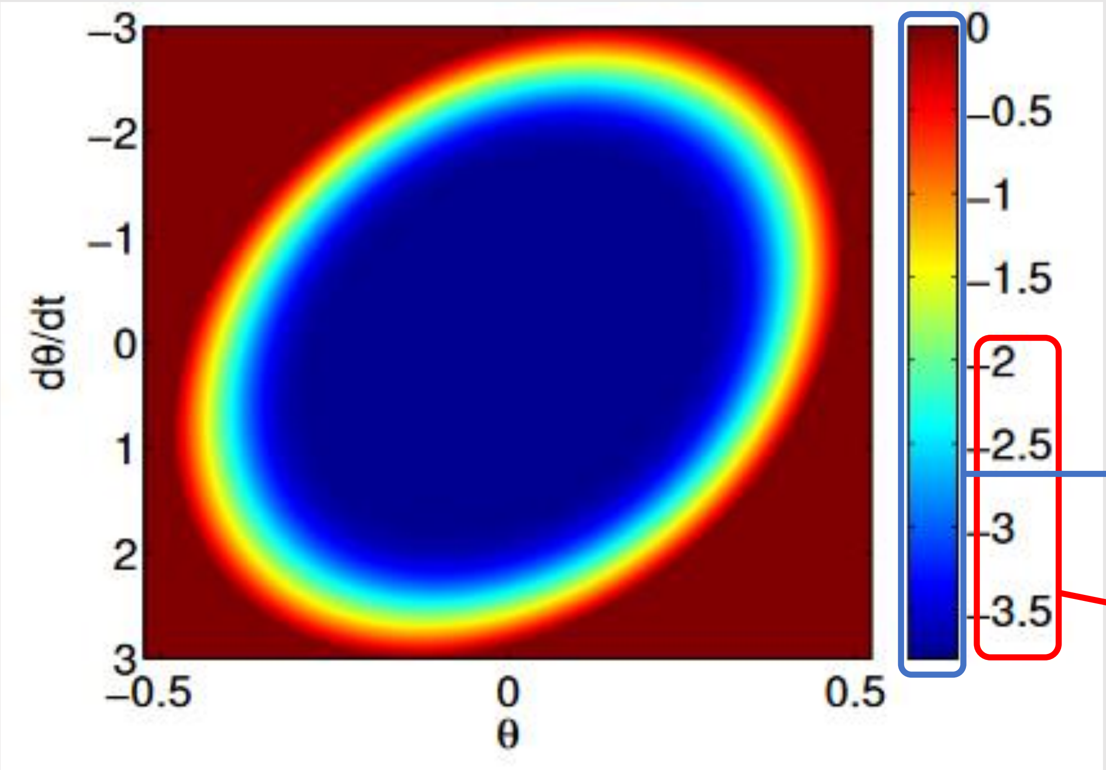
A.s. termination is certified in 20/28 examples

Benchmark	Time (s)	Solution	Dimension	Prob. loops	Prob. Assignments
alain	0.11	yes	2	yes	yes
catmouse	0.08	yes	2	yes	yes
counterex1a	0.1	no		no	no
counterex1c	0.11	yes	3	yes	yes
easy1	0.09	yes	1	yes	yes
exmini	0.09	yes	2	yes	yes
insertsort	0.1	yes	3	yes	yes
ndecr	0.09	yes	2	yes	yes
perfect	0.11	yes	3	yes	yes
perfect2	0.1	yes	3	yes	no
	0.11	no		yes	yes
real2	0.09	no		no	no
realbubble	0.22	yes	3	yes	yes
realselect	0.11	yes	3	yes	yes
realshellsort	0.09	no		yes	no
serpent	0.1	yes	1	yes	yes
sipmabubble	0.1	yes	3	yes	yes
speedDis2	0.09	no		no	no
speedNestedMultiple	0.1	yes	3	yes	yes
speedpldi2	0.09	yes	2	yes	yes
speedpldi4	0.09	yes	3	yes	yes
speedSimpleMultipleDep	0.09	no		no	no
speedSingleSingle2	0.12	yes	2	yes	no
	0.1	no		yes	yes
unperfect	0.1	yes	2	yes	no
	0.16	no		yes	yes
wcet1	0.11	yes	2	yes	yes
while2	0.1	yes	3	yes	yes

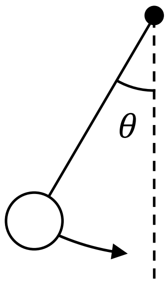
(Agrawal+, POPL'18)

Repulsing supermartingale for lower bound of safety probability

(Steinhardt-Tedrake, IJRR'12; Chatterjee+, POPL'17 etc.)



System: pendulum + noise



Failure ⇔

$\theta > \pi/6$ at time $t \leq$ 1hour

The log-base-10 of the failure probability

>99% safety is guaranteed

(Pr(failure) <1%)

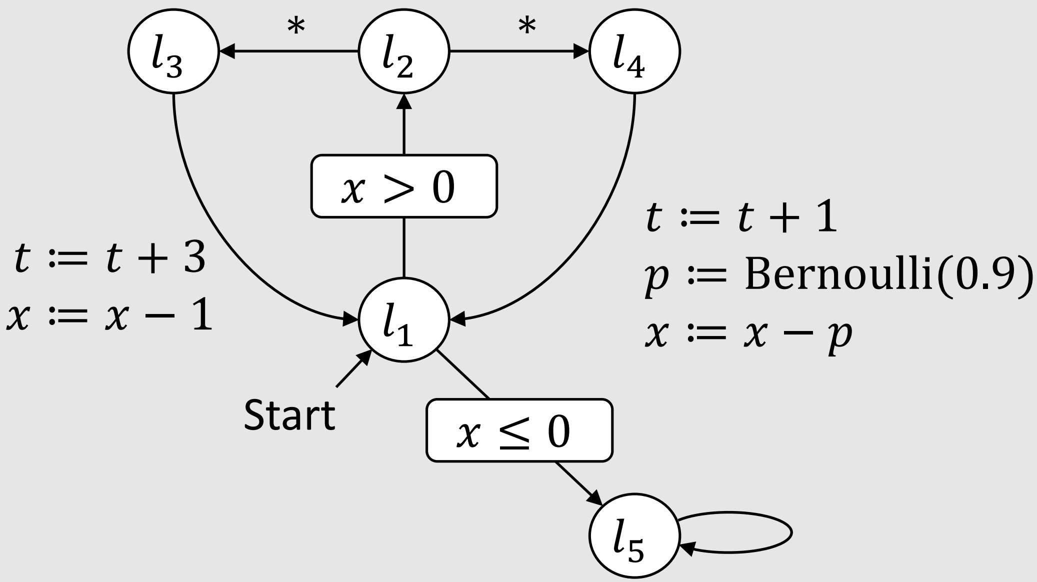
(Steinhardt-Tedrake, IJRR'12)

Outline

- Introduction / preliminaries
  - Our topic: supermartingale for reachability analysis
  - What can supermartingale do?
  - What is supermartingale? / Why does it work?
  - Which property of SM techniques are we interested? - Soundness / completeness
- Our contribution
  - Theoretical part: characterization of SM techniques via KT theorem
  - Implementation and experiments

Semantics: Control flow graph

(Agrawal+, POPL'18 etc.)




```
x := 15; t := 0;
while x > 0 do
  if * then
    t := t + 2;
    x := x - 1
  else
    t := t + 1;
    p := Bernoulli(0.9);
    x := x - p
  fi
assert (t <= 20)
```

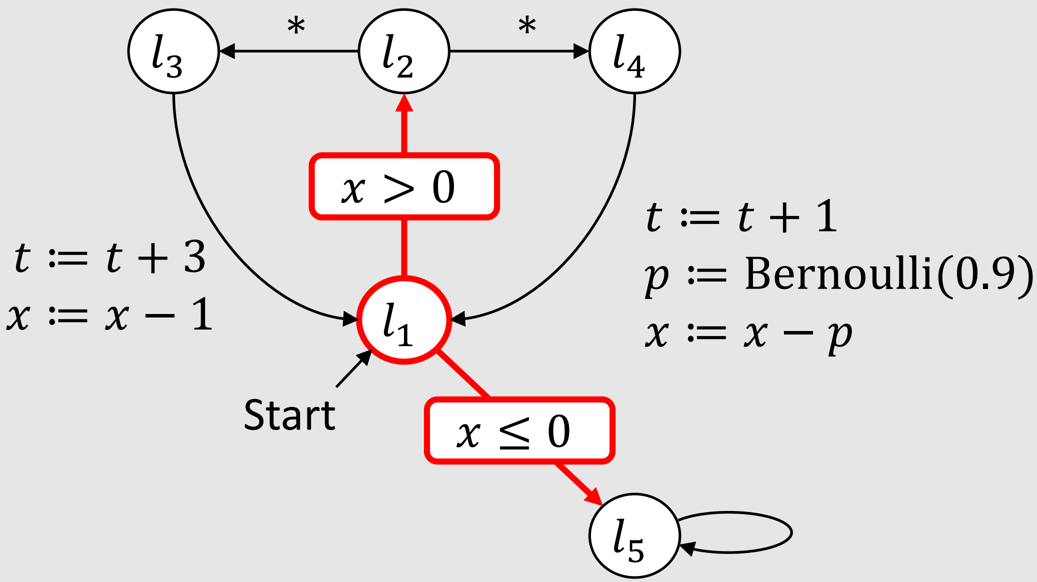
- A state is a pair (program location, memory state)
- Nondet. / prob. branching

finite

$\mathbb{R}^V$

Semantics: Control flow graph

(Agrawal+, POPL'18 etc.)




```
x := 15; t := 0;
while x > 0 do
  if * then
    t := t + 2;
    x := x - 1
  else
    t := t + 1;
    p := Bernoulli(0.9);
    x := x - p
  fi
assert (t <= 20)
```

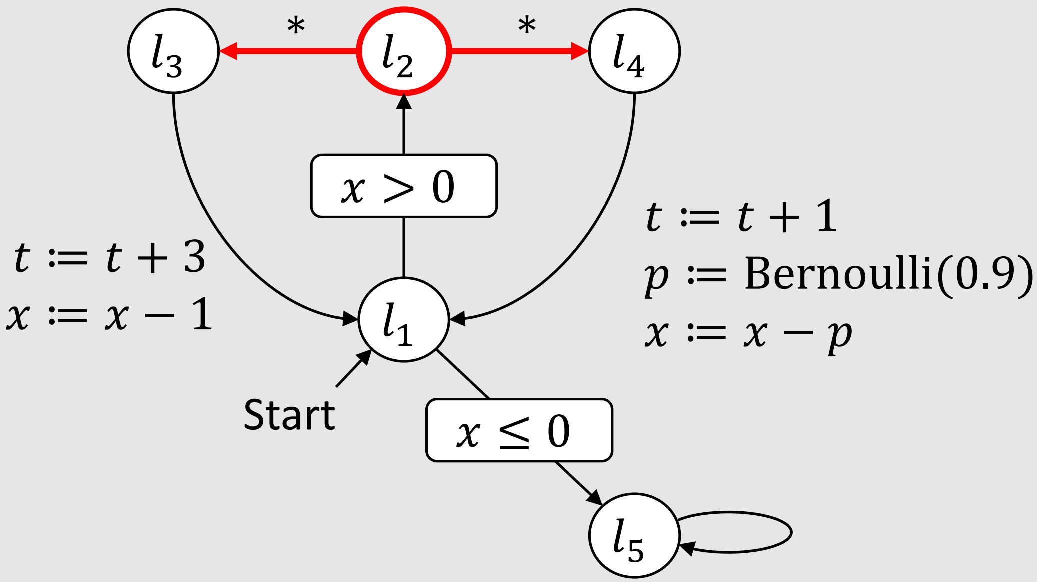
- A state is a pair (program location, memory state)
- Nondet. / prob. branching

finite

$\mathbb{R}^{V}$

Semantics: Control flow graph

(Agrawal+, POPL'18 etc.)




```
x := 15; t := 0;
while x > 0 do
  if * then
    t := t + 2;
    x := x - 1
  else
    t := t + 1;
    p := Bernoulli(0.9);
    x := x - p
  fi
assert (t <= 20)
```

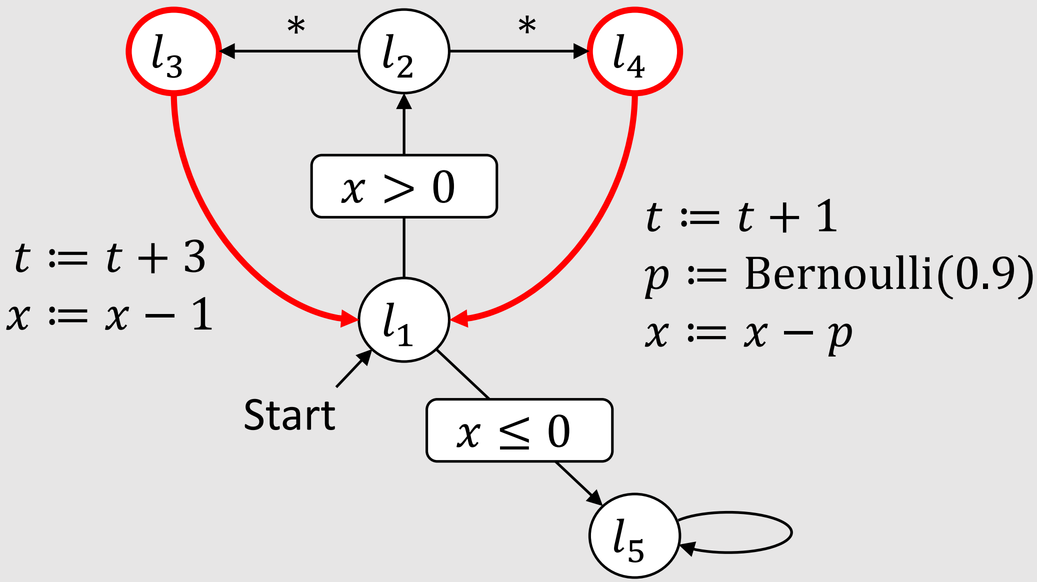
- A state is a pair (program location, memory state)
- Nondet. / prob. branching

finite

$\mathbb{R}^V$

Semantics: Control flow graph

(Agrawal+, POPL'18 etc.)




```
x := 15; t := 0;
while x > 0 do
  if * then
    t := t + 2;
    x := x − 1
  else
    t := t + 1;
    p := Bernoulli(0.9);
    x := x − p
  fi
assert (t <= 20)
```

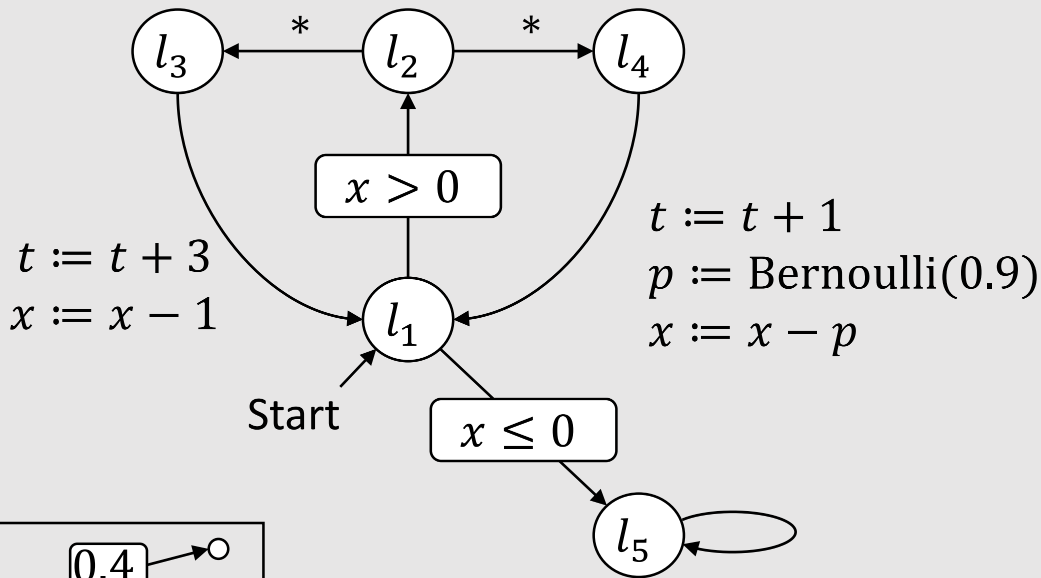
- A state is a pair (program location, memory state)
- Nondet. / prob. branching

finite

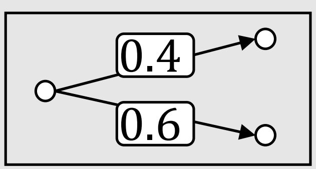
$\mathbb{R}^V$

Semantics: Control flow graph

(Agrawal+, POPL'18 etc.)




```
x := 15; t := 0;
while x > 0 do
  if * then
    t := t + 2;
    x := x - 1
  else
    t := t + 1;
    p := Bernoulli(0.9);
    x := x - p
  fi
assert (t <= 20)
```



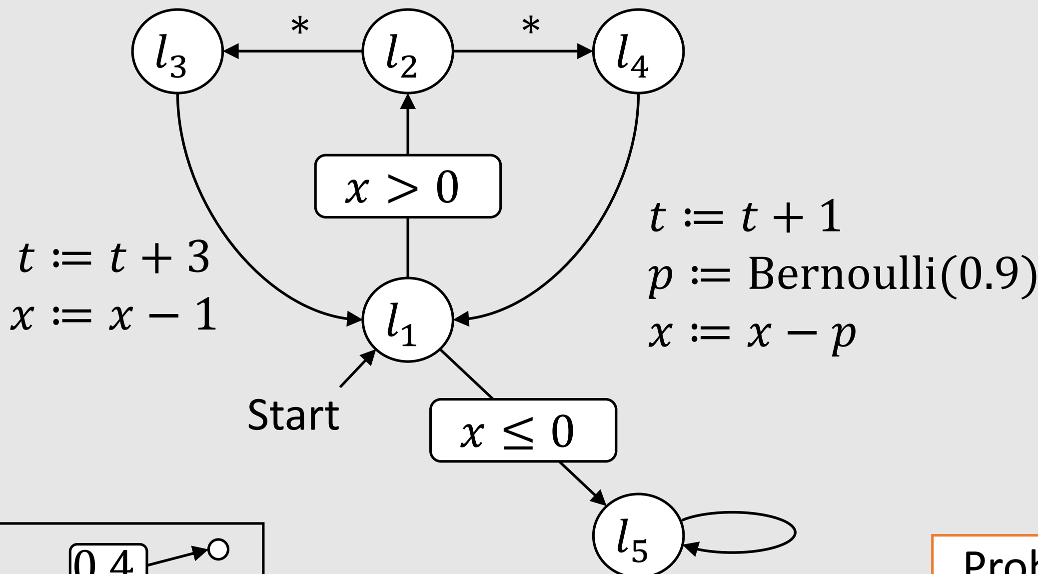
- A state is a pair (program location, memory state)
- Nondet. / prob. branching

finite

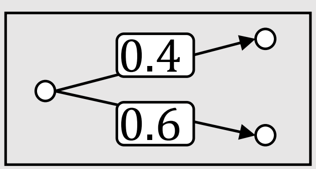
$\mathbb{R}^V$

Semantics: Control flow graph

(Agrawal+, POPL'18 etc.)




```
x := 15; t := 0;
while x > 0 do
  if * then
    t := t + 2;
    x := x - 1
  else
    t := t + 1;
    p := Bernoulli(0.9);
    x := x - p
  fi
assert (t <= 20)
```



Problem

C = (terminating states)

$= \{l_5\} \times \{(x, t, p) \mid t \leq 20\}$

⇒Pr(the system eventually visits the region C)?

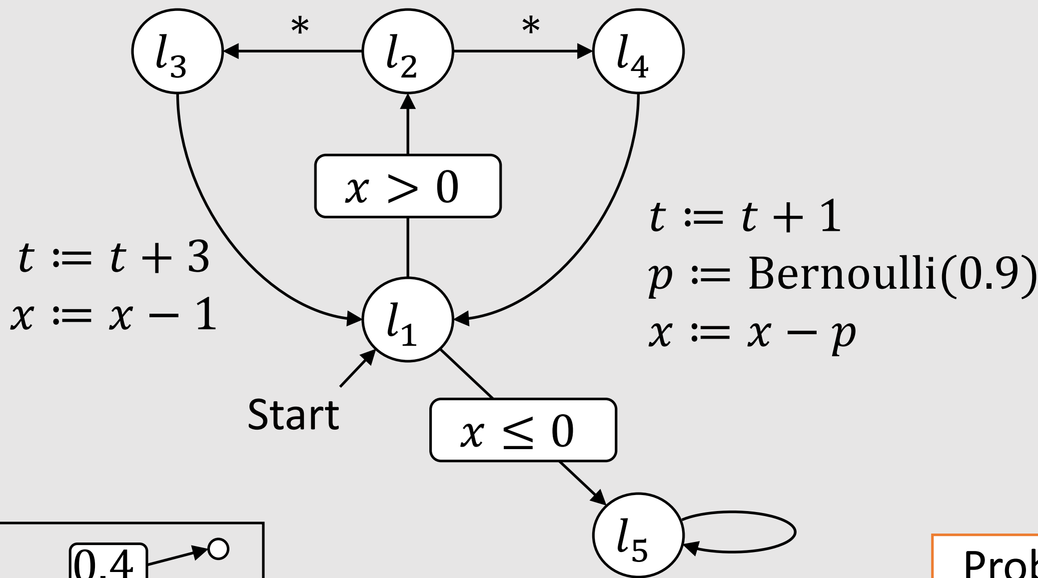
- A state is a pair (program location, memory state)
- Nondet. / prob. branching

finite

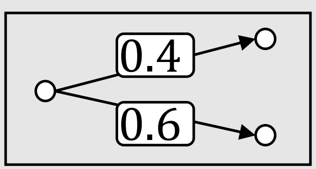
$\mathbb{R}^V$

Semantics: Control flow graph

(Agrawal+, POPL'18 etc.)




```
x := 15; t := 0;
while x > 0 do
  if * then
    t := t + 2;
    x := x - 1
  else
   t := t + 1;
   p := Bernoulli(0.9);
   x := x - p
  fi
assert (t <= 20)
```



Problem

C = (terminating states)

$= \{l_5\} \times \{(x, t, p) \mid t \leq 20\}$

$\Rightarrow$ Pr(the system ... lly visits the reg...

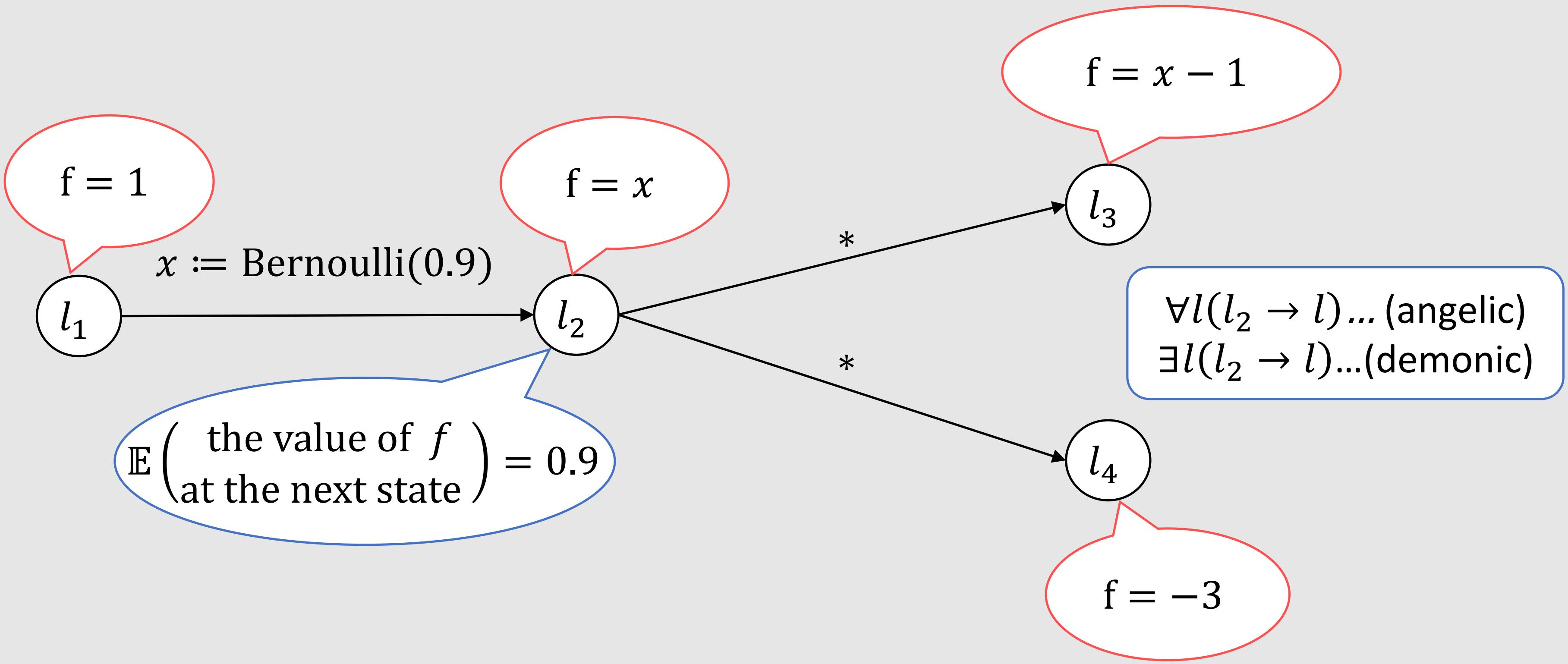
...under angelic/demonic scheduler

- A state is a pair (program location, memory state)
- Nondet. / prob. branching

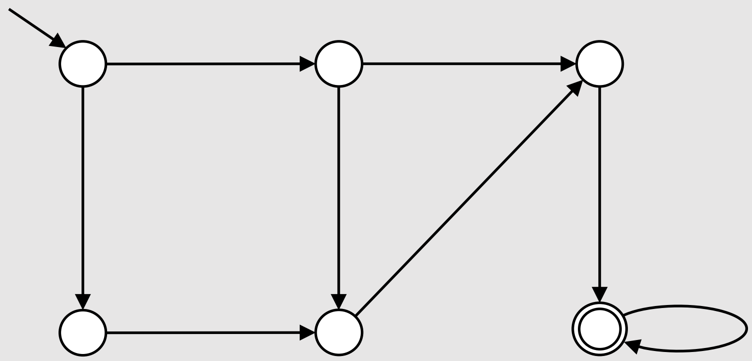
finite

$\mathbb{R}^V$

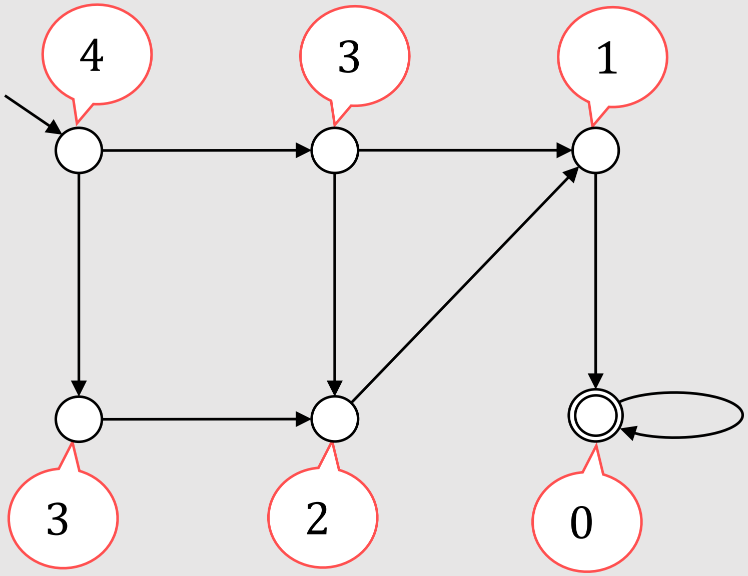
Supermartingale = a function over states that is "non-increasing" through transitions



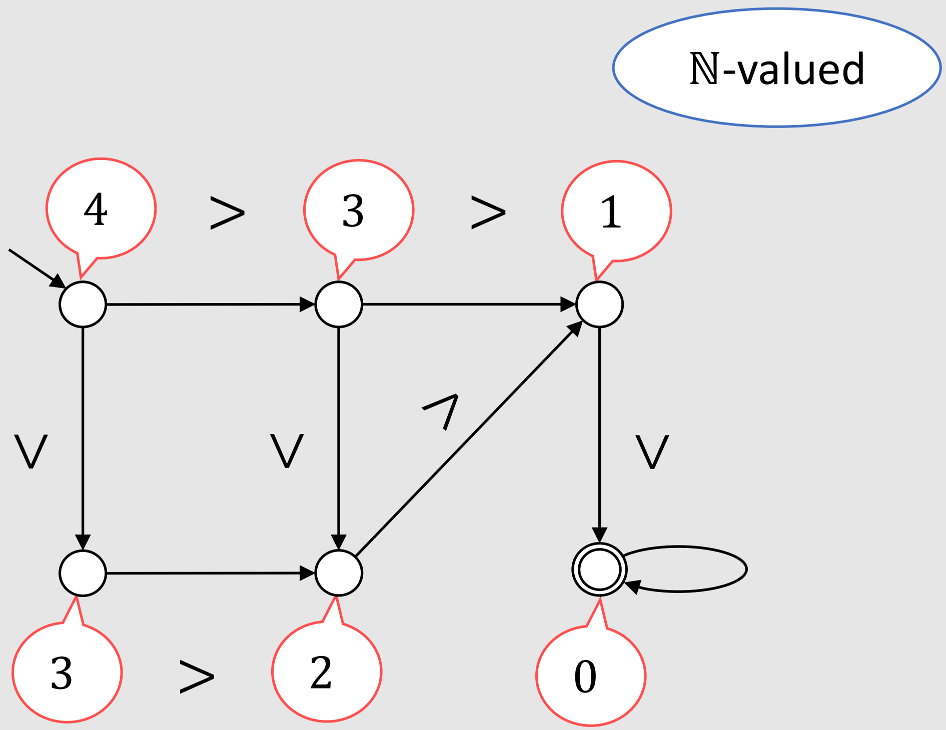
Ranking function



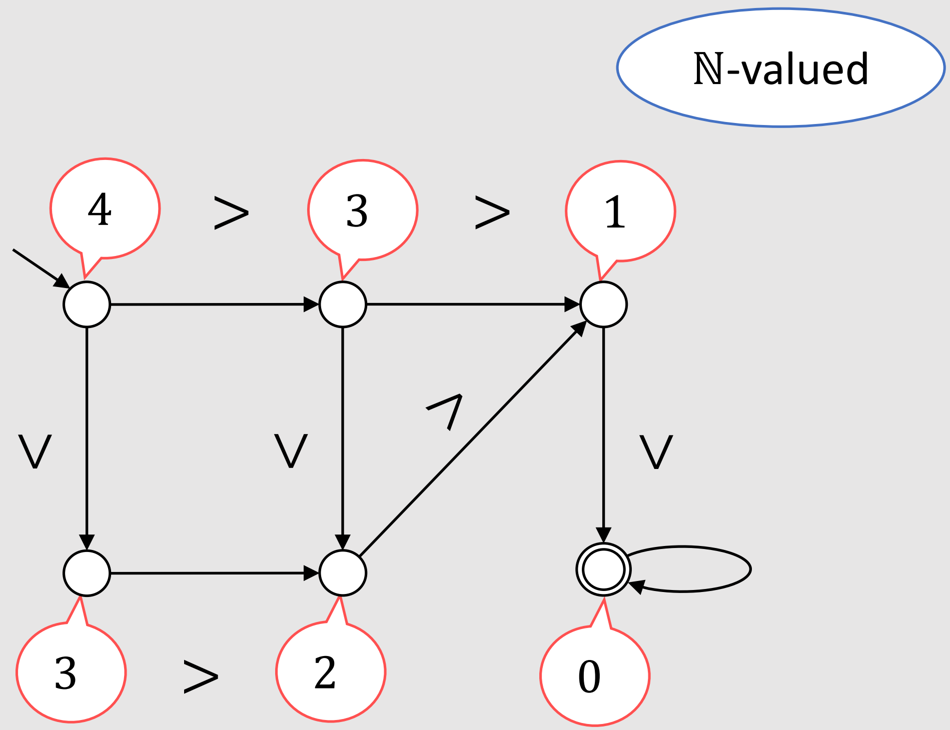
Ranking function



Ranking function

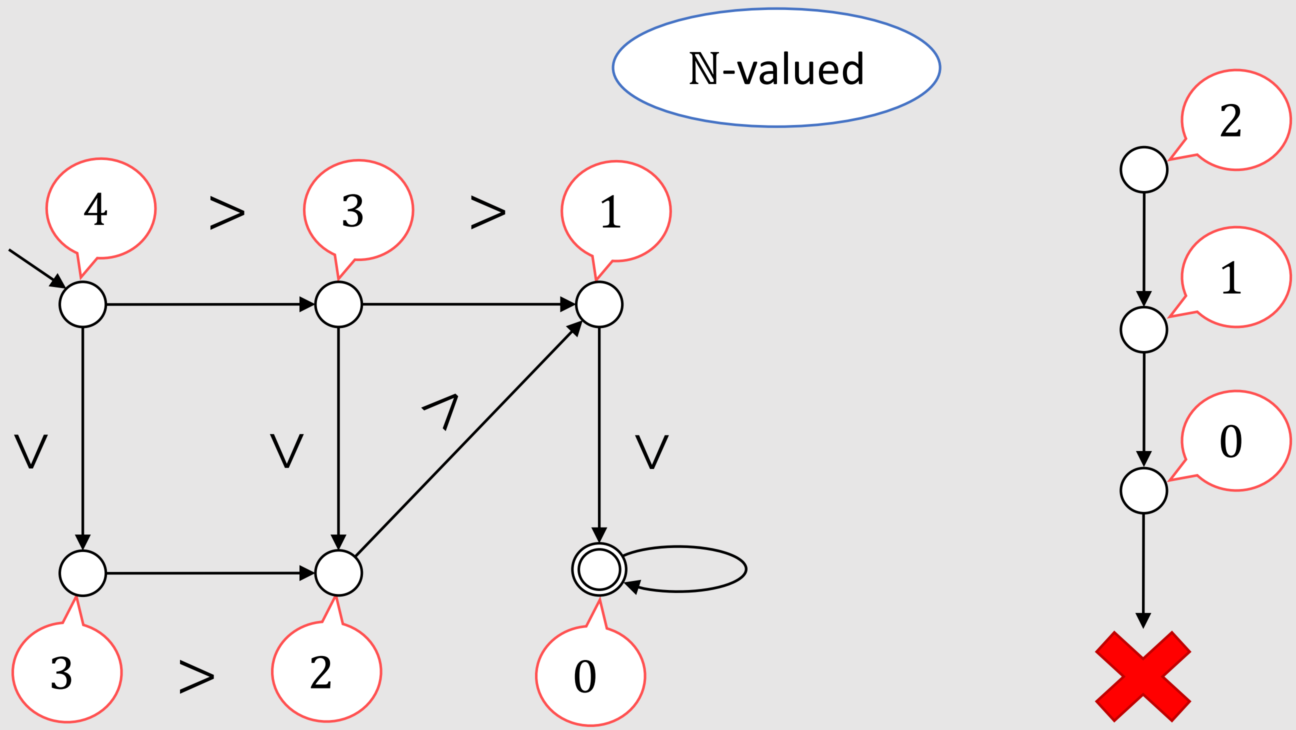


Ranking function



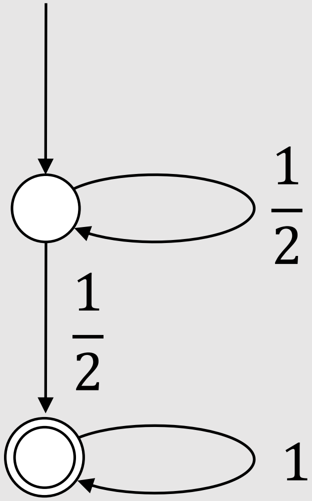
The system eventually visits ◎ (under any nondeterministic choice)

Ranking function

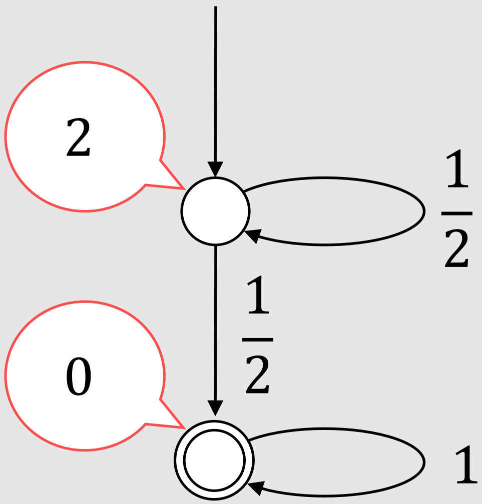


The system eventually visits ◎ (under any nondeterministic choice)

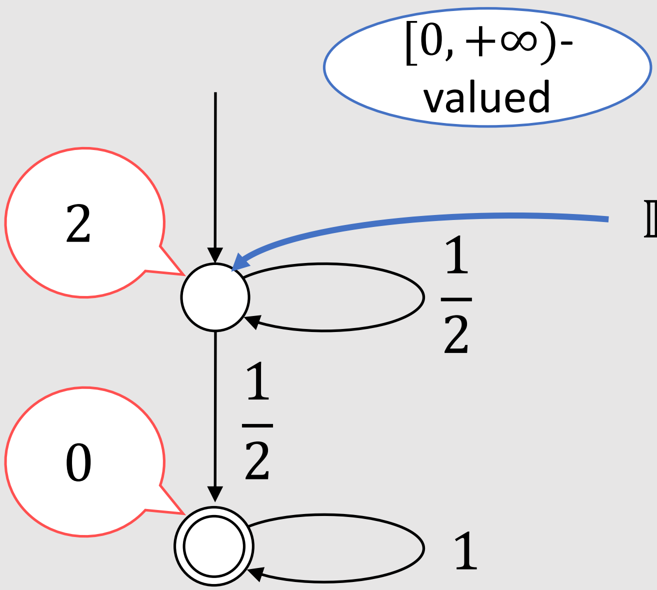
Ranking supermartingale



Ranking supermartingale

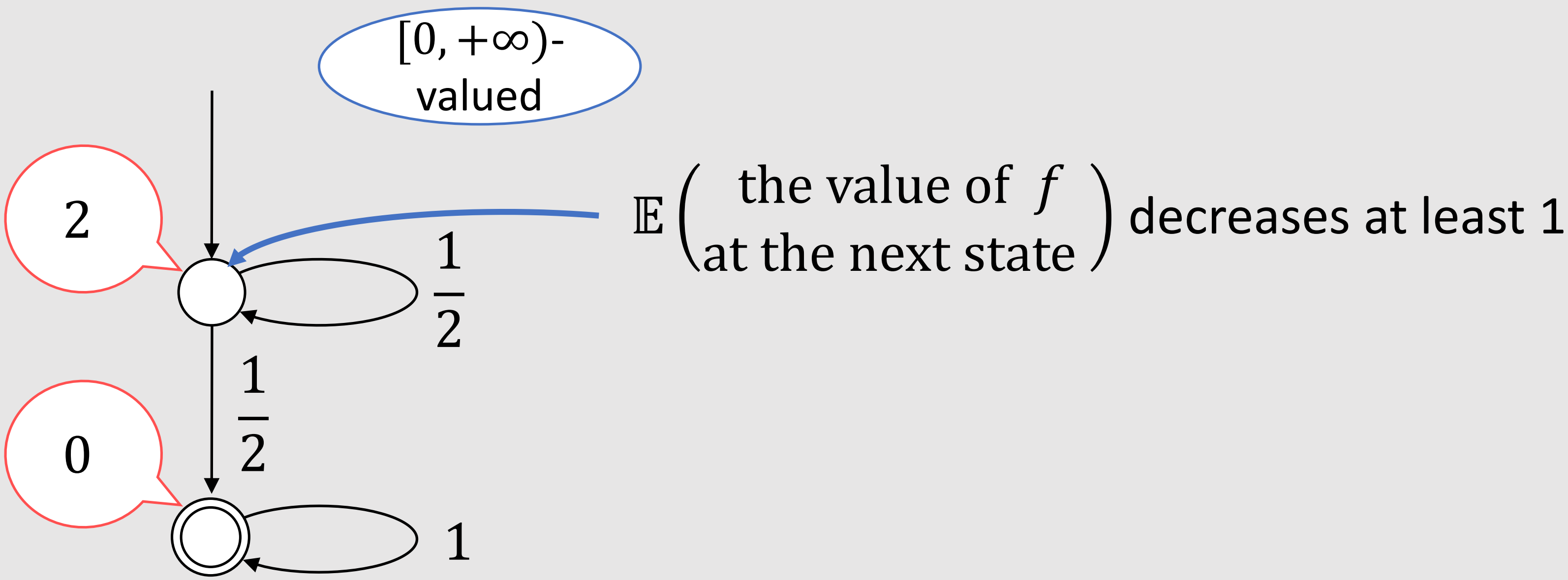


Ranking supermartingale



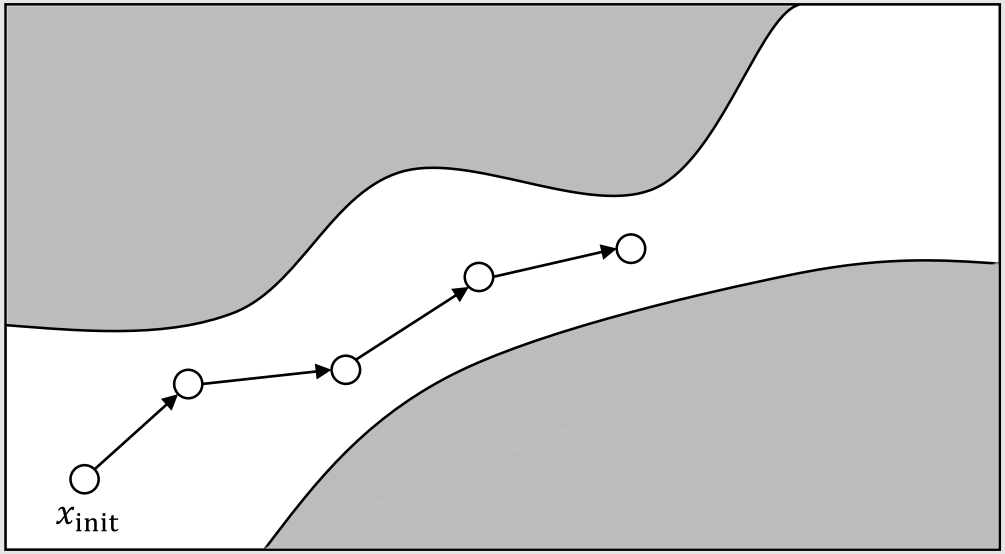
$\mathbb{E}\left(\begin{array}{c}\text{the value of } f \\ \text{at the next state}\end{array}\right)$ decreases at least 1

Ranking supermartingale



The system eventually visits ◎ almost surely

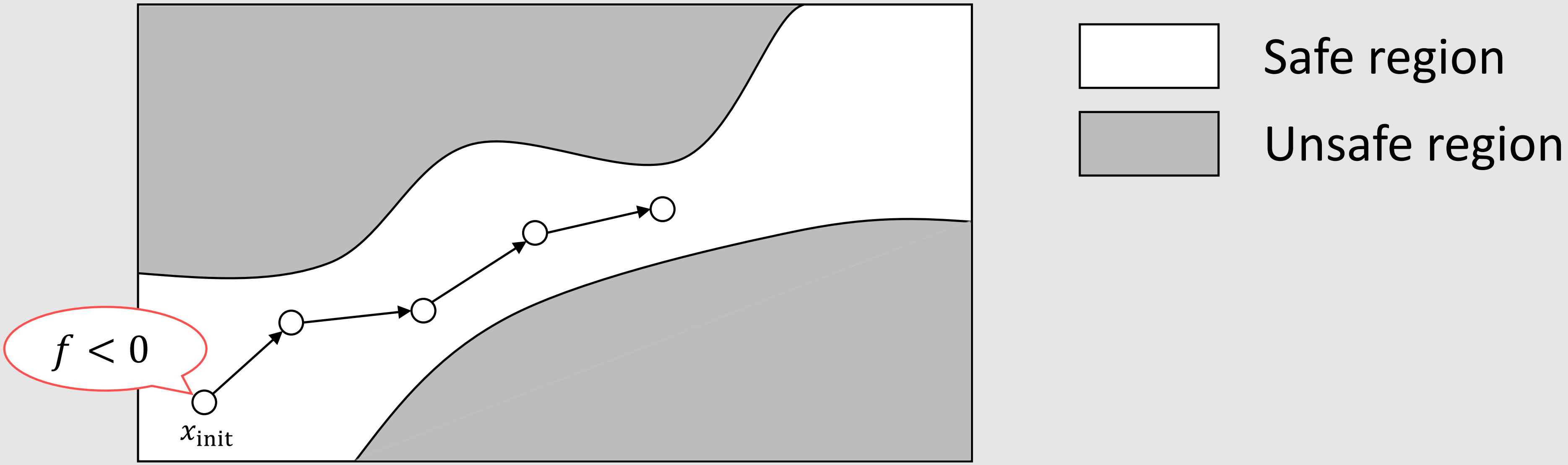
Barrier certificate



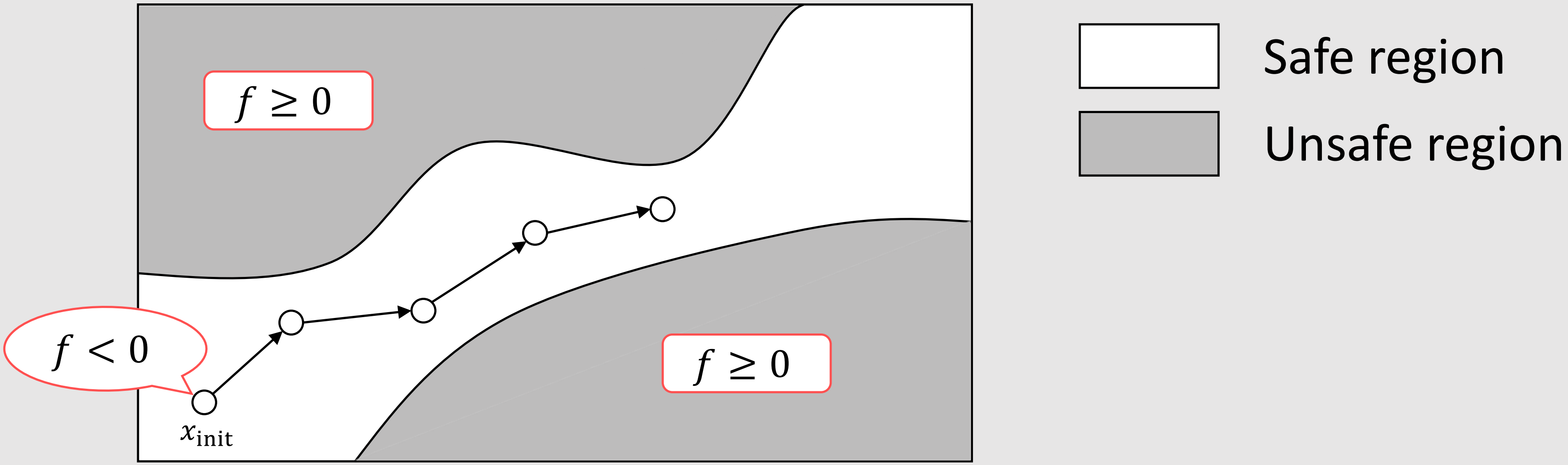
Safe region

Unsafe region

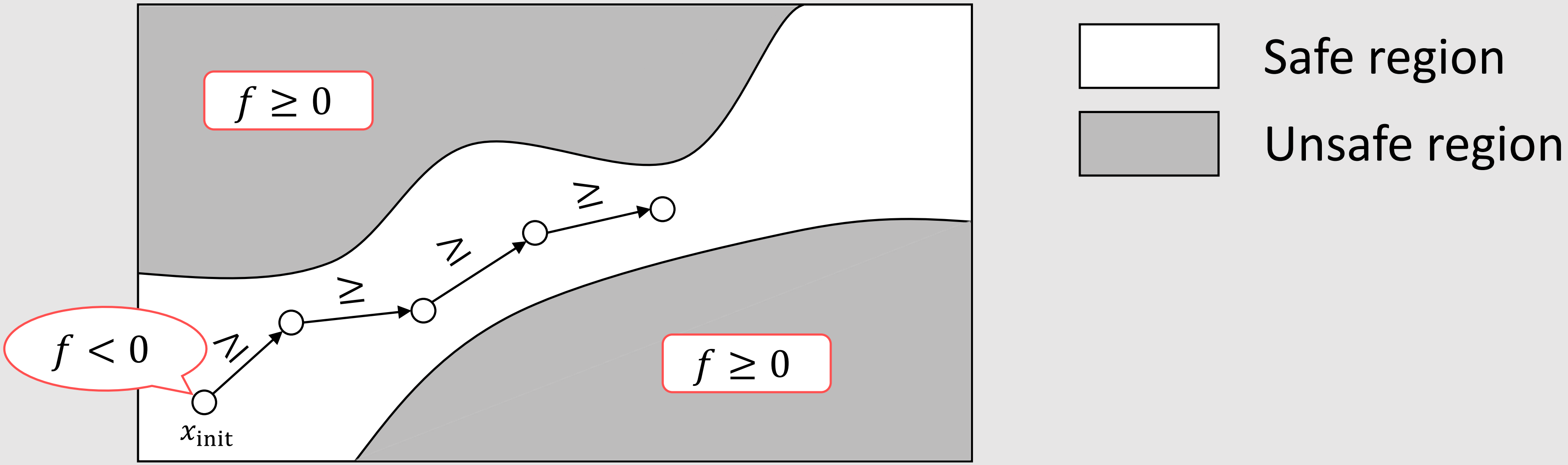
Barrier certificate



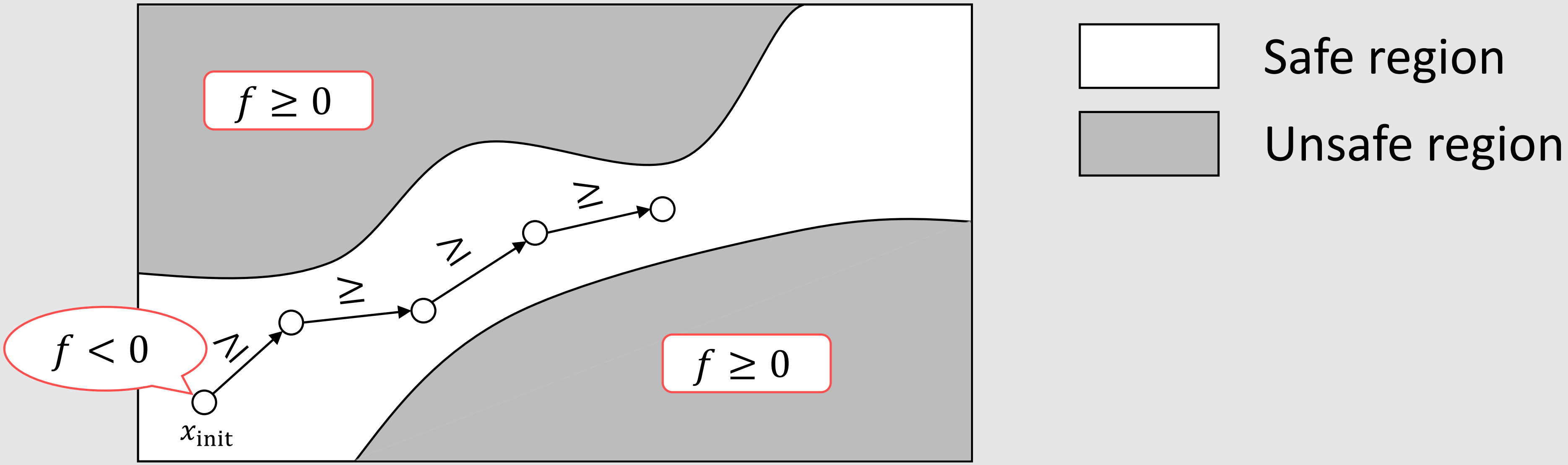
Barrier certificate



Barrier certificate

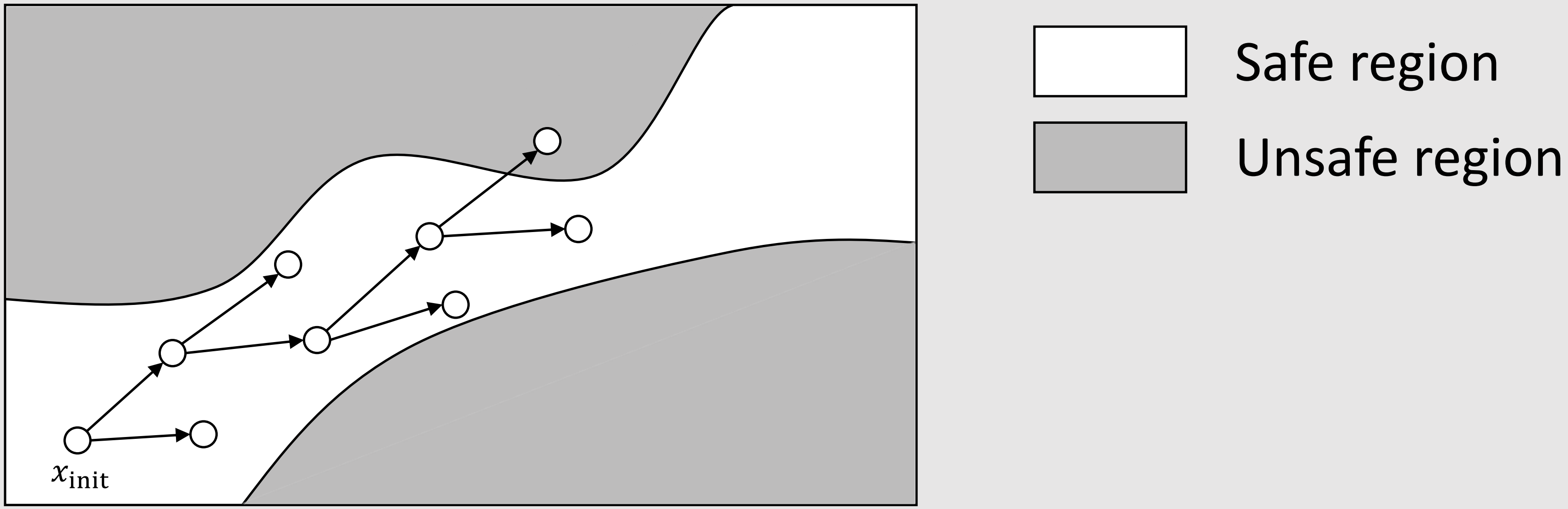


Barrier certificate

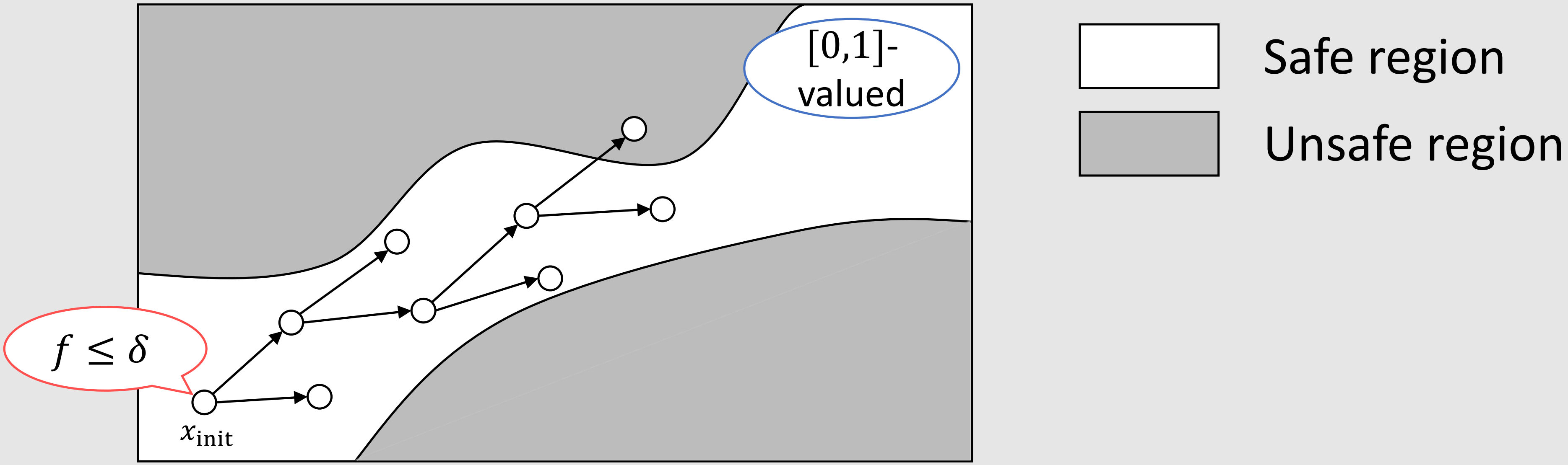


The system does not enter the unsafe region

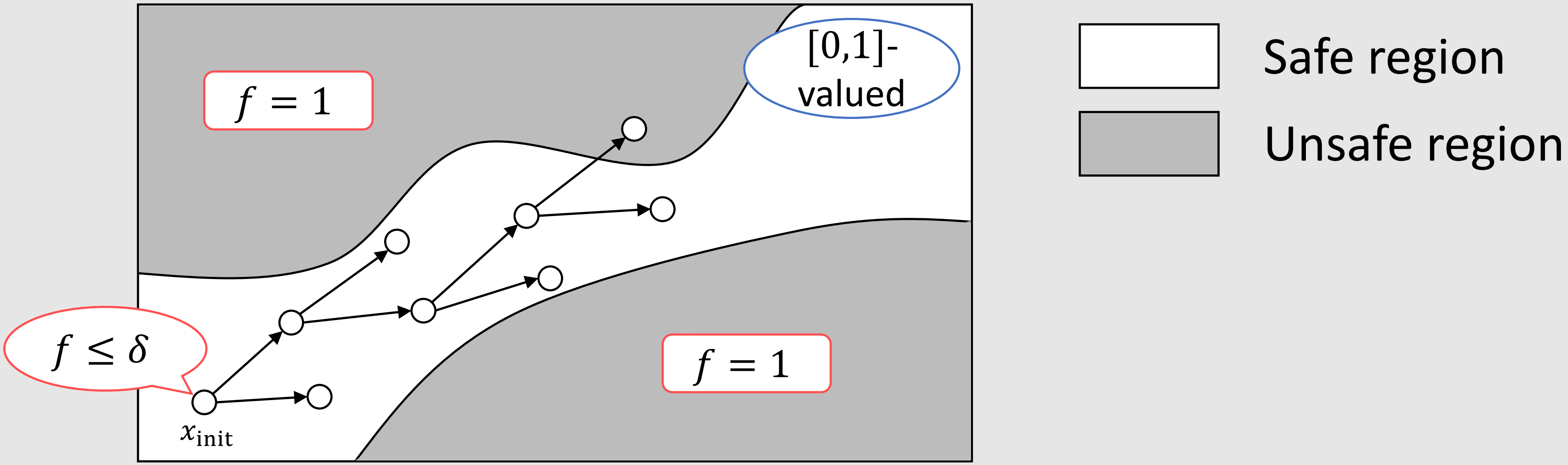
Probabilistic barrier certificate (a.k.a. nonneg. repulsing supermartingale)



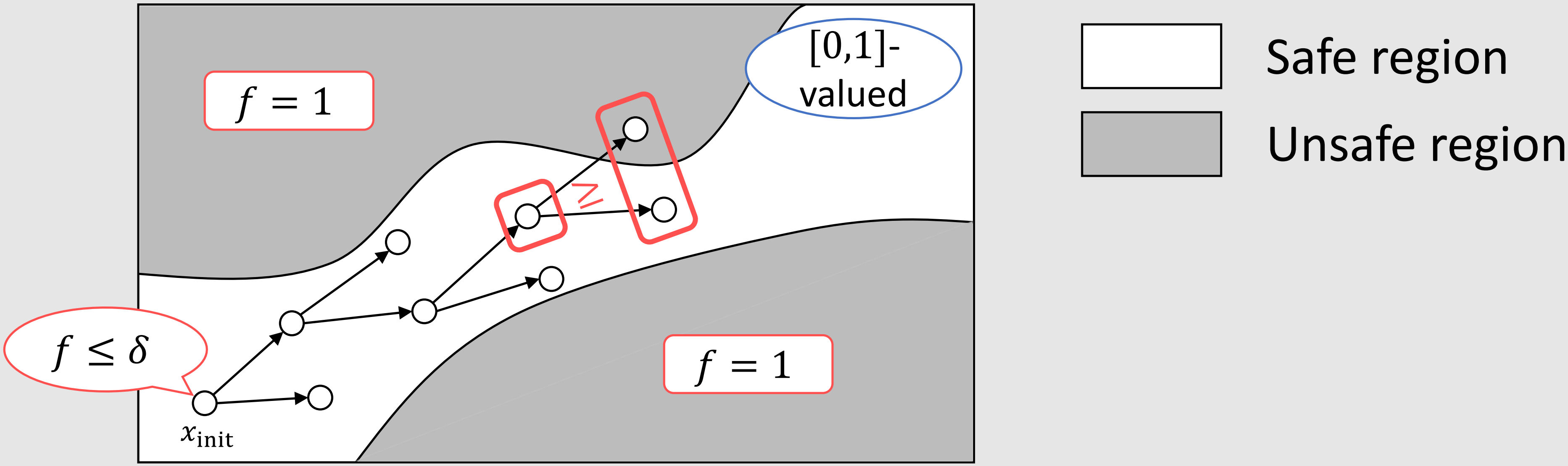
Probabilistic barrier certificate (a.k.a. nonneg. repulsing supermartingale)



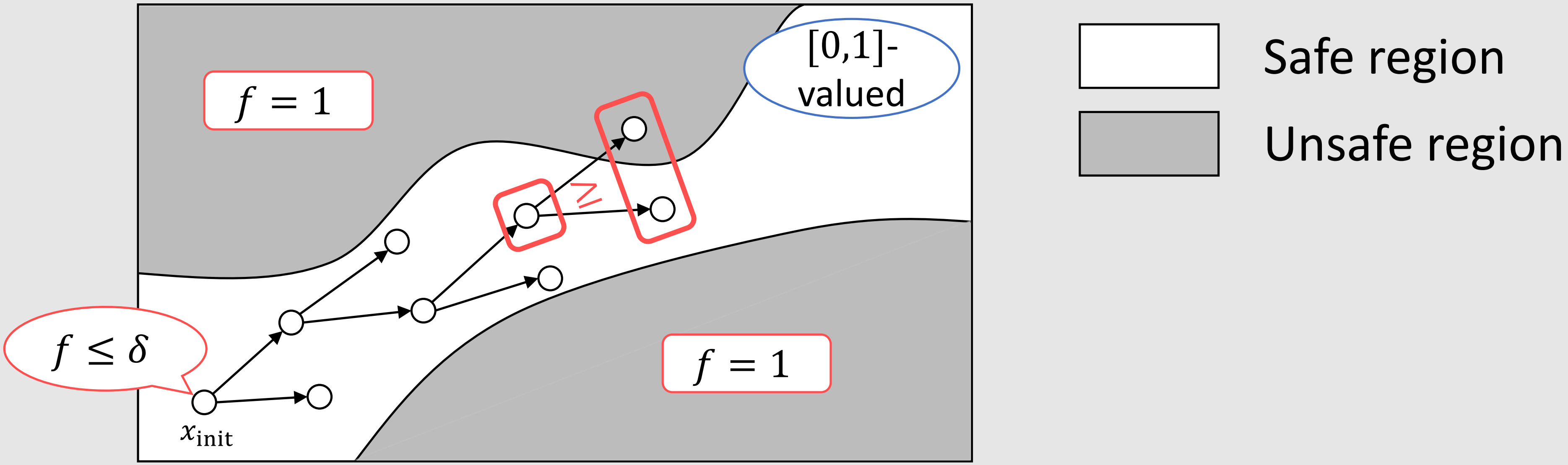
Probabilistic barrier certificate (a.k.a. nonneg. repulsing supermartingale)



Probabilistic barrier certificate (a.k.a. nonneg. repulsing supermartingale)



Probabilistic barrier certificate (a.k.a. nonneg. repulsing supermartingale)



Pr(the system enters the unsafe region) $\leq \delta$

Outline

- Introduction / preliminaries
  - Our topic: supermartingale for reachability analysis
  - What can supermartingale do?
  - What is supermartingale? / Why does it work?
  - Which property of SM techniques are we interested? - Soundness / completeness
- Our contribution
  - Theoretical part: characterization of SM techniques via KT theorem
  - Implementation and experiments

Two objective functions

- Given: a control flow graph, and a subset C of its states
- For $s \in L \times \mathbb{R}^V =$ (state space),

$$\mathbb{E}^{\text{steps}} : s \mapsto \mathbb{E}\left(\begin{array}{c}\text{the number of steps from } s \\ \text{to the region } C\end{array}\right)$$

$$\mathbb{P}^{\text{reach}} : s \mapsto \mathbb{P}\left(\begin{array}{c}\text{the system eventually visits} \\ \text{the region } C \text{ from } s\end{array}\right)$$

Two objective functions

- Given: a control flow graph, and a subset C of its states
- For $s \in L \times \mathbb{R}^V =$ (state space),

$$\mathbb{E}^{\text{steps}} : s \mapsto \mathbb{E}\left(\begin{array}{c}\text{the number of steps from } s \\ \text{to the region } C\end{array}\right)$$

$$\mathbb{P}^{\text{reach}} : s \mapsto \mathbb{P}\left(\begin{array}{c}\text{the system eventually visits} \\ \text{the region } C \text{ from } s\end{array}\right)$$

…under angelic/demonic scheduler

Soundness/completeness

Ranking supermartingale

Soundness: f is a RankSM $\Rightarrow$ $\mathbb{E}^{\mathrm{steps}} \leq f$

$(f(s) < \infty \Rightarrow \mathbb{P}^{\mathrm{reach}}(s) = 1)$

Completeness: $\mathbb{E}^{\mathrm{steps}}$ is a RankSM

Nonnegative repulsing supermartingale

Soundness: f is a RepSM $\Rightarrow$ $\mathbb{P}^{\mathrm{reach}} \leq f$

Completeness: $\mathbb{P}^{\mathrm{reach}}$ is a RepSM

State of the Art

Approximation method	Certificate for	Soundness	Completeness
Additive ranking Supermartingale (Chakarov-Sankaranarayanan, CAV'13 etc.)	$\mathbb{E}^{\mathrm{steps}} < \infty$ ($\mathbb{P}^{\mathrm{reach}} = 1$)	Yes (with nondet. / continuous variable)	Yes (with nondet. / discrete variable)
Nonnegative repulsing supermartingale (Steinhardt+, IJRR'12 etc.)	$\mathbb{P}^{\mathrm{reach}} \leq ?$	Yes (NO nondet. / continuous variable)*	-
γ-scaled submartingale (Urabe+, LICS'17)	$\mathbb{P}^{\mathrm{reach}} \geq ?$	Yes (NO nondet. / continuous variable)	-
ε-decreasing repulsing supermartingale (Chatterjee+, POPL'17)	$\mathbb{P}^{\mathrm{reach}} \leq ?$	Yes (with nondet. / continuous var. / linearity assumpt.)	-

*In [Steinhardt+] continuous-time dynamics is also considered
Soundness for *c-supermartingale* is shown, which is a relaxation of supermartingale

Our contributions

Soundness/completeness of martingale techniques for PPs with continuous variables and nondeterminism

Characterization of martingale techniques via Knaster-Tarski fixed point theorem

Implementation and experiments

Our contributions

Soundness/completeness of martingale techniques for PPs with continuous variables and nondeterminism

Characterization of martingale techniques via Knaster-Tarski fixed point theorem

Implementation and experiments

Soundness/completeness of martingale techniques

Approximation method	Certificate for	Soundness	Completeness
Additive ranking Supermartingale (Chakarov-Sankaranarayanan, CAV'13 etc.)	$\mathbb{E}^{\text{steps}} < \infty$ ($\mathbb{P}^{\text{reach}} = 1$)	Yes (with nondet. / continuous variable)	Yes (with nondet. / discrete variable)
Nonnegative repulsing supermartingale (Steinhardt+, IJRR'12 etc.)	$\mathbb{P}^{\text{reach}} \leq ?$	Yes (NO nondet. / continuous variable)*	-
γ-scaled submartingale (Urabe+, LICS'17)	$\mathbb{P}^{\text{reach}} \geq ?$	Yes (NO nondet. / continuous variable)	-
ε-decreasing repulsing supermartingale (Chatterjee+, POPL'17)	$\mathbb{P}^{\text{reach}} \leq ?$	Yes (with nondet. / continuous var. / linearity assumpt.)	-

*In [Steinhardt+] continuous-time dynamics is also considered
Soundness for *c-supermartingale* is shown, which is a relaxation of supermartingale

Soundness/completeness of martingale techniques

Approximation method	Certificate for	Soundness	Completeness
Additive ranking Supermartingale (Chakarov-Sankaranarayanan, CAV'13 etc.)	$\mathbb{E}^{\mathrm{steps}} < \infty$ $(\mathbb{P}^{\mathrm{reach}} = 1)$	Yes (with nondet. / continuous variable)	Yes (with nondet. / cont. var.)
Nonnegative repulsing supermartingale (Steinhardt+, IJRR'12 etc.)	$\mathbb{P}^{\mathrm{reach}} \leq ?$	Yes (with nondet. / continuous variable)*	
γ-scaled submartingale (Urabe+, LICS'17)	$\mathbb{P}^{\mathrm{reach}} \geq ?$	Yes (with nondet. / cont. var.)	-
ε-decreasing repulsing supermartingale (Chatterjee+, POPL'17)	$\mathbb{P}^{\mathrm{reach}} \leq ?$	Yes (with nondet. / continuous var. / linearity assumpt.)	No

*In [Steinhardt+] continuous-time dynamics is also considered
Soundness for *c-supermartingale* is shown, which is a relaxation of supermartingale

Soundness/completeness of martingale techniques

Approximation method	Certificat...	S...ndness	Completeness
Additive rankin... Superm... (Chakar...			Yes ...det. /
No... super... (Steinhardt+, ...			
γ-scaled submartingale (Urabe+, LICS'17)	$\geq ?$	(with nondet. / cont. var.)	-
ε-decreasing repulsing supermartingale (Chatterjee+, POPL'17)	$\mathbb{P}^{\mathrm{reach}} \leq ?$	Yes (with nondet. / continuous var. / linearity assumpt.)	No

For certain endofunctions Φ and Ψ,

$\mathbb{E}^{\mathrm{steps}} = \mu\Phi$ and $\mathbb{P}^{\mathrm{reach}} = \mu\Psi$

*In [Steinhardt+] continuous-time dynamics is also considered
Soundness for *c-supermartingale* is shown, which is a relaxation of supermartingale

Soundness/completeness of RankSM

Our theorem

$$\mathbb{E}^{\text{steps}} = \mu\Phi$$

The lattice $(\mathcal{F}, \sqsubseteq)$

$\mathcal{F}$ ... the set of all (measurable) functions

$$f : L \times \mathbb{R}^V \to [0, \infty]$$

$\sqsubseteq$ ... $f \sqsubseteq g \iff \forall s.\, f(s) \le g(s)$

Soundness/completeness of RankSM

Our theorem

$$\mathbb{E}^{\text{steps}} = \mu\Phi$$

The lattice $(\mathcal{F}, \sqsubseteq)$

$\mathcal{F}$ ... the set of all (measurable) functions

$$f : L \times \mathbb{R}^V \to [0, \infty]$$

$\sqsubseteq$ ... $f \sqsubseteq g \Leftrightarrow \forall s.\, f(s) \le g(s)$

Soundness

$$\frac{f \text{ is a RankSM}}{\mathbb{E}^{\text{steps}} \sqsubseteq f}$$

Soundness/completeness of RankSM

Our theorem

$$\mathbb{E}^{\text{steps}} = \mu\Phi$$

The lattice $(\mathcal{F}, \sqsubseteq)$

$\mathcal{F}$ ... the set of all (measurable) functions

$$f: L \times \mathbb{R}^V \to [0, \infty]$$

$\sqsubseteq$ ... $\quad f \sqsubseteq g \Leftrightarrow \forall s. f(s) \leq g(s)$

Soundness

$$\frac{f \text{ is a RankSM}}{\mathbb{E}^{\text{steps}} \sqsubseteq f} \quad \Leftrightarrow \quad \frac{\Phi f \sqsubseteq f}{\mu\Phi \sqsubseteq f}$$

Soundness/completeness of RankSM

Our theorem

$$\mathbb{E}^{\text{steps}} = \mu\Phi$$

The lattice $(\mathcal{F}, \sqsubseteq)$

$\mathcal{F}$ ... the set of all (measurable) functions

$$f : L \times \mathbb{R}^V \to [0, \infty]$$

$\sqsubseteq$ ... $f \sqsubseteq g \iff \forall s.\, f(s) \leq g(s)$

Soundness

$$\frac{f \text{ is a RankSM}}{\mathbb{E}^{\text{steps}} \sqsubseteq f} \quad \begin{matrix} \Leftrightarrow \\ \Leftrightarrow \end{matrix} \quad \boxed{\frac{\Phi f \sqsubseteq f}{\mu\Phi \sqsubseteq f}}$$

Knaster-Tarski theorem

Soundness/completeness of RankSM

Our theorem

$$\mathbb{E}^{\text{steps}} = \mu\Phi$$

The lattice $(\mathcal{F}, \sqsubseteq)$

$\mathcal{F}$ ... the set of all (measurable) functions

$$f : L \times \mathbb{R}^V \to [0, \infty]$$

$\sqsubseteq$ ... $\quad f \sqsubseteq g \Leftrightarrow \forall s.\, f(s) \leq g(s)$

Soundness

$$\frac{f \text{ is a RankSM}}{\mathbb{E}^{\text{steps}} \sqsubseteq f} \quad \begin{array}{c}\Leftrightarrow \\ \Leftrightarrow\end{array} \quad \boxed{\frac{\Phi f \sqsubseteq f}{\mu\Phi \sqsubseteq f}}$$

Knaster-Tarski theorem

Completeness

$$\Phi\mathbb{E}^{\text{steps}} \sqsubseteq \mathbb{E}^{\text{steps}}$$

Soundness/completeness of NNRepSM

Our theorem

$$\mathbb{P}^{\mathrm{reach}} = \mu\Psi$$

The lattice $(\mathcal{F}, \sqsubseteq)$

$\mathcal{F}$ ... the set of all (measurable) functions

$$f : L \times \mathbb{R}^V \to [0,1]$$

$\sqsubseteq$ ... $\quad f \sqsubseteq g \Leftrightarrow \forall s. f(s) \leq g(s)$

Soundness

$$\frac{f \text{ is a RepSM}}{\mathbb{P}^{\mathrm{reach}} \sqsubseteq f} \Leftrightarrow \boxed{\frac{\Psi f \sqsubseteq f}{\mu\Psi \sqsubseteq f}}$$

Knaster-Tarski theorem

Completeness

$$\Psi\mathbb{P}^{\mathrm{reach}} \sqsubseteq \mathbb{P}^{\mathrm{reach}}$$

Our contributions

Soundness/completeness of martingale techniques for PPs with continuous variables and nondeterminism

Characterization of martingale techniques via Knaster-Tarski fixed point theorem

Implementation and experiments

Synthesis algorithm

Approximation method	Certificate for	Soundness	Completeness
Additive ranking Supermartingale (Chakarov-Sankaranarayanan, CAV'13 etc.)	$\mathbb{E}^{\mathrm{steps}} < \infty$ ($\mathbb{P}^{\mathrm{reach}} = 1$)	Yes (with nondet. / continuous variable)	Yes (with nondet. / cont. var.)
Nonnegative repulsing supermartingale (Steinhardt+, IJRR'12 etc.)	$\mathbb{P}^{\mathrm{reach}} \leq ?$	Yes (with nondet. / continuous variable)	
γ-scaled submartingale (Urabe+, LICS'17)	$\mathbb{P}^{\mathrm{reach}} \geq ?$	Yes (with nondet. / cont. var.)	-
ε-decreasing repulsing supermartingale (Chatterjee+, POPL'17)	$\mathbb{P}^{\mathrm{reach}} \leq ?$	Yes (with nondet. / continuous var. / linearity assumpt.)	No

- Input: affine/polynomial PP
- Translate PP to
  - control flow graph
  - initial state x_{init}
  - set of terminal states
- For the set F of all affine/polynomial functions over states, solve:

$$\operatorname*{minimize}_{f \in F} f(x_{init}) \quad , \quad \text{subject to (Upper NNRepSupM condition)}$$

- Output: $f(x_{init})$

Overapprox. " $\sup \mathbb{P}^{\mathrm{reach}}$ "

Approximation method	Certificate for	Soundness	Completeness
Additive ranking Supermartingale (Chakarov-Sankaranarayanan, CAV'13 etc.)	$\mathbb{E}^{\mathrm{steps}} < \infty$ ($\mathbb{P}^{\mathrm{reach}} = 1$)	Yes (with nondet. / continuous variable)	Yes (with nondet. / cont. var.)
Nonnegative repulsing supermartingale (Steinhardt+, IJRR'12 etc.)	$\mathbb{P}^{\mathrm{reach}} \leq ?$	Yes (with nondet. / continuous variable)	
γ-scaled submartingale (Urabe+, LICS'17)	$\mathbb{P}^{\mathrm{reach}} \geq ?$	Yes (with nondet. / cont. var.)	-
ε-decreasing repulsing supermartingale (Chatterjee+, POPL'17)	$\mathbb{P}^{\mathrm{reach}} \leq ?$	Yes (with nondet. / continuous var. / linearity assumpt.)	No

Synthesis algorithm

- Input: affine/polynomial PP
- Translate PP to
  - control flow graph
  - initial state x_{init}
  - set of terminal states

Can be reduced to LP/SDP problem
(e.g. Chakarov-Sankaranarayanan, CAV'13; Chatterjee+, CAV'16)

- For the set F of all affine/polynomial functions over states, solve:

$$\underset{f \in F}{\text{minimize}}\ f(x_{init}) \quad , \quad \text{subject to (Upper NNRepSupM condition)}$$

- Output: $f(x_{init})$

Overapprox. “ $\sup \mathbb{P}^{\mathrm{reach}}$ ”

Synthesis algorithm

Approximation method	Certificate for	Soundness	Completeness
Additive ranking Supermartingale (Chakarov-Sankaranarayanan, CAV'13 etc.)	$\mathbb{E}^{\mathrm{steps}} < \infty$ ($\mathbb{P}^{\mathrm{reach}} = 1$)	Yes (with nondet. / continuous variable)	Yes (with nondet. / cont. var.)
Nonnegative repulsing supermartingale (Steinhardt+, IJRR'12 etc.)	$\mathbb{P}^{\mathrm{reach}} \leq ?$	Yes (with nondet. / continuous variable)	
γ-scaled submartingale (Urabe+, LICS'17)	$\mathbb{P}^{\mathrm{reach}} \geq ?$	Yes (with nondet. / cont. var.)	-
ε-decreasing repulsing supermartingale (Chatterjee+, POPL'17)	$\mathbb{P}^{\mathrm{reach}} \leq ?$	Yes (with nondet. / continuous var. / linearity assumpt.)	No

- Input: affine/polynomial PP
- Translate PP to
  - control flow graph
  - initial state x_{init}
  - set of terminal states

Can be reduced to LP problem
(e.g. Chakarov-Sankaranarayanan, CAV'13)

- For the set F of all affine functions over states, solve:

$$\max_{f \in F} f(x_{init}) \quad , \quad \text{subject to (Lower } \gamma\text{-SclSubM condition)}$$

- Output: $f(x_{init})$

Underapprox. " $\inf \mathbb{P}^{\mathrm{reach}}$ "

Approximation method	Certificate for	Soundness	Completeness
Additive ranking Supermartingale (Chakarov-Sankaranarayanan, CAV'13 etc.)	$\mathbb{E}^{\mathrm{steps}} < \infty$ ($\mathbb{P}^{\mathrm{reach}} = 1$)	Yes (with nondet. / continuous variable)	Yes (with nondet. / cont. var.)
Nonnegative repulsing supermartingale (Steinhardt+, IJRR'12 etc.)	$\mathbb{P}^{\mathrm{reach}} \leq ?$	Yes (with nondet. / continuous variable)	
γ-scaled submartingale (Urabe+, LICS'17)	$\mathbb{P}^{\mathrm{reach}} \geq ?$	Yes (with nondet. / cont. var.)	-
ε-decreasing repulsing supermartingale (Chatterjee+, POPL'17)	$\mathbb{P}^{\mathrm{reach}} \leq ?$	Yes (with nondet. / continuous var. / linearity assumpt.)	No

Experiments

γ-scaled submartingale

		Prog. III (linear)	
	param.	time (s)	bound
(a-1)	$p_1 = 0.2$ $p_2 = 0.4$	0.026	≥ 0
	$p_1 = 0.8$ $p_2 = 0.1$	0.022	≥ 0.751
(a-2)	$M_1 = -1$ $M_2 = 2$	0.033	≥ 0
	$M_1 = -2$ $M_2 = 1$	0.033	≥ 0.767
(a-3)	$M_1 = -1$ $M_2 = 2$	0.028	≥ 0
	$M_1 = -2$ $M_2 = 1$	0.040	≥ 0.801
(b)	$c = 0.1$ $p = 0.5$	0.056	≥ 0
	$c = 0.1$ $p = 0.1$	0.054	≥ 0.148

Nonnegative repulsing submartingale

		Prog. I (linear)		Prog. II (deg.-2 poly.)		Prog. II (deg.-3 poly.)	
	param.	time (s)	bound	time (s)	bound	time (s)	bound
(a-1)	$p_1 = 0.2$ $p_2 = 0.4$	0.021	≤ 0.825	530.298	≤ 0.6552	572.393	≤ 0.6555
	$p_1 = 0.8$ $p_2 = 0.1$	0.024	≤ 1	526.519	≤ 1.0	561.327	≤ 1.0

- Input: adversarial random walk (similar to the reading ex.)
- Nontrivial bounds found in 50% cases

Experiments

Approximation method	Certificate for	Soundness	Completeness
Additive ranking Supermartingale (Chakarov-Sankaranarayanan, CAV'13 etc.)	$\mathbb{E}^{\text{steps}} < \infty$ ($\mathbb{P}^{\text{reach}} = 1$)	Yes (with nondet. / continuous variable)	Yes (with nondet. / cont. var.)
Nonnegative repulsing supermartingale (Steinhardt+, IJRR'12 etc.)	$\mathbb{P}^{\text{reach}} \leq ?$	Yes (with nondet. / continuous variable)	
γ-scaled submartingale (Urabe+, LICS'17)	$\mathbb{P}^{\text{reach}} \geq ?$	Yes (with nondet. / cont. var.)	-
ε-decreasing repulsing supermartingale (Chatterjee+, POPL'17)	$\mathbb{P}^{\text{reach}} \leq ?$	Yes (with nondet. / continuous var. / linearity assumpt.)	No

	true reachability probability	U-NNRepSupM	1-RepSupM
(c-1)	$\frac{(0.4/0.6)^5 - (0.4/0.6)^{10}}{1-(0.4/0.6)^{10}} \approx 0.116$	0.505	< 1
(c-2)	0.5	0.5	—
(c-3)	$\int_0^1 \left(\frac{0.25}{0.75}\right)^{\lceil \log_2(1/x) \rceil} dx \approx 0.2$	0.5	—
(c-4)	$\left(\frac{0.25}{0.75}\right)^1 \approx 0.333$	—	< 1

Observed comparative advantage of nonnegative RepSM over ε-decreasing RepSM

Thank you for your attention ☺

Approximation method	Certificate for	Soundness	Completeness
Additive ranking Supermartingale (Chakarov-Sankaranarayanan, CAV'13 etc.)	$\mathbb{E}^{\text{steps}} < \infty$ $(\mathbb{P}^{\text{reach}} = 1)$	Yes (with nondet. / continuous variable)	Yes (with nondet. / cont. var.)
Nonnegative repulsing supermartingale (Steinhardt+, IJRR'12 etc.)	$\mathbb{P}^{\text{reach}} \leq ?$	Yes (with nondet. / continuous variable)*	
γ-scaled submartingale (Urabe+, LICS'17)	$\mathbb{P}^{\text{reach}} \geq ?$	Yes (with nondet. / cont. var.)	-
ε-decreasing repulsing supermartingale (Chatterjee+, POPL'17)	$\mathbb{P}^{\text{reach}} \leq ?$	Yes (with nondet. / continuous var. / linearity assumpt.)	No

*In [Steinhardt+] continuous-time dynamics is also considered
Soundness for *c-supermartingale* is shown, which is a relaxation of supermartingale