Quantitative Verification of Parameterized Systems

Rayna Dimitrova

MPI-SWS

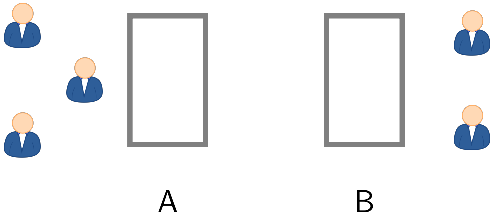
Joint work with Luis María Ferrer Fioriti, Holger Hermanns and Rupak Majumdar

The Choice Coordination problem

1 2 … K

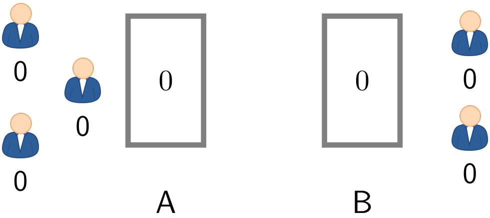
- N processes have to agree on exactly one of K alternatives.
- The processes communicate via K shared variables over Σ.
- Size of the alphabet Σ for deterministic protocols?
  - in general: $|\Sigma| = N + 2$ is sufficient [Fischer,Rabin]
  - for $k = 2$: $|\Sigma| = \frac{N}{2} + 2$ is sufficient
  - lower bound: $|\Sigma| > \frac{1}{2}\sqrt[3]{N}$ [Rabin'82]

Rabin's Choice Coordination protocol



- Fixed synchronization alphabet $\Sigma = \{0, \ldots, M\}$ with M even
- Pair-up the elements of Σ: $0, (1,2), (3,4), \ldots, (M-1, M)$
- For a pair (a, b), define $\widehat{a} = b$ and $\widehat{b} = a$.

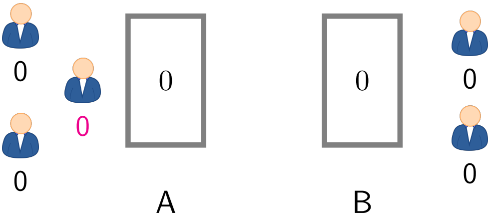
Rabin's Choice Coordination protocol



Initially, all values are 0.

At each step, pick a person outside A or B and perform an action.

Rabin's Choice Coordination protocol

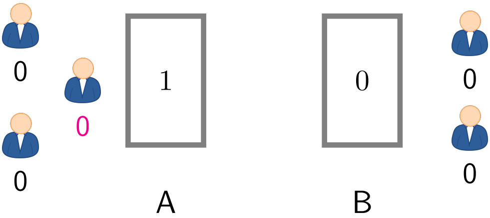


If $v@A$ and $v = a$, and $a < M - 1$ then set

$$a = \begin{cases} a+2 & \text{with probability } \frac{1}{2}, \\ \widehat{(a+2)} & \text{with probability } \frac{1}{2}. \end{cases}$$

Set v to a and move to B.

Rabin's Choice Coordination protocol

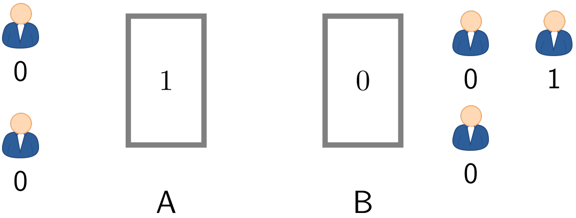


If $v@A$ and $v = a$, and $a < M - 1$ then set

$$a = \begin{cases} a + 2 & \text{with probability } \frac{1}{2}, \\ \widehat{(a+2)} & \text{with probability } \frac{1}{2}. \end{cases}$$

Set v to a and move to B.

Rabin's Choice Coordination protocol

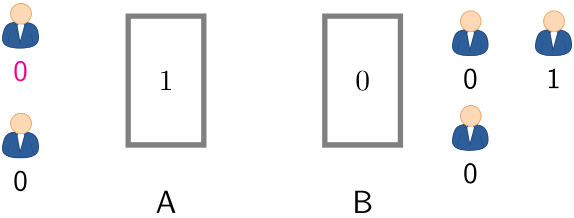


If $v@A$ and $v = a$, and $a < M - 1$ then set

$$a = \begin{cases} a+2 & \text{with probability } \frac{1}{2}, \\ \widehat{(a+2)} & \text{with probability } \frac{1}{2}. \end{cases}$$

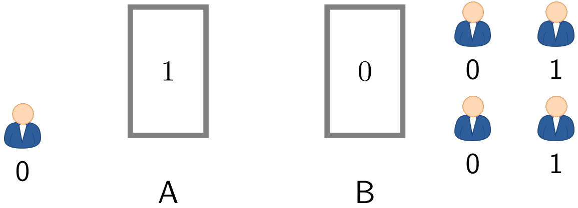
Set v to a and move to B.

Rabin's Choice Coordination protocol



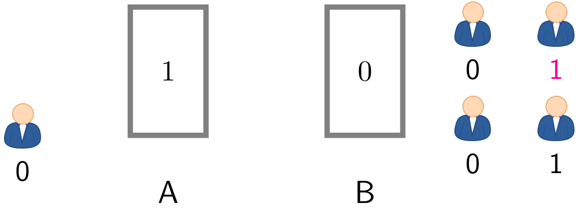
If $v@A$ and $v < a$, then set v to a and move to B.

Rabin's Choice Coordination protocol



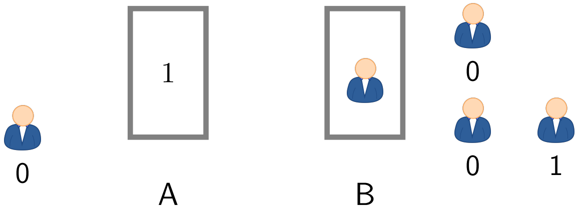
If $v@A$ and $v < a$, then set v to a and move to B.

Rabin's Choice Coordination protocol



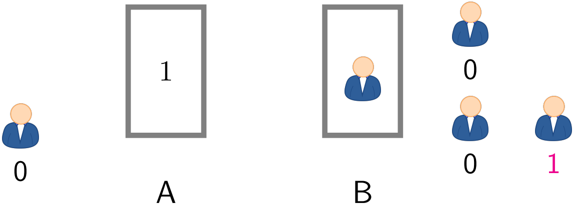
If $v@B$ then $v > b$, then enter location B.

Rabin's Choice Coordination protocol



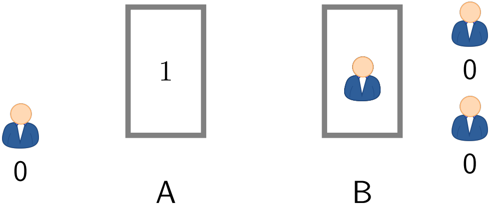
If $v@B$ then $v > b$, then enter location B.

Rabin's Choice Coordination protocol



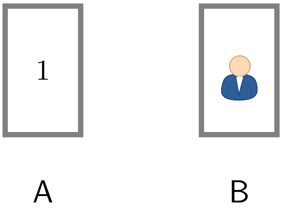
If $v@B$ and B was chosen, then enter location B.

Rabin's Choice Coordination protocol



If $v@B$ and B was chosen, then enter location B.

Rabin's Choice Coordination protocol



The protocol terminates with probability $1 - \frac{1}{2^{\frac{M}{2}}}$,
where $\Sigma = \{0, \ldots, M\}$ is the synchronization alphabet.

Quantitative verification of parameterized systems

Model: probabilistic choice + nondeterminism

State-space: infinite (or weakly finite)

- model-checking cannot be applied directly

Property: quantitative

- cannot use methods for almost-sure termination

[Esparza, Gaiser, Kiefer @ CAV'12]
[Chakarov, Sankaranarayanan @ CAV'13]
[Ferrer Fioriti, Hermanns @ POPL'15]
[Lin,Rümmer @ CAV'16]

A deductive proof system for PCTL*

quantitative temporal properties	yes
nondeterminism	yes
infinite state space	yes

[D., Ferrer Fioriti, Hermanns, Majumdar @ TACAS'16]

A deductive proof system for PCTL*

Deductive proof systems
for **non-probabilistic** systems
for CTL* [Kesten,Pnueli] and
for ATL* [Slanina,Sipma,Manna]

Lyapunov ranking functions
for **almost-sure termination**
[Bournez,Garnier]

Proof rules for **quantitative temporal** properties

Probabilistic programs

Probabilistic programs

Variables

- $N \in \mathbb{N}$: number of processes
- $a, b \in \mathbb{N}$: shared variables at location A (resp. B)
- $n_{v@A}, n_{v@B} \in \mathbb{N}$: number of processes holding value $v \in \{0, \ldots, M\}$ outside location A (B)

$$out_A = \sum_{v=0}^{M} n_{v@A}, \quad out_B = \sum_{v=0}^{M} n_{v@B}$$

- $in_A, in_B \in \mathbb{N}$: number of processes inside location A (resp. B)

Probabilistic programs

Variables

- $N \in \mathbb{N}$: number of processes
- $a, b \in \mathbb{N}$: shared variables at location A (resp. B)
- $n_{v@A}, n_{v@B} \in \mathbb{N}$: number of processes holding value $v \in \{0, \ldots, M\}$ outside location A (B)

$$out_A = \sum_{v=0}^{M} n_{v@A}, \quad out_B = \sum_{v=0}^{M} n_{v@B}$$

- $in_A, in_B \in \mathbb{N}$: number of processes inside location A (resp. B)

Nondeterministic choice (resolved by scheduler)

- choose a guarded command of the program to be executed

Probabilistic programs

Variables

- $N \in \mathbb{N}$: number of processes
- $a, b \in \mathbb{N}$: shared variables at location A (resp. B)
- $n_{v@A}, n_{v@B} \in \mathbb{N}$: number of processes holding value $v \in \{0, \ldots, M\}$ outside location A (B)

$$out_A = \sum_{v=0}^{M} n_{v@A}, \quad out_B = \sum_{v=0}^{M} n_{v@B}$$

- $in_A, in_B \in \mathbb{N}$: number of processes inside location A (resp. B)

Nondeterministic choice (resolved by scheduler)

- choose a guarded command of the program to be executed

Probabilistic transitions

- set a to $(a+2)$ or to $(\widehat{a+2})$ with probability $\frac{1}{2}$ each

Specifications

probabilistic temporal properties

Starting at any initial state, under every possible scheduler, Rabin's protocol eventually terminates with probability at least $1 - \frac{1}{2^{\frac{M}{2}}}$.

Specifications

probabilistic temporal properties

Starting at any initial state, under every possible scheduler, Rabin's protocol eventually terminates with probability at least $1 - \frac{1}{2^{\frac{M}{2}}}$.

expressed in Probabilistic Computational Tree Logic (PCTL*)

$$\Diamond(out_A = 0 \wedge out_B = 0)$$

LTL operators

$\Diamond$	eventually
$\Box$	globally

Specifications

probabilistic temporal properties

Starting at any initial state, under every possible scheduler, Rabin's protocol eventually terminates with probability at least $1 - \frac{1}{2^{\frac{M}{2}}}$.

expressed in Probabilistic Computational Tree Logic (PCTL*)

$$\mathbb{P}^{\forall}_{\geq 1 - \frac{1}{2^{\frac{M}{2}}}} \left(\Diamond (out_A = 0 \wedge out_B = 0) \right)$$

LTL operators

$\Diamond$	eventually
$\Box$	globally

probabilistic quantifiers

$\mathbb{P}^{\exists}_{\bowtie p}$	exists a scheduler
$\mathbb{P}^{\forall}_{\bowtie p}$	for all schedulers

Specifications

probabilistic temporal properties

Starting at any initial state, under every possible scheduler, Rabin's protocol eventually terminates with probability at least $1 - \frac{1}{2^{\frac{M}{2}}}$.

expressed in Probabilistic Computational Tree Logic (PCTL*)

$$\varphi_{init} \rightarrow \mathbb{P}^{\forall}_{\geq 1-\frac{1}{2^{\frac{M}{2}}}}\,(\Diamond(out_A = 0 \wedge out_B = 0))$$

LTL operators

$\Diamond$	eventually
$\Box$	globally

probabilistic quantifiers

$\mathbb{P}^{\exists}_{\bowtie p}$	exists a scheduler
$\mathbb{P}^{\forall}_{\bowtie p}$	for all schedulers

Outline

$$\dfrac{\dfrac{\text{Lyapunov ranking function } \delta}{P \vdash \varphi_{init} \to \mathbb{P}^{\forall}_{=1}(\Diamond(\varphi_{term} \vee \varphi_{stuck}))}\,\textsc{until}^{\forall}_{=1} \qquad \dfrac{\text{ranking function } r}{P \vdash \varphi_{init} \to \mathbb{P}^{\forall}_{\leq p}(\Diamond \varphi_{stuck})}\,\textsc{until}^{\forall}_{\leq q^m}}{P \vdash \varphi_{init} \to \mathbb{P}^{\forall}_{\geq 1-p}(\Diamond \varphi_{term})}\,\textsc{until}^{\forall}_{\geq 1-p}$$

Outline

almost-sure reachability:

Lyapunov ranking function δ

ranking function r

$$\frac{}{P \vdash \varphi_{init} \to \mathbb{P}^{\forall}_{=1}(\Diamond(\varphi_{term} \vee \varphi_{stuck}))}\ \textsc{until}^{\forall}_{=1}$$

$$\frac{}{P \vdash \varphi_{init} \to \mathbb{P}^{\forall}_{\leq p}(\Diamond\, \varphi_{stuck})}\ \textsc{until}^{\forall}_{\leq q^m}$$

$$\frac{}{P \vdash \varphi_{init} \to \mathbb{P}^{\forall}_{\geq 1-p}(\Diamond\, \varphi_{term})}\ \textsc{until}^{\forall}_{\geq 1-p}$$

Rule for almost-sure reachability

Prove $P \vdash \mathbb{P}^{\forall}_{=1}(\Diamond\, \varphi_{term})$, where $\varphi_{term} \equiv out_A = 0 \wedge out_B = 0$?

Rule for almost-sure reachability

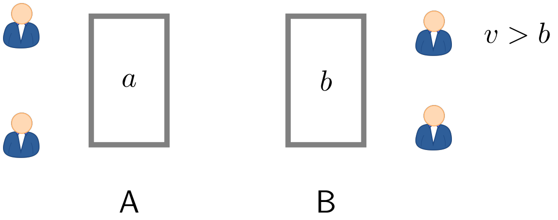
Prove $P \vdash \mathbb{P}^{\forall}_{=1}(\Diamond \varphi_{term})$, where $\varphi_{term} \equiv out_A = 0 \wedge out_B = 0$?

Lyapunov ranking function maps states to $(\mathbb{R}_{\geq 0}, \succ)$, where $\succ$ is well-founded, and $\delta(s) \succ \mathbb{E}(\delta' \mid s)$ when s not in the target set.

Rule for almost-sure reachability

Prove $P \vdash \mathbb{P}^{\forall}_{=1}(\Diamond \varphi_{term})$, where $\varphi_{term} \equiv out_A = 0 \land out_B = 0$?

Lyapunov ranking function maps states to $(\mathbb{R}_{\geq 0}, \succ)$, where $\succ$ is well-founded, and $\delta(s) \succ \mathbb{E}(\delta' \mid s)$ when s not in the target set.

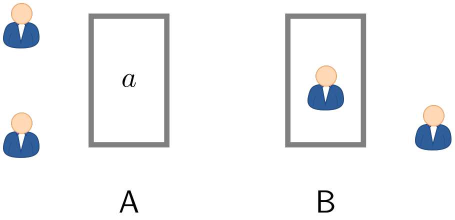


Decreases $\delta_1(s) = out_A + out_B$.

Rule for almost-sure reachability

Prove $P \vdash \mathbb{P}^{\forall}_{=1}(\Diamond \varphi_{term})$, where $\varphi_{term} \equiv out_A = 0 \wedge out_B = 0$?

Lyapunov ranking function maps states to $(\mathbb{R}_{\geq 0}, \succ)$, where $\succ$ is well-founded, and $\delta(s) \succ \mathbb{E}(\delta' \mid s)$ when s not in the target set.

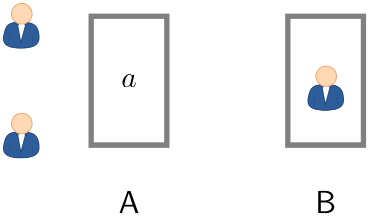


Decreases $\delta_1(s) = out_A + out_B$.

Rule for almost-sure reachability

Prove $P \vdash \mathbb{P}^{\forall}_{=1}(\Diamond \varphi_{term})$, where $\varphi_{term} \equiv out_A = 0 \wedge out_B = 0$?

Lyapunov ranking function maps states to $(\mathbb{R}_{\geq 0}, \succ)$, where $\succ$ is well-founded, and $\delta(s) \succ \mathbb{E}(\delta' \mid s)$ when s not in the target set.

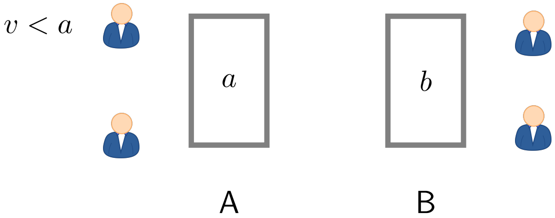


Decreases $\delta_1(s) = out_A + out_B$.

Rule for almost-sure reachability

Prove $P \vdash \mathbb{P}^{\forall}_{=1}(\Diamond \varphi_{term})$, where $\varphi_{term} \equiv out_A = 0 \wedge out_B = 0$?

Lyapunov ranking function maps states to $(\mathbb{R}_{\geq 0}, \succ)$, where $\succ$ is well-founded, and $\delta(s) \succ \mathbb{E}(\delta' \mid s)$ when s not in the target set.

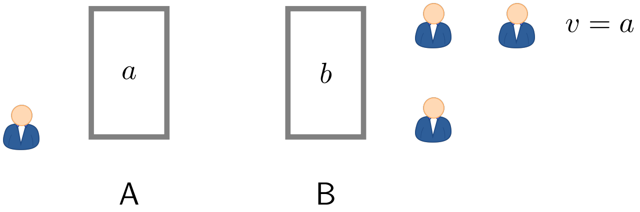


Decreases $\delta_2(s) = \sum_{v<a}(n_{v@A} + n_{v@B}) + \sum_{v<b}(n_{v@A} + n_{v@B})$.

Rule for almost-sure reachability

Prove $P \vdash \mathbb{P}^{\forall}_{=1}(\Diamond \varphi_{term})$, where $\varphi_{term} \equiv out_A = 0 \wedge out_B = 0$?

Lyapunov ranking function maps states to $(\mathbb{R}_{\geq 0}, \succ)$, where $\succ$ is well-founded, and $\delta(s) \succ \mathbb{E}(\delta' \mid s)$ when s not in the target set.



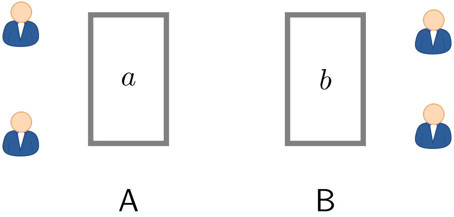
Decreases $\delta_2(s) = \sum_{v<a}(n_{v@A} + n_{v@B}) + \sum_{v<b}(n_{v@A} + n_{v@B})$.

Rule for almost-sure reachability

Prove $P \vdash \mathbb{P}^{\forall}_{=1}(\Diamond \varphi_{term})$, where $\varphi_{term} \equiv out_A = 0 \wedge out_B = 0$?

Lyapunov ranking function maps states to $(\mathbb{R}_{\geq 0}, \succ)$, where $\succ$ is well-founded, and $\delta(s) \succ \mathbb{E}(\delta' \mid s)$ when s not in the target set.

$v = a$

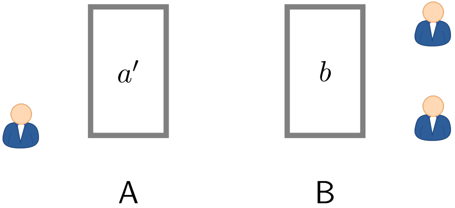


Decreases in expectation $\delta_3(s) = \begin{cases} 3 & \text{if } a = b, \\ 2 & \text{if } a \neq b \text{ and } \widehat{a} \neq b, \\ 0 & \text{if } \widehat{a} = b. \end{cases}$

Rule for almost-sure reachability

Prove $P \vdash \mathbb{P}^{\forall}_{=1}(\Diamond \varphi_{term})$, where $\varphi_{term} \equiv out_A = 0 \wedge out_B = 0$?

Lyapunov ranking function maps states to $(\mathbb{R}_{\geq 0}, \succ)$, where $\succ$ is well-founded, and $\delta(s) \succ \mathbb{E}(\delta' \mid s)$ when s not in the target set.



$v = a'$

$$a' = \begin{cases} a + 2 & \text{w.p. } \frac{1}{2}, \\ \widehat{(a+2)} & \text{w.p. } \frac{1}{2}. \end{cases}$$

Decreases in expectation $\delta_3(s) = \begin{cases} 3 & \text{if } a = b, \\ 2 & \text{if } a \neq b \text{ and } \widehat{a} \neq b, \\ 0 & \text{if } \widehat{a} = b. \end{cases}$

Rule for almost-sure reachability

Prove $P \vdash \mathbb{P}^{\forall}_{=1}(\Diamond \varphi_{term})$, where $\varphi_{term} \equiv out_A = 0 \wedge out_B = 0$?

Lyapunov ranking function maps states to $(\mathbb{R}_{\geq 0}, \succ)$, where $\succ$ is well-founded, and $\delta(s) \succ \mathbb{E}(\delta' \mid s)$ when s not in the target set.

Take $\delta(s) = \delta_1(s) + \delta_2(s) + (2N+1) \cdot \delta_3(s)$.

Rule for almost-sure reachability

Prove $P \vdash \mathbb{P}^{\forall}_{=1}(\Diamond \varphi_{term})$, where $\varphi_{term} \equiv out_A = 0 \wedge out_B = 0$?

Lyapunov ranking function maps states to $(\mathbb{R}_{\geq 0}, \succ)$, where $\succ$ is well-founded, and $\delta(s) \succ \mathbb{E}(\delta' \mid s)$ when s not in the target set.

We need idle transitions when $a = b = M - 1$ or $a = b = M$.

No variable changes, so no Lyapunov ranking function.

Rule for almost-sure reachability

Prove $P \vdash \mathbb{P}^{\forall}_{=1}(\Diamond \varphi_{term})$, where $\varphi_{term} \equiv out_A = 0 \wedge out_B = 0$?

Lyapunov ranking function maps states to $(\mathbb{R}_{\geq 0}, \succ)$, where $\succ$ is well-founded, and $\delta(s) \succ \mathbb{E}(\delta' \mid s)$ when s not in the target set.

Prove the weaker property

$P \vdash \mathbb{P}^{\forall}_{=1}(\Diamond(\varphi_{term} \vee \varphi_{stuck}))$,
where $\varphi_{stuck} \equiv (a = M - 1 \wedge b = M - 1 \vee a = M \wedge b = M)$.

Outline

Lyapunov ranking function δ

ranking function r

$$\dfrac{}{P \vdash \varphi_{init} \to \mathbb{P}^{\forall}_{=1}(\Diamond(\varphi_{term} \lor \varphi_{stuck}))}\ \textsc{until}^{\forall}_{=1} \qquad \dfrac{}{P \vdash \varphi_{init} \to \mathbb{P}^{\forall}_{\leq p}(\Diamond\, \varphi_{stuck})}\ \textsc{until}^{\forall}_{\leq q^m}$$

$$\dfrac{}{P \vdash \varphi_{init} \to \mathbb{P}^{\forall}_{\geq 1-p}(\Diamond\, \varphi_{term})}\ \textsc{until}^{\forall}_{\geq 1-p}$$

Outline

quantitative reachability:

Lyapunov ranking function δ

ranking function r

$$\dfrac{\dfrac{\text{}}{P \vdash \varphi_{init} \to \mathbb{P}^{\forall}_{=1}(\Diamond(\varphi_{term} \lor \varphi_{stuck}))}\ \textsc{until}^{\forall}_{=1} \qquad \dfrac{\text{}}{P \vdash \varphi_{init} \to \mathbb{P}^{\forall}_{\leq p}(\Diamond\, \varphi_{stuck})}\ \textsc{until}^{\forall}_{\leq q^m}}{P \vdash \varphi_{init} \to \mathbb{P}^{\forall}_{\geq 1-p}(\Diamond\, \varphi_{term})}\ \textsc{until}^{\forall}_{\geq 1-p}$$

A rule for quantitative reachability

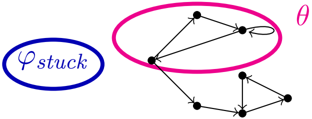
Prove $P \vdash \varphi_{init} \to \mathbb{P}^{\forall}_{\leq q^m}(\Diamond \varphi_{stuck})$ for $q = \frac{1}{2}$, and $m = \frac{M}{2}$.

A rule for quantitative reachability

Prove $P \vdash \varphi_{init} \rightarrow \mathbb{P}^{\forall}_{\leq q^m}(\Diamond\, \varphi_{stuck})$ for $q = \frac{1}{2}$, and $m = \frac{M}{2}$.

auxiliary assertion θ

- $P \vdash \theta \rightarrow \mathbb{P}^{\forall}_{=1}(\Box \neg\varphi_{stuck})$



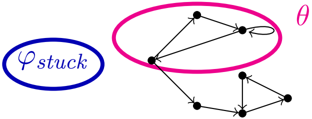
A rule for quantitative reachability

Prove $P \vdash \varphi_{init} \to \mathbb{P}^{\forall}_{\leq q^m}(\Diamond \varphi_{stuck})$ for $q = \frac{1}{2}$, and $m = \frac{M}{2}$.

auxiliary assertion θ

- $P \vdash \theta \to \mathbb{P}^{\forall}_{=1}(\Box \neg \varphi_{stuck})$

function r that maps states to $\mathbb{N}$



A rule for quantitative reachability

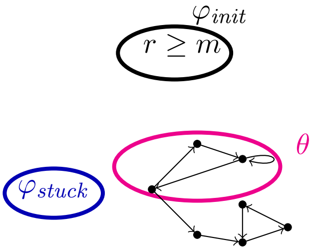
Prove $P \vdash \varphi_{init} \to \mathbb{P}^{\forall}_{\leq q^m}(\Diamond \varphi_{stuck})$ for $q = \frac{1}{2}$, and $m = \frac{M}{2}$.

auxiliary assertion θ

- $P \vdash \theta \to \mathbb{P}^{\forall}_{=1}(\Box \neg\varphi_{stuck})$

function r that maps states to $\mathbb{N}$

- for $s \in \varphi_{init}$, $r(s) \geq m$



A rule for quantitative reachability

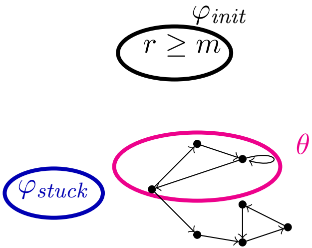
Prove $P \vdash \varphi_{init} \rightarrow \mathbb{P}^{\forall}_{\leq q^m}(\Diamond\, \varphi_{stuck})$ for $q = \frac{1}{2}$, and $m = \frac{M}{2}$.

auxiliary assertion θ

- $P \vdash \theta \rightarrow \mathbb{P}^{\forall}_{=1}(\Box \neg\varphi_{stuck})$

function r that maps states to $\mathbb{N}$

- for $s \in \varphi_{init}$, $r(s) \geq m$
- if $r(s) > 0$, then $s \notin \varphi_{stuck}$



A rule for quantitative reachability

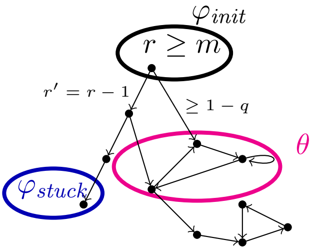
Prove $P \vdash \varphi_{init} \to \mathbb{P}^{\forall}_{\leq q^m}(\Diamond\, \varphi_{stuck})$ for $q = \frac{1}{2}$, and $m = \frac{M}{2}$.

auxiliary assertion θ

- $P \vdash \theta \to \mathbb{P}^{\forall}_{=1}(\Box \neg \varphi_{stuck})$

function r that maps states to $\mathbb{N}$

- for $s \in \varphi_{init}$, $r(s) \geq m$
- if $r(s) > 0$, then $s \notin \varphi_{stuck}$
- for states $s \notin \theta$, $r(s') \geq r(s)$ or
  $r(s') = r(s) - 1$ with prob. $\leq q$
  $s' \in \theta$ with probability $\geq 1 - q$



A rule for quantitative reachability

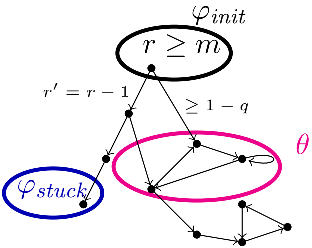
Prove $P \vdash \varphi_{init} \rightarrow \mathbb{P}^{\forall}_{\leq q^m}(\Diamond \varphi_{stuck})$ for $q = \frac{1}{2}$, and $m = \frac{M}{2}$.

auxiliary assertion θ

- $P \vdash \theta \rightarrow \mathbb{P}^{\forall}_{=1}(\Box \neg \varphi_{stuck})$

function r that maps states to $\mathbb{N}$

- for $s \in \varphi_{init}$, $r(s) \geq m$
- if $r(s) > 0$, then $s \notin \varphi_{stuck}$
- for states $s \notin \theta$, $r(s') \geq r(s)$ or
  $r(s') = r(s) - 1$ with prob. $\leq q$
  $s' \in \theta$ with probability $\geq 1 - q$



$r(s) = 0$ reached with probability $\leq q^m$

A rule for quantitative reachability

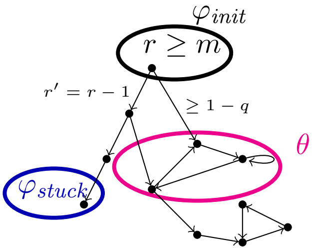
Prove $P \vdash \varphi_{init} \rightarrow \mathbb{P}^{\forall}_{\leq q^m}(\Diamond\, \varphi_{stuck})$ for $q = \frac{1}{2}$, and $m = \frac{M}{2}$.

auxiliary assertion θ

- $P \vdash \theta \rightarrow \mathbb{P}^{\forall}_{=1}(\Box \neg\varphi_{stuck})$

function r that maps states to $\mathbb{N}$

- for $s \in \varphi_{init}$, $r(s) \geq m$
- if $r(s) > 0$, then $s \notin \varphi_{stuck}$
- for states $s \notin \theta$, $r(s') \geq r(s)$ or
  $r(s') = r(s) - 1$ with prob. $\leq q$
  $s' \in \theta$ with probability $\geq 1 - q$



$r(s) = 0$ reached with probability $\leq q^m$

$$\text{Take } \theta \equiv \widehat{a} = b \text{ and } r(s) = \begin{cases} \frac{M}{2} - \min(\lceil \frac{a}{2} \rceil, \lceil \frac{b}{2} \rceil) & \text{if } \widehat{a} \neq b, \\ \frac{M}{2} - \min(\lceil \frac{a}{2} \rceil, \lceil \frac{b}{2} \rceil) + 1 & \text{if } \widehat{a} = b. \end{cases}$$

Outline

Lyapunov ranking function δ ranking function r

$$\dfrac{\dfrac{}{P \vdash \varphi_{init} \rightarrow \mathbb{P}^{\forall}_{=1}(\Diamond(\varphi_{term} \vee \varphi_{stuck}))}\,\textsc{until}^{\forall}_{=1} \qquad \dfrac{}{P \vdash \varphi_{init} \rightarrow \mathbb{P}^{\forall}_{\leq p}(\Diamond\,\varphi_{stuck})}\,\textsc{until}^{\forall}_{\leq q^m}}{P \vdash \varphi_{init} \rightarrow \mathbb{P}^{\forall}_{\geq 1-p}\,(\Diamond\,\varphi_{term})}\,\textsc{until}^{\forall}_{\geq 1-p}$$

Deductive Proof System for PCTL*

Proof rule for nested state formulas

BASIC-STATE

Proof rules for probabilistic LTL properties

BASIC-PATH, $\text{REC}^{\circlearrowleft}_{=1}$, $\text{REC}^{\circlearrowleft}_{>0}$, $\text{REC}^{\circlearrowleft}_{\geq p}$

Proof rules for invariance

$\text{INV}^{\circlearrowleft}_{=1}$, $\text{INV}^{\circlearrowleft}_{>0}$, $\text{INV}^{\circlearrowleft}_{\bowtie p}$

Proof rules for reachability

$\text{UNTIL}^{\circlearrowleft}_{=1}$, $\text{UNTIL}^{\circlearrowleft}_{>0}$, $\text{UNTIL}^{\circlearrowleft}_{\geq p}$
$\text{UNTIL}^{\circlearrowleft}_{\geq p^m}$, $\text{UNTIL}^{\circlearrowleft}_{\leq p^m}$, $\text{UNTIL}^{\forall}_{\geq 1-p}$

Additional proof rules

$\text{NEXT}^{\circlearrowleft}_{=1}$, $\text{NEXT}^{\circlearrowleft}_{>0}$, $\text{NEXT}^{\circlearrowleft}_{\bowtie p}$, GEN, MP, AND, OR
$\text{UNTIL}^{\circlearrowleft}_{\geq p_1 \cdot p_2}$, $\overline{\text{INV}}^{\forall}_{\geq p}$, $\overline{\text{REC}}^{\circlearrowleft}_{=1}$

Deductive Proof System for PCTL*

Proof rule for nested state formulas

BASIC-STATE

Proof rules for probabilistic LTL properties

BASIC-PATH, $\mathrm{REC}^{\circlearrowleft}_{=1}$, $\mathrm{REC}^{\circlearrowleft}_{>0}$, $\mathrm{REC}^{\circlearrowleft}_{\geq p}$

Proof rules for invariance

$\mathrm{INV}^{\circlearrowleft}_{=1}$, $\mathrm{INV}^{\circlearrowleft}_{>0}$, $\mathrm{INV}^{\circlearrowleft}_{\bowtie p}$

Proof rules for reachability

$\mathrm{UNTIL}^{\circlearrowleft}_{=1}$,$\mathrm{UNTIL}^{\circlearrowleft}_{>0}$, $\mathrm{UNTIL}^{\circlearrowleft}_{\geq p}$
$\mathrm{UNTIL}^{\circlearrowleft}_{\geq p^m}$, $\mathrm{UNTIL}^{\circlearrowleft}_{\leq p^m}$,$\mathrm{UNTIL}^{\forall}_{\geq 1-p}$

Additional proof rules

$\mathrm{NEXT}^{\circlearrowleft}_{=1}$, $\mathrm{NEXT}^{\circlearrowleft}_{>0}$, $\mathrm{NEXT}^{\circlearrowleft}_{\bowtie p}$, GEN, MP, AND, OR
$\mathrm{UNTIL}^{\circlearrowleft}_{\geq p_1 \cdot p_2}$,$\overline{\mathrm{INV}}^{\forall}_{\geq p}$, $\overline{\mathrm{REC}}^{\circlearrowleft}_{=1}$

Summary

Deductive proof system

- for discrete infinite-state probabilistic systems,
- applicable to quantitative temporal properties,
- sound, and for finite-state systems also complete,
- useful for verification of parameterized systems.

Thank you for your attention!

http://www.mpi-sws.org/~rayna/