Probabilistic Model Checking

Pedro R. D'Argenio

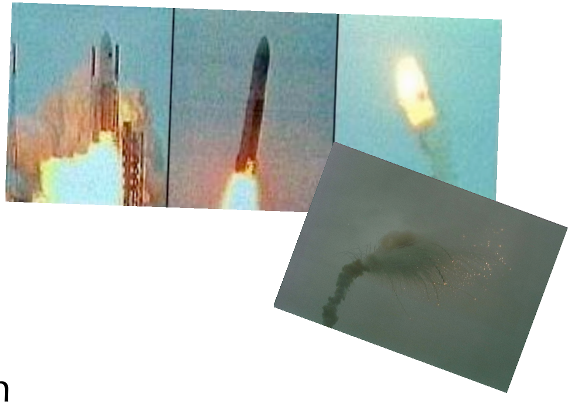
Universidad Nacional de Córdoba – CONICET
https://cs.famaf.unc.edu.ar/~dargenio/

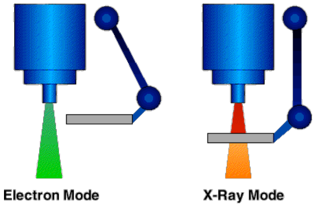
ICTAC 2023 Training School on Applied Formal Methods

Famous Errors

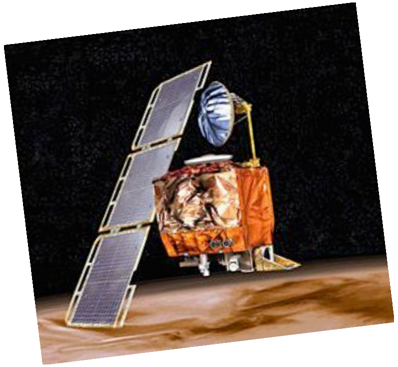
Pentium:
FDIV

Ariane 5:
64 bits fp
vs 16 bits int



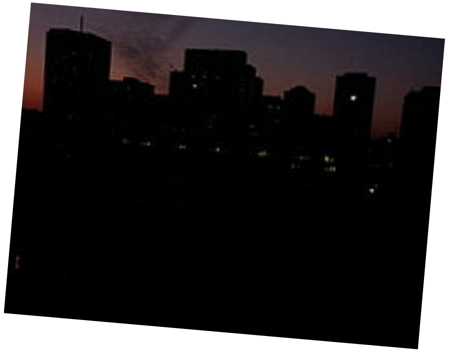


Therac-25:
Race Condition



Mars Climate
Orbiter:
Metric vs Imperial

Northeast blackout
in 2003:
Race Condition



Heartbleed:
Security

CONICET

UNC

More errors

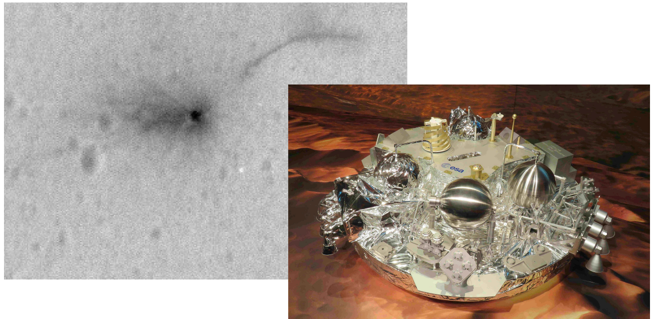
911 blackout:
MAX value reached

Nest Thermostat:
Battery drained

Nissan airbag:
Incorrect sensing

Boeing 737 MAX 8:
Incorrect sensing

Schiaparelli Landing Demonstrator Module:
Multiple errors



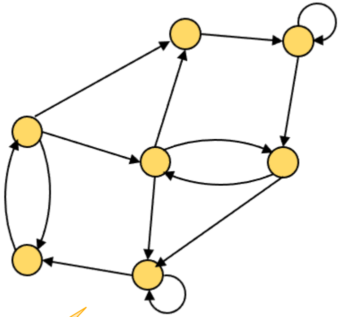
The problem of correctness…

$$\mathit{System} \vDash \mathit{Property}$$

Usually an abstraction describing the behavior

Describes what is expected from the system (The correctness criteria)

The problem of correctness…
…using Model Checking



$\models \quad \Box\,(\text{send(file)} \Rightarrow \Diamond\, \text{receive(file)}\,)$

A graph representing nondeterministic behavior

Properties that represent boolean behavior on executions

CONICET

UNC

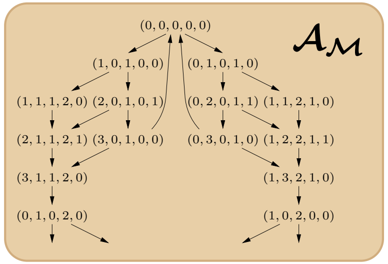
Model Checking

¿ $\mathcal{M} \models \phi$?

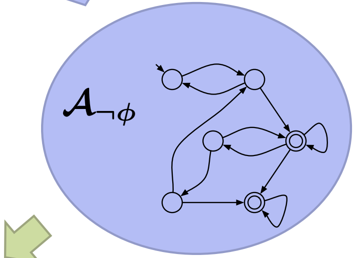
$\mathcal{M}$

```
  int y1 = 0;
  int y2 = 0;
  short in_critical = 0;

  active proctype process_1() {        active proctype process_2() {
    do                                   do
    :: true ->                           :: true ->
0:       y1 = y2+1;                  0:       y2 = y1+1;
1:       ((y2==0) || (y1<=y2));      1:       ((y1==0) || (y2<y1));
         in_critical++;                       in_critical++;
2:       in_critical--;              2:       in_critical--;
3:       y1 = 0;                     3:       y2 = 0;
    od                                   od
  }                                    }
```

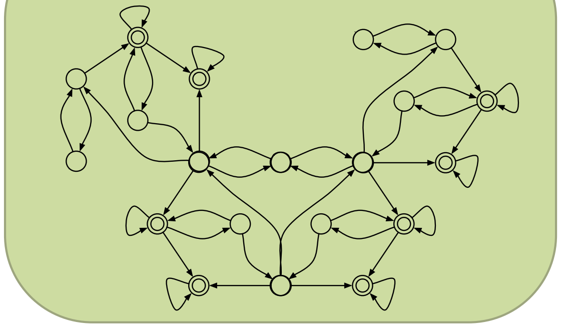


ϕ : $\Box \Diamond crit_1 \wedge \Box \Diamond crit_2$



Normally the problem reduces to graph analysis

¿ $\mathcal{A}_{\mathcal{M}} \cap \mathcal{A}_{\neg\phi} = \emptyset$?

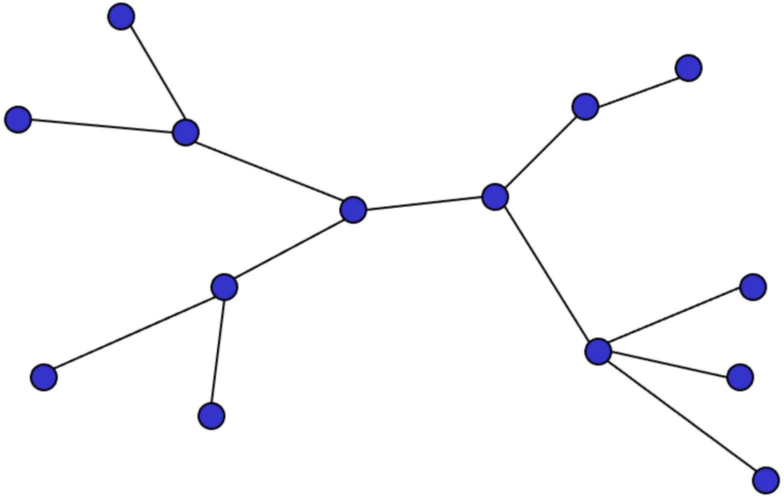


Limitations of classical Model Checking

- Many algorithms propose better solutions using randomness as a new ingredient
  - Leader Election Protocol in IEEE 1394 “Firewire”
  - Binary Exponential Backoff Algorithm in IEEE 802.3 “Ethernet”

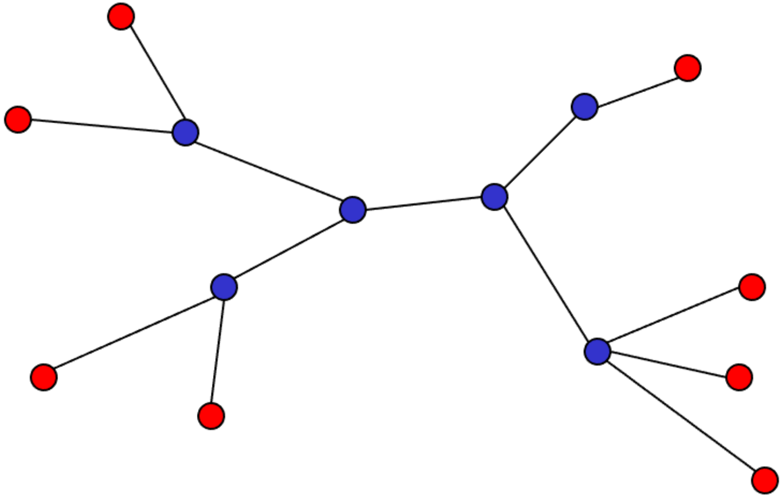
Limitations of classical Model Checking

- Many algorithms propose better solutions using randomness as a new ingredient
  - ➡ Leader Election Protocol in IEEE 1394 “Firewire”
  - Binary Exponential Backoff Algorithm in IEEE 802.3 “Ethernet”



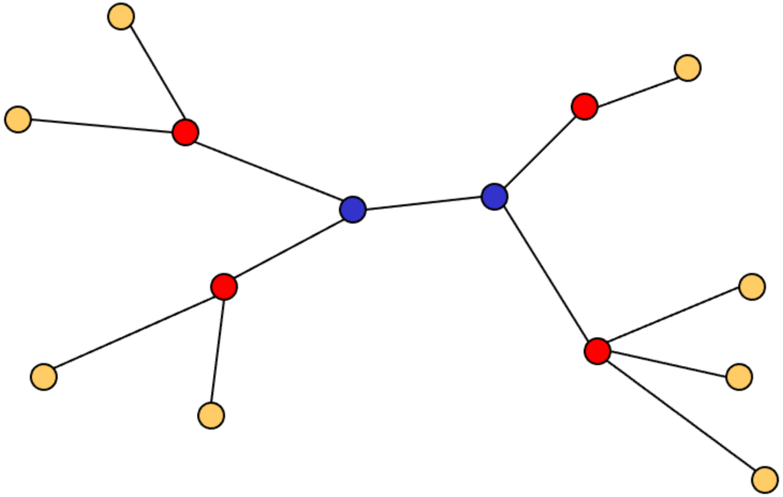
Limitations of classical Model Checking

- Many algorithms propose better solutions using randomness as a new ingredient
  - Leader Election Protocol in IEEE 1394 “Firewire”
  - Binary Exponential Backoff Algorithm in IEEE 802.3 “Ethernet”



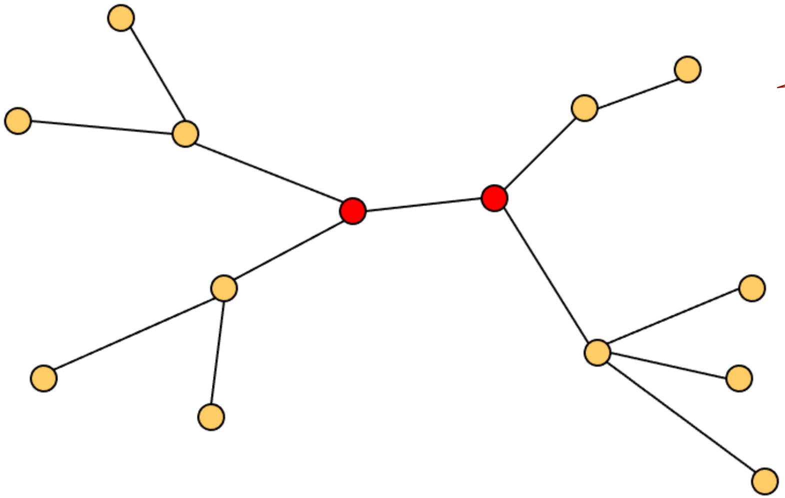
Limitations of classical Model Checking

- Many algorithms propose better solutions using randomness as a new ingredient
  - Leader Election Protocol in IEEE 1394 “Firewire”
  - Binary Exponential Backoff Algorithm in IEEE 802.3 “Ethernet”



Limitations of classical Model Checking

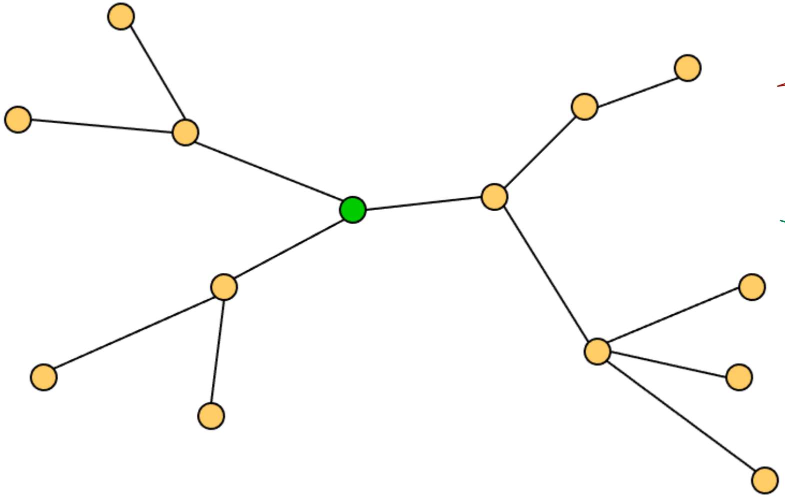
- Many algorithms propose better solutions using randomness as a new ingredient
  - Leader Election Protocol in IEEE 1394 “Firewire”
  - Binary Exponential Backoff Algorithm in IEEE 802.3 “Ethernet”



Root contention!

Limitations of classical Model Checking

- Many algorithms propose better solutions using randomness as a new ingredient
  - Leader Election Protocol in IEEE 1394 “Firewire”
  - Binary Exponential Backoff Algorithm in IEEE 802.3 “Ethernet”



Root contention!

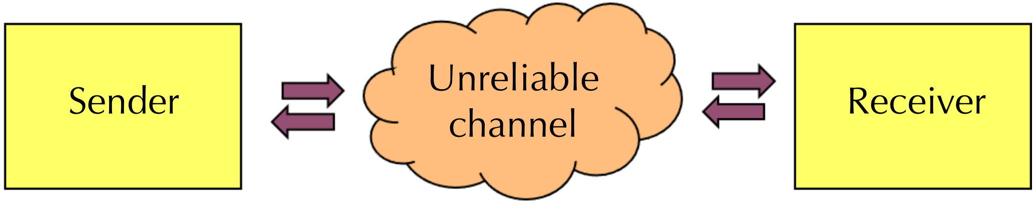
It is solved by “flipping coins”

Limitations of classical Model Checking

- Many times, correctness cannot be asserted qualitatively. Instead, the validity of a property can only be measured quantitatively
  - Bounded Retransmission Protocol in Philips RC6
  - Binary Exponential Backoff Algorithm in IEEE 802.3 “Ethernet”

Limitations of classical Model Checking

- Many times, correctness cannot be asserted qualitatively. Instead, the validity of a property can only be measured quantitatively
  - Bounded Retransmission Protocol in Philips RC6
  - Binary Exponential Backoff Algorithm in IEEE 802.3 “Ethernet”

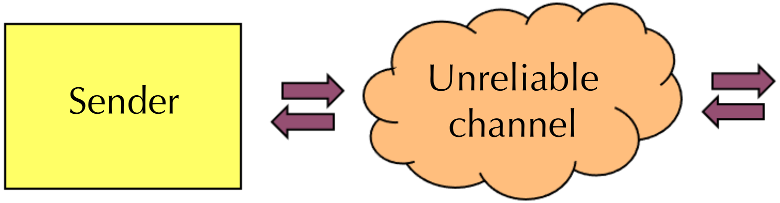


Suppose transmission of a file with ABP or sliding window:

$$\Box\ (\text{send(file)} \Rightarrow \Diamond\ \text{receive(file)}\ )$$

Limitations of classical Model Checking

- Many times, correctness cannot be asserted qualitatively. Instead, the validity of a property can only be measured quantitatively
  - Bounded Retransmission Protocol in Philips RC6
  - Binary Exponential Backoff Algorithm in IEEE 802.3 “Ethernet”



Unrealistic assumption!

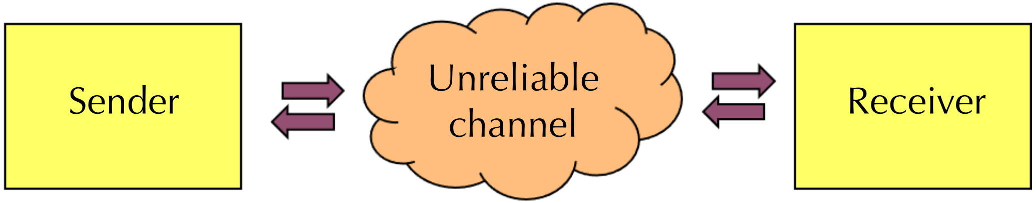
Suppose transmission of a file with ABP or sliding window:

$$\Box \, (\text{send}(\text{file}) \Rightarrow \Diamond \, \text{receive}(\text{file}) \,)$$

Holds, under the assumption of infinite retrials

Limitations of classical Model Checking

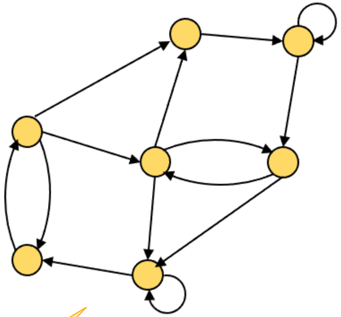
- Many times, correctness cannot be asserted qualitatively. Instead, the validity of a property can only be measured quantitatively
  - Bounded Retransmission Protocol in Philips RC6
  - Binary Exponential Backoff Algorithm in IEEE 802.3 “Ethernet”



If the protocol has a bounded number of retransmissions before aborting (e.g. BRP):

$$\xcancel{\Box\,(\mathrm{send}(\mathrm{file}) \Rightarrow \Diamond\,\mathrm{receive}(\mathrm{file})\,)}$$

Probabilistic Model Checking

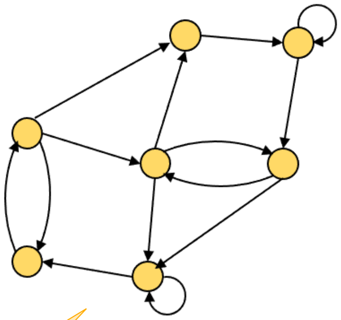


$\models \quad \Box\,(\mathrm{send(file)} \Rightarrow \Diamond\,\mathrm{receive(file)}\,)$

A graph representing nondeterministic behavior

Properties that represent boolean behavior on executions

Probabilistic Model Checking



$$\models \quad \Box\ (\text{send(file)} \Rightarrow \Diamond\ \text{receive(file)}\ )$$

A g

no

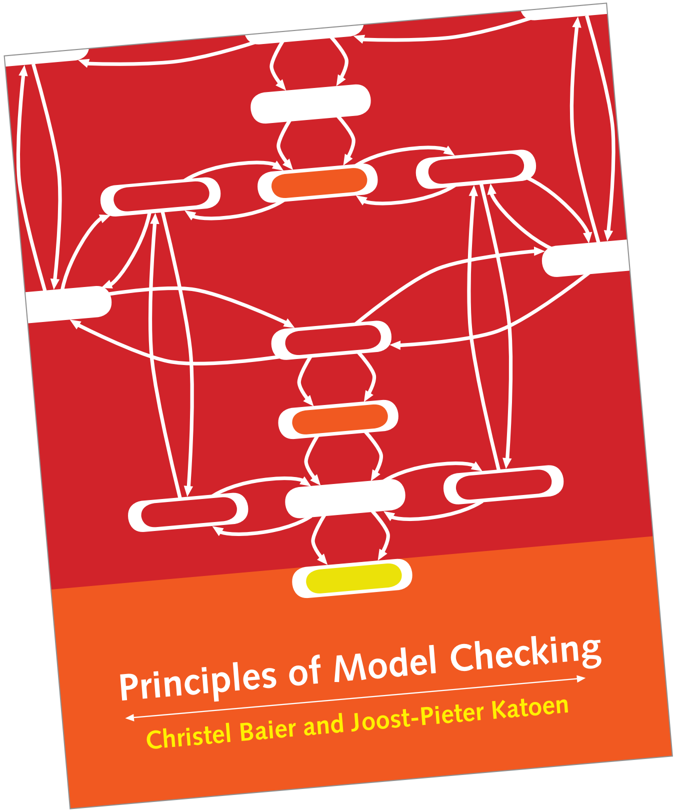
Probabilistic behavior should also be considered

Properties that

re ior on

It should also include a way to quantify probabilities

Before continuing, I must say:


Principles of Model Checking
Christel Baier and Joost-Pieter Katoen

The course borrows from Chapter 10 of

Principles of Model Checking by

Christel Baier & Joost-Pieter Katoen

published in 2008 by the MIT press

Markov Chains

Discrete Time Markov Chain (DTMC)

A DTMC is a structure

$$(S, \mathbf{P}, s_0, AP, L)$$

where

- ❖ S is a denumerable set of states, where $s_0 \in S$ is the initial state,
- ❖ $\mathbf{P} : S \times S \to [0,1]$ is the probabilistic transition function, such that, for every $s \in S$, $\sum_{s' \in S} \mathbf{P}(s, s') = 1$, and
- ❖ $L : S \to \mathscr{P}(AP)$ is a labelling function, where AP is a a set of atomic propositions.

Discrete Ti ov Chain (DTMC)

In model checking we only consider a finite set of states

A DTMC is a structure

$$(S, \mathbf{P}, s_0, AP, L)$$

$\mathbf{P}(s,s')$ is the probability to move to state s' conditioned to the system being at state s.

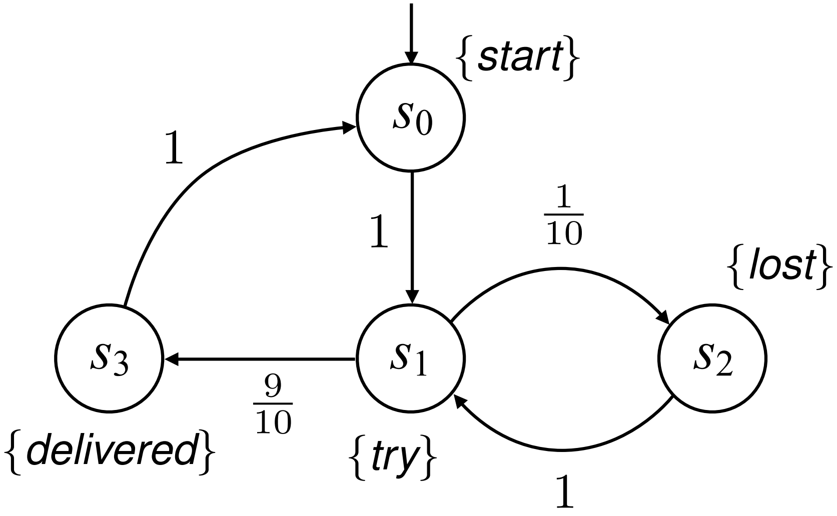
where

- ❖ S is a denumerable set of states, where $s_0 \in S$ is the initial state,
- ❖ $\mathbf{P} : S \times S \to [0,1]$ is the probabilistic transition function, such that, for every $s \in S$, $\sum_{s' \in S} \mathbf{P}(s,s') = 1$, and
- ❖ $L : S \to \mathscr{P}(AP)$ is a labelling function, where AP is a a set of atomic propositions.

CONICET

UNC

A toy protocol



$S = \{s_0, s_1, s_2, s_3\}$

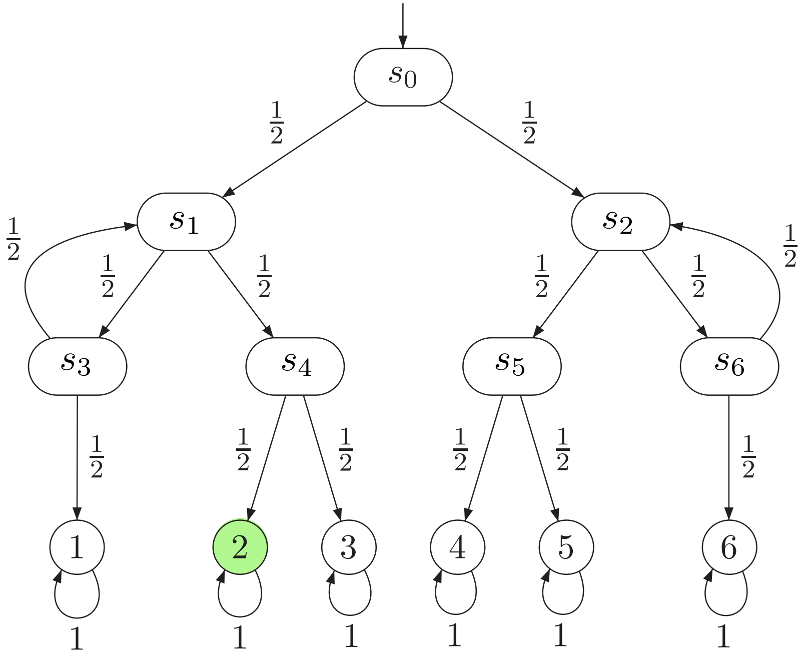
s_0 is the initial state

$$\mathbf{P} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{10} & \frac{9}{10} \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$AP = \{$*start*, *try*, *delivered*, *lost*$\}$

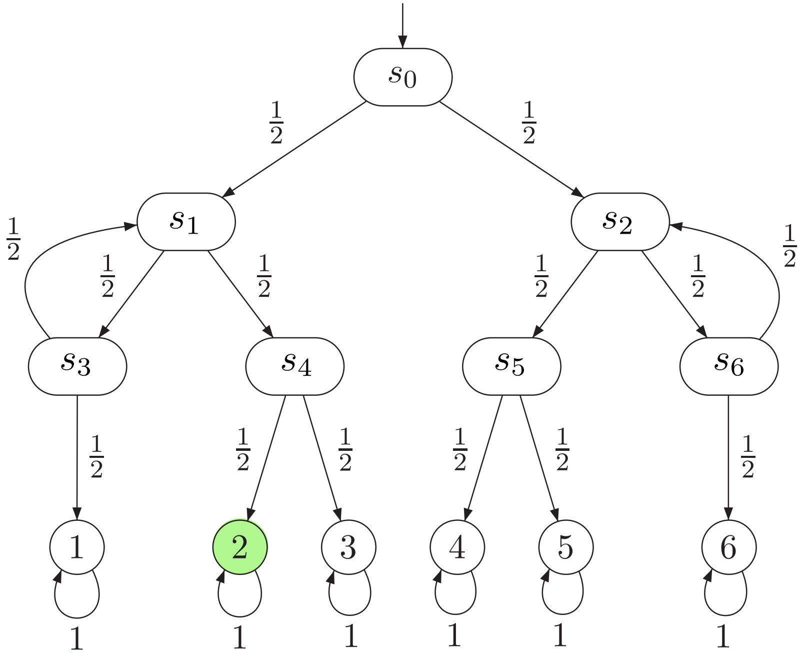
$L(s_0) = \{$*start*$\}$
$L(s_1) = \{$*try*$\}$
$L(s_2) = \{$*lost*$\}$
$L(s_3) = \{$*delivered*$\}$

Simulating a die with a coin



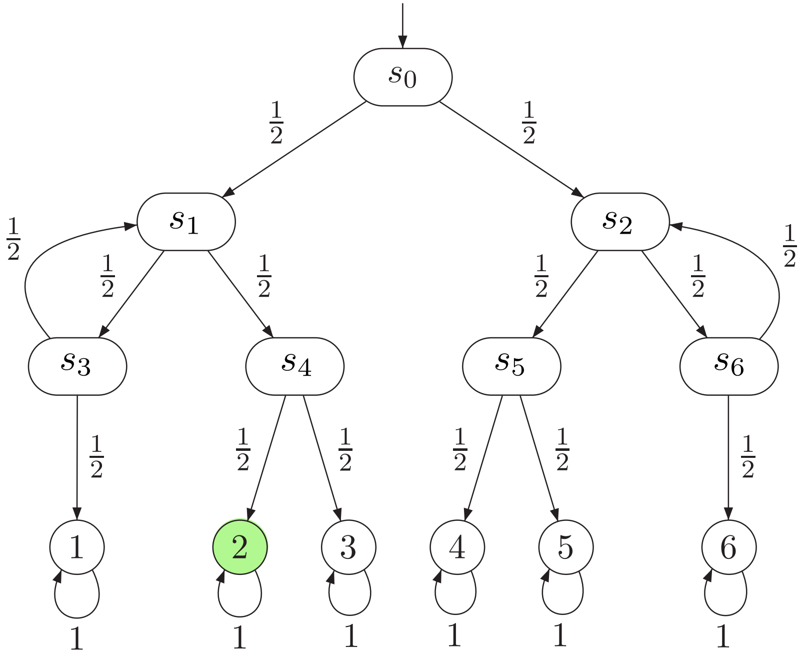
$P(\Diamond\, 2)$?

Simulating a die with a coin



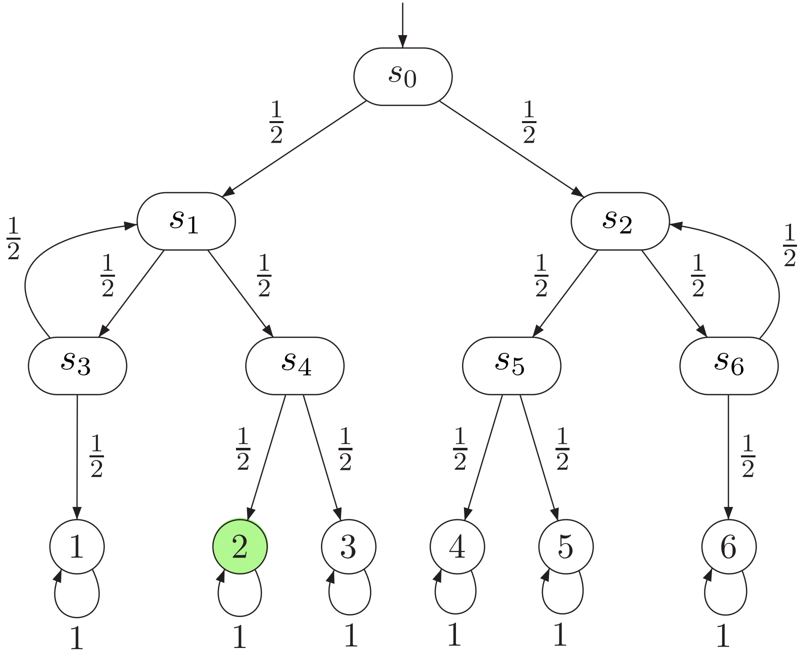
$$P(s_0 s_1 s_4 2) + P(s_0 s_1 s_3 s_1 s_4 2) + P(s_0 s_1 s_3 s_1 s_3 s_1 s_4 2) + P(s_0 s_1 s_3 s_1 s_3 s_1 s_3 s_1 s_4 2) + \cdots$$

Simulating a die with a coin



$$\underbrace{P(s_0 s_1 s_4 2)}_{\mathbf{P}(s_0,s_1)\cdot\mathbf{P}(s_1,s_4)\cdot\mathbf{P}(s_4,2)} + P(s_0 s_1 s_3 s_1 s_4 2) + P(s_0 s_1 s_3 s_1 s_3 s_1 s_4 2) + P(s_0 s_1 s_3 s_1 s_3 s_1 s_3 s_1 s_4 2) + \cdots$$

Simulating a die with a coin

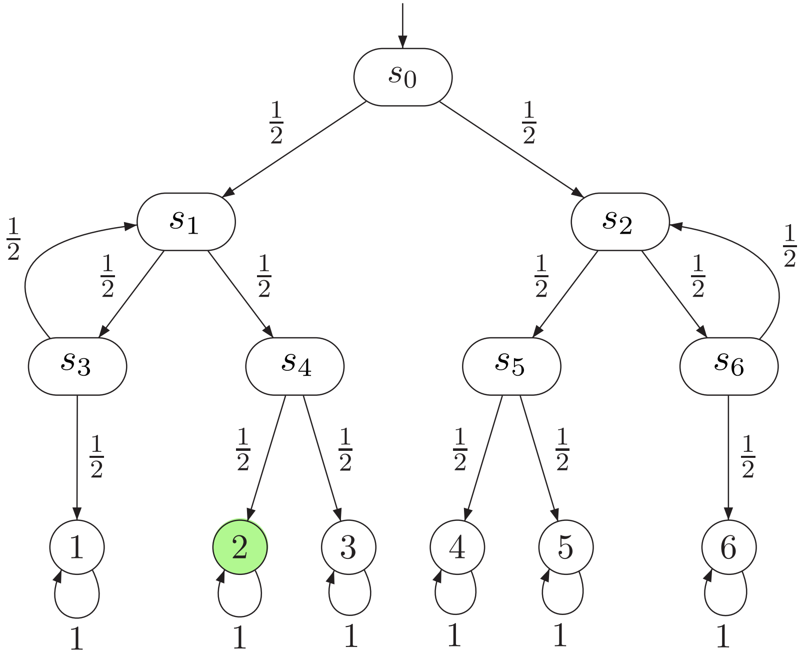


$$\underbrace{P(s_0s_1s_42)}_{\frac{1}{8}} + P(s_0s_1s_3s_1s_42) + P(s_0s_1s_3s_1s_3s_1s_42) + P(s_0s_1s_3s_1s_3s_1s_3s_1s_42) + \cdots$$

CONICET

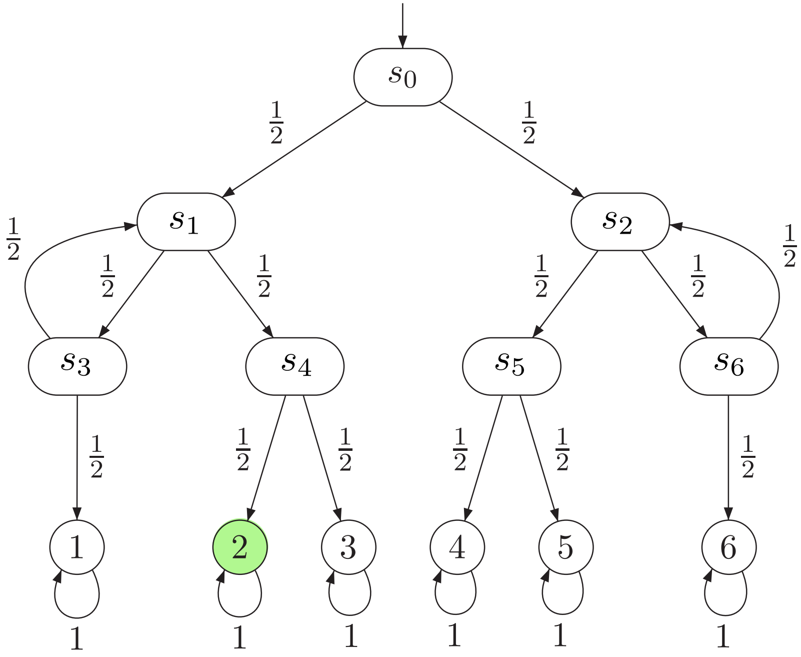
UNC

Simulating a die with a coin



$$\underbrace{P(s_0s_1s_42)}_{\frac{1}{8}} + \underbrace{P(s_0s_1s_3s_1s_42)}_{\frac{1}{32}} + \underbrace{P(s_0s_1s_3s_1s_3s_1s_42)}_{\frac{1}{128}} + \underbrace{P(s_0s_1s_3s_1s_3s_1s_3s_1s_42)}_{\frac{1}{512}} + \cdots$$

Simulating a die with a coin



How do we calculate this formally?

$$\underbrace{P(s_0 s_1 s_4 2)}_{\frac{1}{8}} + \underbrace{P(s_0 s_1 s_3 s_1 s_4 2)}_{\frac{1}{32}} + \underbrace{P(s_0 s_1 s_3 s_1 s_3 s_1 s_4 2)}_{\frac{1}{128}} + \underbrace{P(s_0 s_1 s_3 s_1 s_3 s_1 s_3 s_1 s_4 2)}_{\frac{1}{512}} + \cdots$$

Probability space defined by a DTMC

- The sample space is the set of all *plausible* infinite executions:

$$\Omega = S^\omega$$

- The σ-algebra is the one generated by the set of all *cylinders*, i.e., by all sets of the form

$$\mathit{Cyl}(\pi) = \{\rho \in S^\omega \mid \pi \text{ es prefijo de } \rho\}$$

where $\pi \in S^*$ is a *finite* sequence of states

- For each state $s \in S$ define the unique probability measure such that

$$\mathrm{Pr}_s(\mathit{Cyl}(s_1 s_2 \ldots s_n)) \;=\; \mathbf{1}_s(s_1) \cdot \mathbf{P}(s_1, s_2) \cdot \mathbf{P}(s_2, s_3) \cdots \mathbf{P}(s_{n-1}, s_n)$$

where $\mathbf{1}_s(s) = 1$ and $\mathbf{1}_s(t) = 0$ otherwise

Probability space defined by a DTMC

- The sample space is the set of all *plausible* infinite executions:

  $$\Omega = S^\omega$$

- The σ-algebra is the one generated by the set of all *cylinders*, i.e., by all sets of the form

  $$\mathit{Cyl}(\pi) = \{\rho \in S^\omega \mid \pi \text{ es prefijo de } \rho\}$$

  where $\pi \in S^*$ is a *finite* sequence of states

- For each state $s \in S$ define the unique probability measure such that

  $$\mathrm{Pr}_s(\mathit{Cyl}(s_1 s_2 \ldots s_n)) \;=\; \mathbf{1}_s(s_1) \cdot \mathbf{P}(s_1, s_2) \cdot \mathbf{P}(s_2, s_3) \cdots \mathbf{P}(s_{n-1}, s_n)$$

  where $\mathbf{1}_s(s) = 1$ and $\mathbf{1}_s(t) = 0$ otherwise

Probability space defined by a DTMC

- The sample space is the set of all *plausible* infinite executions:

$$\Omega = S^\omega$$

- The σ-algebra is the one generated by the set of all *cylinders*, i.e., by all sets of the form

$$\mathit{Cyl}(\pi) = \{\rho \in S^\omega \mid \pi \text{ es prefijo de } \rho\}$$

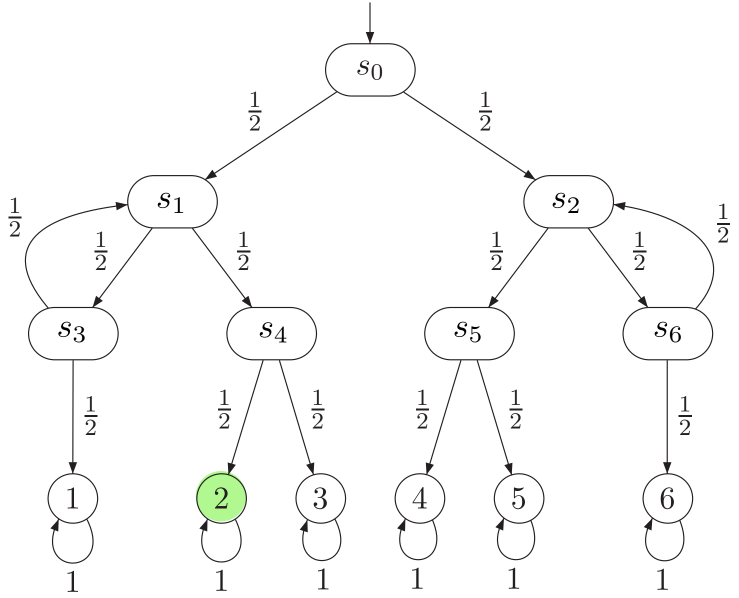
where $\pi \in S^*$ is a *finite* sequence of states

- For each state $s \in S$ define the unique probability measure such that

$$\mathrm{Pr}_s(\mathit{Cyl}(s_1 s_2 \dots s_n)) \;=\; \mathbf{1}_s(s_1) \cdot \mathbf{P}(s_1 s_2 s_3 \dots s_n)$$

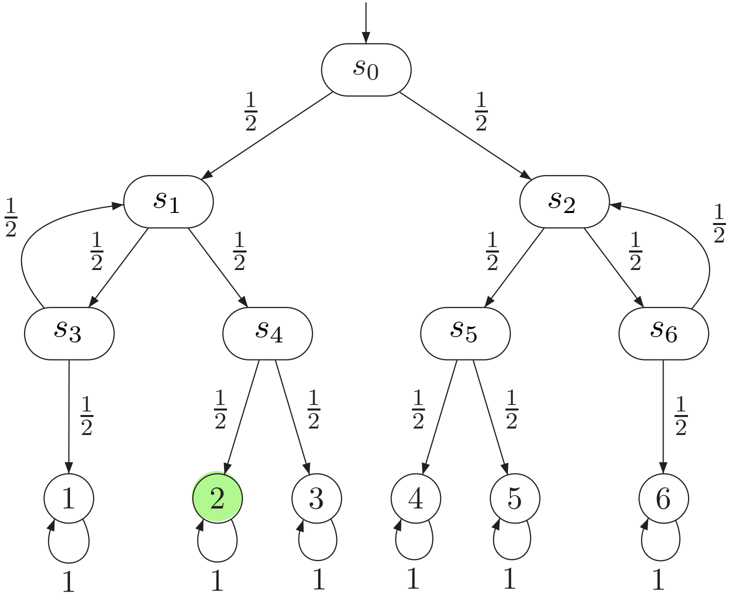
where $\mathbf{1}_s(s) = 1$ and $\mathbf{1}_s(t) = 0$ otherwise

Simulating a die with a coin



$$
\begin{aligned}
\Pr(\Diamond 2) &= \Pr(\{\rho \in S^\omega \mid \exists i \in \mathbb{N} : \rho(i) = 2\}) \\
&= \Pr(\bigcup\{\mathit{Cyl}(\pi) \mid \mathit{last}(\pi) = 2\}) \\
&= \Pr(\bigcup\{\mathit{Cyl}(\pi) \mid \pi \in s_0 s_1 (s_3 s_1)^* s_4 2\}) \\
&= \textstyle\sum_{n\in\mathbb{N}} \mathbf{P}(s_0 s_1 (s_3 s_1)^n s_4 2) \\
&= \textstyle\sum_{n\in\mathbb{N}} \frac{1}{2^{2n+3}} = \frac{1}{6}
\end{aligned}
$$

Simulating a die with a coin



$$\begin{aligned}
\Pr(\Diamond 2) &= \Pr(\{\rho \in S^\omega \mid \exists i \in \mathbb{N} : \rho(i) = 2\}) \\
&= \Pr(\bigcup\{\mathit{Cyl}(\pi) \mid \mathit{last}(\pi) = 2\}) \\
&= \Pr(\bigcup\{\mathit{Cyl}(\pi) \mid \pi \in s_0 s_1 (s_3 s_1)^* s_4 2\}) \\
&= \textstyle\sum_{n\in\mathbb{N}} \mathbf{P}(s_0 s_1 (s_3 s_1)^n s_4 2) \\
&= \textstyle\sum_{n\in\mathbb{N}} \frac{1}{2^{2n+3}} = \frac{1}{6}
\end{aligned}$$

But, how does the computer calculate this?

Quantitative reachability properties

Reachability properties

The probability of reaching a set of states B

$$\begin{aligned}\Pr_s(\Diamond B) &= \Pr_s(\{\rho \in S^\omega \mid \exists i \in \mathbb{N} : \rho(i) \in B\}) \\ &= \Pr_s(\bigcup\{\mathit{Cyl}(\pi) \mid \mathit{last}(\pi) \in B\}) \\ &= \sum_{s_0 \ldots s_n \in (S \setminus B)^* B} \mathbf{1}_s(s_0) \cdot \mathbf{P}(s_0 \ldots s_n)\end{aligned}$$

If $s \in B$ then

$$\Pr_s(\Diamond B) = 1$$

Reachability properties

If $s \notin B$

$$
\begin{aligned}
\Pr_s(\Diamond B) &= \sum_{s_0 \ldots s_n \in (S \setminus B)^* B} \mathbf{1}_s(s_0) \cdot \mathbf{P}(s_0 \ldots s_n) \\
&= \sum_{s_0 \ldots s_n \in (S \setminus B)^* B} \mathbf{1}_s(s_0) \cdot \prod_{i=0}^{n-1} \mathbf{P}(s_i, s_{i+1}) \\
&= \sum_{s_0 \ldots s_n \in (S \setminus B)^* B \wedge s_1 \notin B} \mathbf{1}_s(s_0) \cdot \prod_{i=0}^{n-1} \mathbf{P}(s_i, s_{i+1}) + \sum_{s_1 \in B} \mathbf{1}_s(s_0) \cdot \mathbf{P}(s_0, s_1) \\
&= \sum_{s_1 \ldots s_n \in (S \setminus B)^* B \wedge s_1 \notin B} \mathbf{P}(s, s_1) \cdot \prod_{i=1}^{n-1} \mathbf{P}(s_i, s_{i+1}) + \sum_{s_1 \in B} \mathbf{P}(s, s_1) \\
&= \sum_{s_1 \notin B} \mathbf{P}(s, s_1) \cdot \underbrace{\sum_{t_1 \ldots t_n \in (S \setminus B)^* B} \mathbf{1}_{s_1}(t_1) \cdot \prod_{i=1}^{n-1} \mathbf{P}(t_i, t_{i+1})}_{\Pr_{s_1}(\Diamond B)} + \sum_{s_1 \in B} \mathbf{P}(s, s_1)
\end{aligned}
$$

Reachability properties

If $s \notin B$

$$
\begin{aligned}
\mathrm{Pr}_s(\Diamond B) &= \sum_{s_0 \ldots s_n \in (S \setminus B)^* B} \mathbf{1}_s(s_0) \cdot \mathbf{P}(s_0 \ldots s_n) \\
&= \sum_{s_0 \ldots s_n \in (S \setminus B)^* B} \mathbf{1}_s(s_0) \cdot \prod_{i=0}^{n-1} \mathbf{P}(s_i, s_{i+1}) \\
&= \sum_{s_0 \ldots s_n \in (S \setminus B)^* B \wedge s_1 \notin B} \mathbf{1}_s(s_0) \cdot \prod_{i=0}^{n-1} \mathbf{P}(s_i, s_{i+1}) + \sum_{s_1 \in B} \mathbf{1}_s(s_0) \cdot \mathbf{P}(s_0, s_1) \\
&= \sum_{s_1 \ldots s_n \in (S \setminus B)^* B \wedge s_1 \notin B} \mathbf{P}(s, s_1) \cdot \prod_{i=1}^{n-1} \mathbf{P}(s_i, s_{i+1}) + \sum_{s_1 \in B} \mathbf{P}(s, s_1) \\
&= \sum_{s_1 \notin B} \mathbf{P}(s, s_1) \cdot \sum_{t_1 \ldots t_n \in (S \setminus B)^* B} \mathbf{1}_{s_1}(t_1) \cdot \prod_{i=1}^{n-1} \mathbf{P}(t_i, t_{i+1}) + \sum_{s_1 \in B} \mathbf{P}(s, s_1) \\
&= \sum_{s_1 \notin B} \mathbf{P}(s, s_1) \cdot \mathrm{Pr}_{s_1}(\Diamond B) + \sum_{s_1 \in B} \mathbf{P}(s, s_1)
\end{aligned}
$$

Reachability properties

If $s \notin B$

$$
\begin{aligned}
\boxed{\mathrm{Pr}_s(\Diamond B)} &= \sum_{s_0 \dots s_n \in (S \setminus B)^* B} \mathbf{1}_s(s_0) \cdot \mathbf{P}(s_0 \dots s_n) \\
&= \sum_{s_0 \dots s_n \in (S \setminus B)^* B} \mathbf{1}_s(s_0) \cdot \prod_{i=0}^{n-1} \mathbf{P}(s_i, s_{i+1}) \\
&= \sum_{s_0 \dots s_n \in (S \setminus B)^* B \wedge s_1 \notin B} \mathbf{1}_s(s_0) \cdot \prod_{i=0}^{n-1} \mathbf{P}(s_i, s_{i+1}) + \sum_{s_1 \in B} \mathbf{1}_s(s_0) \cdot \mathbf{P}(s_0, s_1) \\
&= \sum_{s_1 \dots s_n \in (S \setminus B)^* B \wedge s_1 \notin B} \mathbf{P}(s, s_1) \cdot \prod_{i=1}^{n-1} \mathbf{P}(s_i, s_{i+1}) + \sum_{s_1 \in B} \mathbf{P}(s, s_1) \\
&= \sum_{s_1 \notin B} \mathbf{P}(s, s_1) \cdot \sum_{t_1 \dots t_n \in (S \setminus B)^* B} \mathbf{1}_{s_1}(t_1) \cdot \prod_{i=1}^{n-1} \mathbf{P}(t_i, t_{i+1}) + \sum_{s_1 \in B} \mathbf{P}(s, s_1) \\
&= \sum_{s_1 \notin B} \mathbf{P}(s, s_1) \cdot \boxed{\mathrm{Pr}_{s_1}(\Diamond B)} + \sum_{s_1 \in B} \mathbf{P}(s, s_1)
\end{aligned}
$$

CONICET

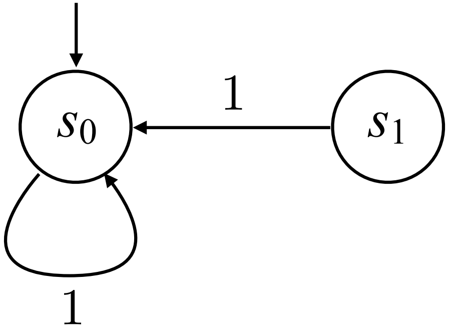
UNC

Reachability properties

The following set of equations is obtained (one for each $s \notin B$)

$$x_s = \sum_{t \notin B} \mathbf{P}(s,t) \cdot x_t + \sum_{t \in B} \mathbf{P}(s,t)$$

Be aware! The system of equations may not have unique solution:



if $B = \{s_1\}$, the system of equations only contains equation:

$$x_{s_0} = x_{s_0}$$

which has infinite solutions

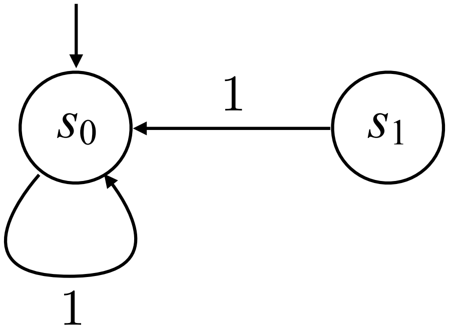
Reachability properties

Note that the only interesting states are those reaching B (otherwise the reachability probability is 0)

The following set of equations is obtained (one for each $s \notin B$

$$x_s = \sum_{t \notin B} \mathbf{P}(s,t) \cdot x_t + \sum_{t \in B} \mathbf{P}(s,t)$$

Be aware! The system of equations may not have unique solution:



if $B = \{s_1\}$, the system of equations only contains equation:

$$x_{s_0} = x_{s_0}$$

which has infinite solutions

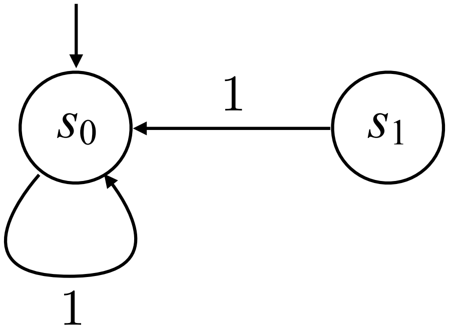
Reachability properties

Note that the only interesting states are those reaching B (otherwise the reachability probability is 0)

The following set of equations is obtained (one for each $s \notin$

$$x_s = \sum_{t \in Pre^*(B) \setminus B} \mathbf{P}(s,t) \cdot x_t + \sum_{t \in B} \mathbf{P}(s,t)$$

Be aware! The system of equations may not have unique solution:



if $B = \{s_1\}$, the system of equations only contains equation:

$$x_{s_0} = x_{s_0}$$

which has infinite solutions

CONICET

UNC

$Pre^*(B) = \{s \in S \mid \Pr_s(\Diamond B) > 0\}$
is the set of all states that may reach B.
It is calculated by graph analysis

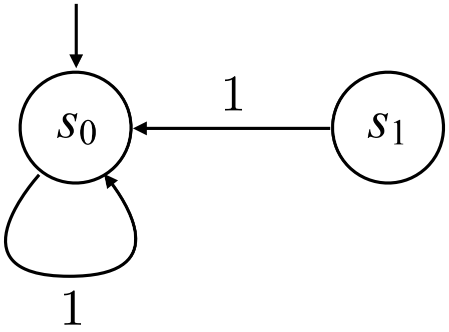
chability properties

Note that the only interesting states are those reaching B (otherwise the reachability probability is 0)

The following s of equations is obtained (one for each $s \notin$

$$x_s = \sum_{t \in Pre^*(B) \setminus B} \mathbf{P}(s,t) \cdot x_t + \sum_{t \in B} \mathbf{P}(s,t)$$

Be aware! The system of equations may not have unique solution:



if $B = \{s_1\}$, the system of equations only contains equation:

$$x_{s_0} = x_{s_0}$$

which has infinite solutions

Reachability properties

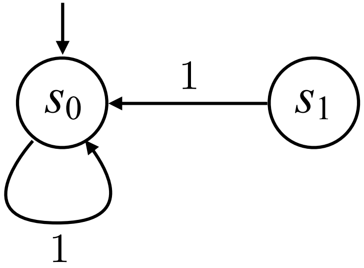
The complete system of equations is defined by:

$$x_s = \sum_{t \in \mathit{Pre}^*(B) \backslash B} \mathbf{P}(s,t) \cdot x_t + \sum_{t \in B} \mathbf{P}(s,t) \qquad \text{if } s \in \mathit{Pre}^*(B) \backslash B$$

$$x_s = 1 \qquad \text{if } s \in B$$

$$x_s = 0 \qquad \text{if } s \notin \mathit{Pre}^*(B) \cup B$$

For the example, the system of equations is



$$x_{s_0} = 0$$

$$x_{s_1} = 1$$

This system of equations has a unique solution

Reachability properties

Calculated using techniques like Gaussian elimination, Jacobi or Gauss-Seidel

Computed in polynomial time

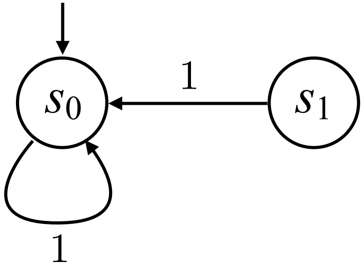
The complete system of equations is defined by:

$$x_s = \sum_{t \in Pre^*(B)\setminus B} \mathbf{P}(s,t) \cdot x_t + \sum_{t \in B} \mathbf{P}(s,t) \qquad \text{if } s \in Pre^*(B)\setminus B$$

$$x_s = 1 \qquad \text{if } s \in B$$

$$x_s = 0 \qquad \text{if } s \notin Pre^*(B) \cup B$$

For the example, the system of equations is

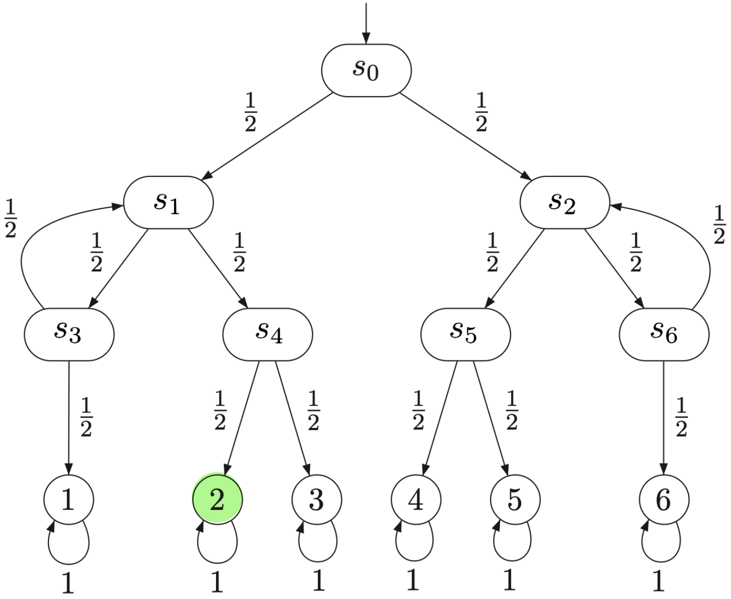


$$x_{s_0} = 0$$

$$x_{s_1} = 1$$

This system of equations has a unique solution

Simulating a die with a coin



$$x_s = \sum_{t \in Pre^*(B)\setminus B} \mathbf{P}(s,t) \cdot x_t + \sum_{t \in B} \mathbf{P}(s,t) \qquad \text{if } s \in Pre^*(B)\setminus B$$

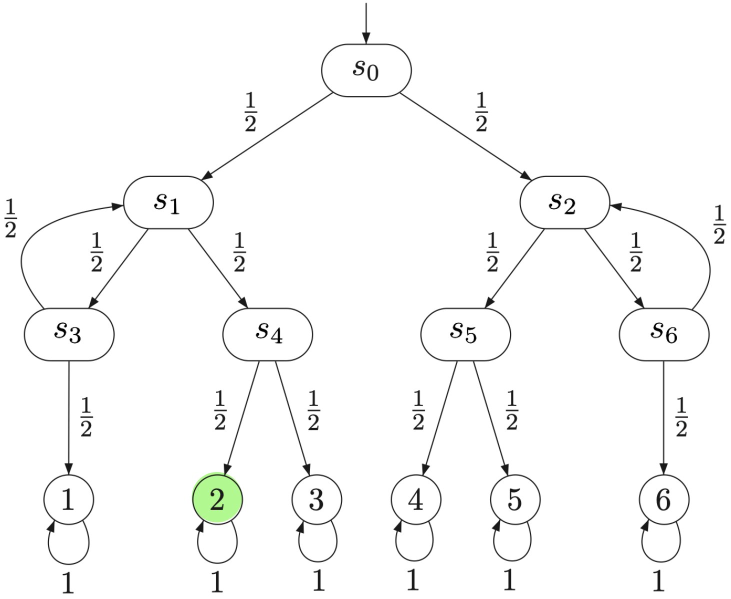
$$x_s = 1 \qquad \text{if } s \in B$$

$$x_s = 0 \qquad \text{if } s \notin Pre^*(B) \cup B$$

CONICET

UNC

Simulating a die with a coin



$$x_2 = 1$$

B

$$x_s = \sum_{t \in Pre^*(B) \setminus B} \mathbf{P}(s,t) \cdot x_t + \sum_{t \in B} \mathbf{P}(s,t) \qquad \text{if } s \in Pre^*(B) \setminus B$$

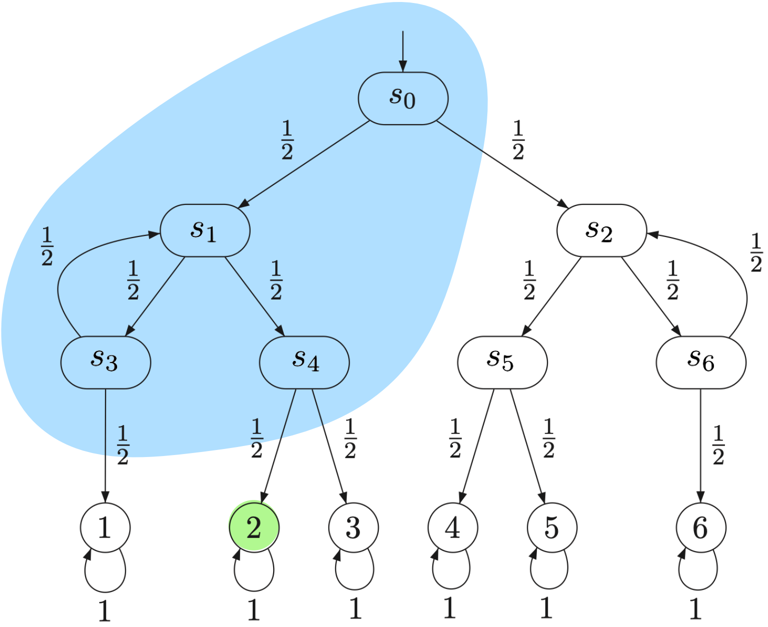
$$x_s = 1 \qquad \text{if } s \in B$$

$$x_s = 0 \qquad \text{if } s \notin Pre^*(B) \cup B$$

CONICET

UNC

Simulating a die with a coin



Pre$^*(B) \setminus B$

$$x_{s_0} = \frac{1}{2} \cdot x_{s_1}$$

$$x_{s_1} = \frac{1}{2} \cdot x_{s_3} + \frac{1}{2} \cdot x_{s_4}$$

$$x_{s_3} = \frac{1}{2} \cdot x_{s_1}$$

$$x_{s_4} = \frac{1}{2}$$

B

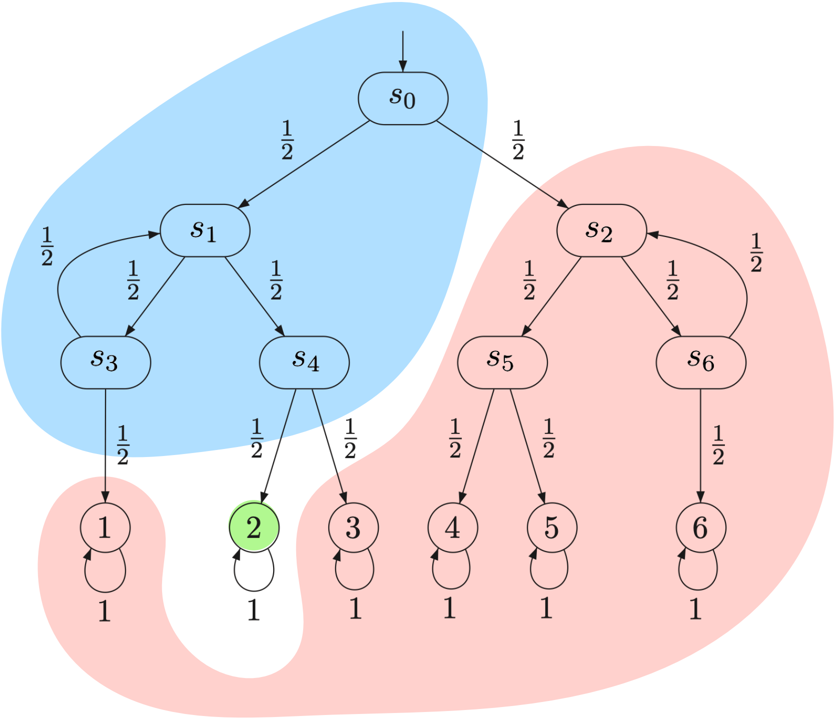
$$x_2 = 1$$

$x_s = \sum_{t \in Pre^*(B) \setminus B} \mathbf{P}(s,t) \cdot x_t + \sum_{t \in B} \mathbf{P}(s,t)$	if $s \in Pre^*(B) \setminus B$
$x_s = 1$	if $s \in B$
$x_s = 0$	if $s \notin Pre^*(B) \cup B$

CONICET

UNC

Simulating a die with a coin



$Pre^*(B) \setminus B$

$$x_{s_0} = \frac{1}{2} \cdot x_{s_1}$$

$$x_{s_1} = \frac{1}{2} \cdot x_{s_3} + \frac{1}{2} \cdot x_{s_4}$$

$$x_{s_3} = \frac{1}{2} \cdot x_{s_1}$$

$$x_{s_4} = \frac{1}{2}$$

B

$$x_2 = 1$$

$S \setminus Pre^*(B)$

$$x_s = 0\ , \qquad \text{if } s \notin \{s_0, s_1, s_3, s_4, 2\}$$

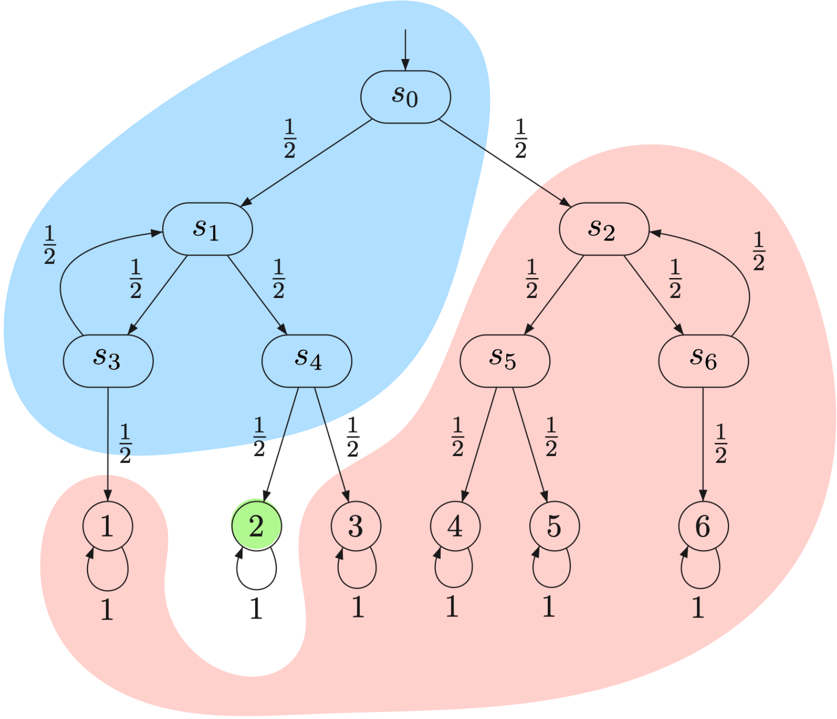
$$x_s = \sum_{t \in Pre^*(B) \setminus B} \mathbf{P}(s,t) \cdot x_t + \sum_{t \in B} \mathbf{P}(s,t) \qquad \text{if } s \in Pre^*(B) \setminus B$$

$$x_s = 1 \qquad \text{if } s \in B$$

$$x_s = 0 \qquad \text{if } s \notin Pre^*(B) \cup B$$

Simulating a die with a coin

It's up to you to check that indeed $x_{s_0} = \frac{1}{6}$



Pre$^*(B) \setminus B$

$$x_{s_0} = \frac{1}{2} \cdot x_{s_1}$$

$$x_{s_1} = \frac{1}{2} \cdot x_{s_3} + \frac{1}{2} \cdot x_{s_4}$$

$$x_{s_3} = \frac{1}{2} \cdot x_{s_1}$$

$$x_{s_4} = \frac{1}{2}$$

B

$$x_2 = 1$$

$S \setminus \mathit{Pre}^*(B)$

$$x_s = 0\ , \qquad \text{if } s \notin \{s_0, s_1, s_3, s_4, 2\}$$

$$x_s = \begin{cases} \displaystyle\sum_{t \in \mathit{Pre}^*(B) \setminus B} \mathbf{P}(s,t) \cdot x_t + \sum_{t \in B} \mathbf{P}(s,t) & \text{if } s \in \mathit{Pre}^*(B) \setminus B \\ x_s = 1 & \text{if } s \in B \\ x_s = 0 & \text{if } s \notin \mathit{Pre}^*(B) \cup B \end{cases}$$

CONICET

UNC

Bounded reachability

(exact: $\mathrm{Pr}_{s_0}(\Diamond^{=n} B)$)

- The probability transition function $\mathbf{P}$ defines the probability of moving from one state to another in one single step
- Then the probability of moving from s to t in two steps is

$$\sum_{s \in S} \mathbf{P}(s, s') \cdot \mathbf{P}(s', t) = (\mathbf{P} \cdot \mathbf{P})(s, t) = \mathbf{P}^2(s, t)$$

Bounded reachability

(exact: $\Pr_{s_0}(\Diamond^{=n} B)$)

- The probability transition function **P** defines the probability of moving from one state to another in one single step
- Then the probability of moving from s to t in two steps is

P is a matrix!

$$\sum_{s \in S} \mathbf{P}(s, s') \cdot \mathbf{P}(s', t) = (\mathbf{P} \cdot \mathbf{P})(s, t) = \mathbf{P}^2(s, t)$$

- In general, the probability of reaching t on n steps from the initial state is:

$$\Theta_n(t) = \mathbf{P}^n(s_0, t)$$

- Then, the probability of reaching a state in B in exactly n steps is

$$\Pr_{s_0}(\Diamond^{=n} B) = \sum_{t \in B} \Theta_n(t)$$

… so, this is calculated with matrix multiplication

Bounded reachability
(upper bound)

- Given the DTMC *M* construct the DTMC M_B by making all states in *B* absorbing:

$$\mathbf{P}_{M_B}(s,t) = \begin{cases} 1 & \text{if } t = s \in B \\ 0 & \text{if } t \neq s \in B \\ \mathbf{P}_M(s,t) & \text{if } s \notin B \end{cases}$$

- Then calculate

$$\Pr_{s_0}^{M}(\Diamond^{\leq n} B) = \Pr_{s_0}^{M_B}(\Diamond^{=n} B) = \sum_{t \in B} \Theta_n^{M_B}(t)$$

Constrained reachability

(until operator)

- The probability of reaching states in *B* passing only through states in *C*:

$$\mathrm{Pr}_{s_0}(C \,\mathtt{U}\, B) \qquad \underbrace{\mathrm{Pr}_{s_0}(C \,\mathtt{U}^{=n}\, B) \qquad \mathrm{Pr}_{s_0}(C \,\mathtt{U}^{\leq n}\, B)}_{\text{bounded versions}}$$

Constrained reachability
(until operator)

- The probability of reaching states in *B* passing only through states in *C*:

$$\Pr_{s_0}(C \,\mathtt{U}\, B) \qquad \Pr_{s_0}(C \,\mathtt{U}^{=n}\, B) \qquad \Pr_{s_0}(C \,\mathtt{U}^{\leq n}\, B)$$

- Construct the DTMC *M*$^{\mathtt{U}}$ from *M* by making states not in *C* ∪ *B* absorbing:

$$\mathbf{P}_{M^{\mathtt{U}}}(s,t) = \begin{cases} 1 & \text{if } t = s \notin (C \cup B) \\ 0 & \text{if } t \neq s \notin (C \cup B) \\ \mathbf{P}_M(s,t) & \text{if } s \in (C \cup B) \end{cases}$$

- Then calculate:

$$\Pr_{s_0}^{M}(C \,\mathtt{U}\, B) = \Pr_{s_0}^{M^{\mathtt{U}}}(\Diamond B)$$

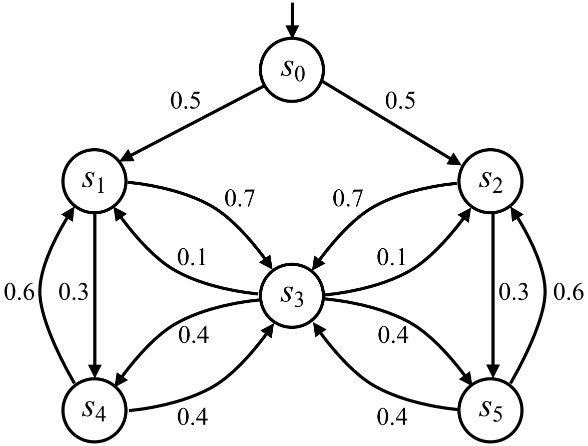
$$\Pr_{s_0}^{M}(C \,\mathtt{U}^{=n}\, B) = \Pr_{s_0}^{M^{\mathtt{U}}}(\Diamond^{=n} B)$$

$$\Pr_{s_0}^{M}(C \,\mathtt{U}^{\leq n}\, B) = \Pr_{s_0}^{M^{\mathtt{U}}}(\Diamond^{\leq n} B)$$

CONICET

UNC

Constrained reachability

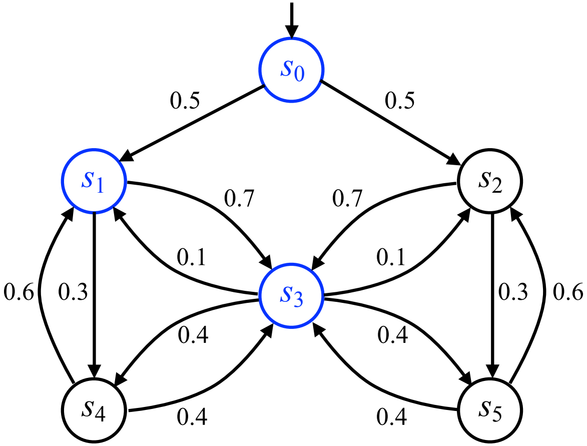


Let $C = \{s_0, s_1, s_3\}$

and $B = \{s_4\}$

$\Pr_{s_0}(C \, \mathtt{U}^{=4} \, B)$?

Constrained reachability

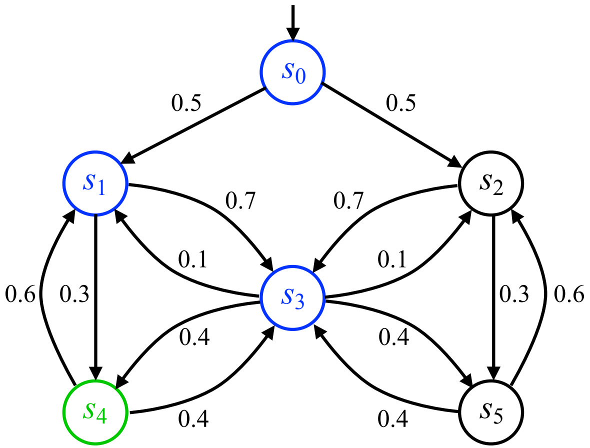


Let $C = \{s_0, s_1, s_3\}$

and $B = \{s_4\}$

$\Pr_{s_0}(C \, \mathtt{U}^{=4} \, B)$?

Constrained reachability

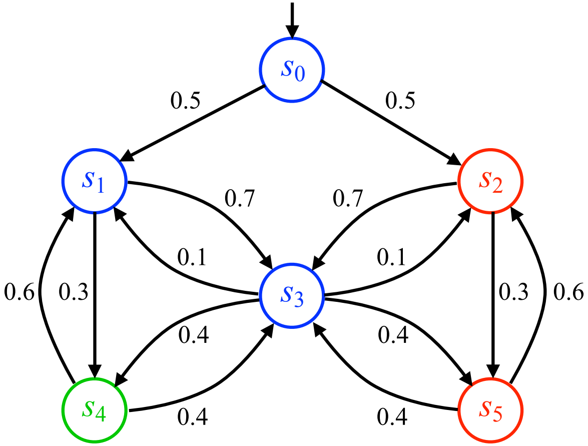


Let $C = \{s_0, s_1, s_3\}$

and $B = \{s_4\}$

$\Pr_{s_0}(C \,\mathsf{U}^{=4}\, B)$?

Constrained reachability

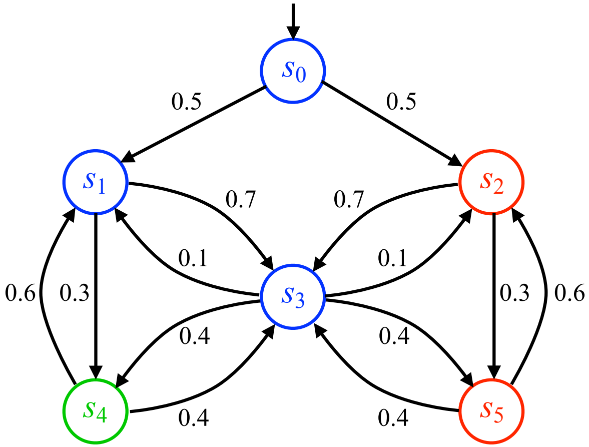


Let $C = \{s_0, s_1, s_3\}$

and $B = \{s_4\}$

$\Pr_{s_0}(C \, \mathsf{U}^{=4} \, B)$?

Constrained reachability



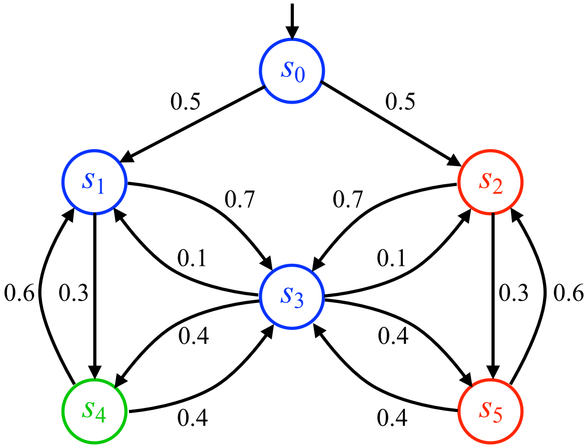
Let $C = \{s_0, s_1, s_3\}$

and $B = \{s_4\}$

$\Pr_{s_0}(C \, \mathtt{U}^{=4} \, B)$?

1) Calculate $M^{\mathtt{U}}$

Constrained reachability



Let $C = \{s_0, s_1, s_3\}$

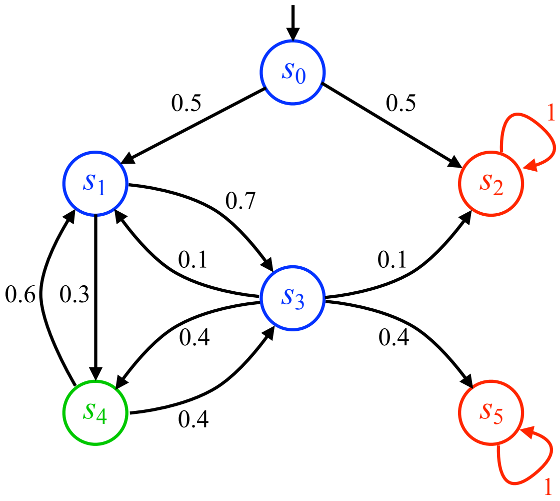
and $B = \{s_4\}$

$\Pr_{s_0}(C \, \mathtt{U}^{=4} \, B)$?

1) Calculate $M^{\mathtt{U}}$

i.e. make states not in C or B absorbing

Constrained reachability



Let $C = \{s_0, s_1, s_3\}$

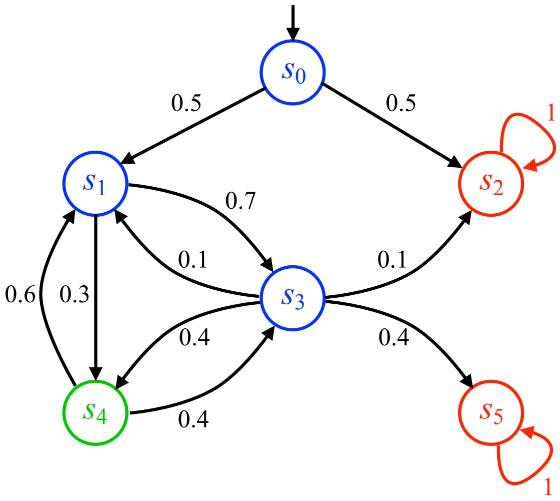
and $B = \{s_4\}$

$\Pr_{s_0}(C \, \mathtt{U}^{=4} \, B)$?

1) Calculate $M^{\mathtt{U}}$

i.e. make states not in *C* or *B* absorbing

Constrained reachability



Let $C = \{s_0, s_1, s_3\}$

and $B = \{s_4\}$

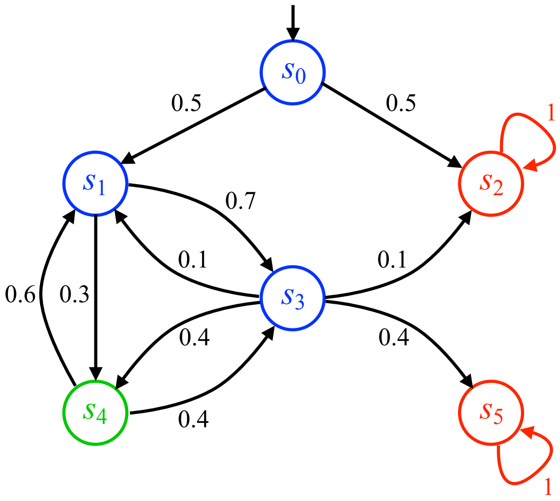
$\Pr_{s_0}(C \, \mathtt{U}^{=4} \, B)$?

1) Calculate $M^{\mathtt{U}}$

2) Calculate $\Pr^{M^{\mathtt{U}}}_{s_0}(\Diamond^{=4} B)$

i.e. make states not in C or B absorbing

Constrained reachability



Let $C = \{s_0, s_1, s_3\}$

and $B = \{s_4\}$

$\Pr_{s_0}(C \, \mathsf{U}^{=4} \, B)$?

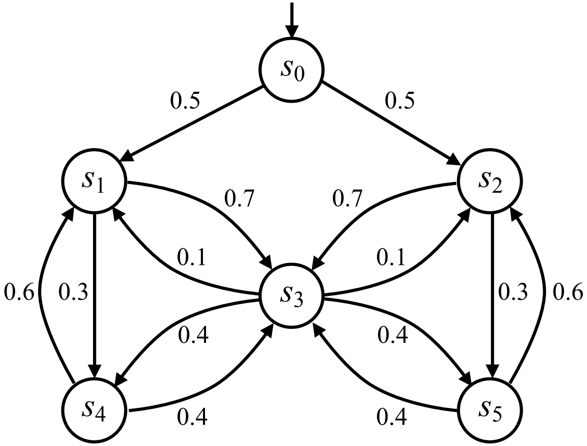
1) Calculate M^{U}

2) Calculate $\Pr^{M^{\mathsf{U}}}_{s_0}(\Diamond^{=4} B)$

i.e. make states not in C or B absorbing

Notice that $\Pr_{s_0}(C \, \mathsf{U} \, B)$ can be obtained in this DTMC by calculating $\Pr^{M^{\mathsf{U}}}_{s_0}(\Diamond B)$ instead

Constrained reachability

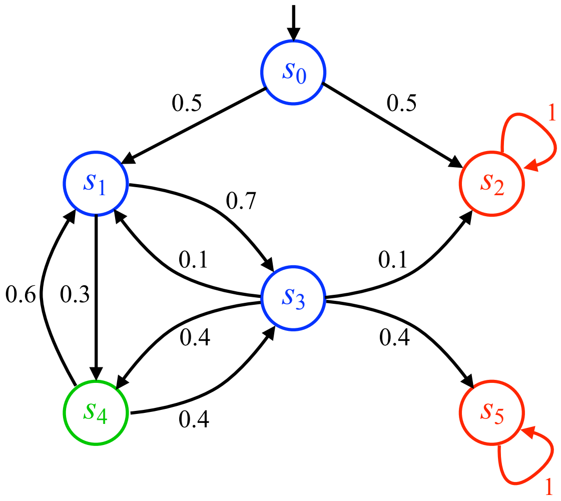


Let $\quad C = \{s_0, s_1, s_3\}$

and $\quad B = \{s_4\}$

$\Pr_{s_0}(C \, \mathsf{U}^{\leq 4} \, B)$?

Constrained reachability



Let $C = \{s_0, s_1, s_3\}$

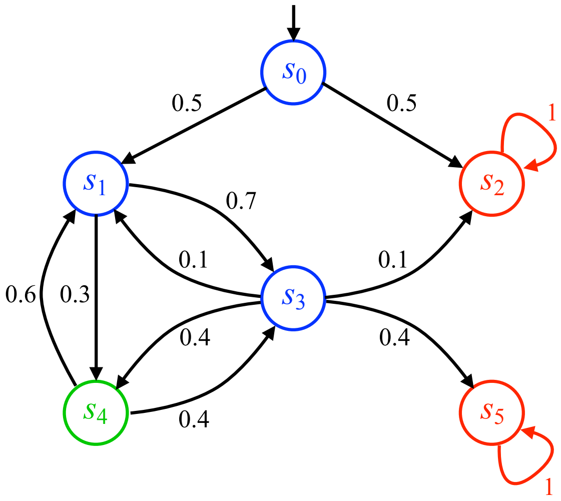
and $B = \{s_4\}$

$\Pr_{s_0}(C \, \mathtt{U}^{\leq 4} \, B)$?

1) Calculate $M^{\mathtt{U}}$

i.e. make states not in C or B absorbing

Constrained reachability



Let $C = \{s_0, s_1, s_3\}$

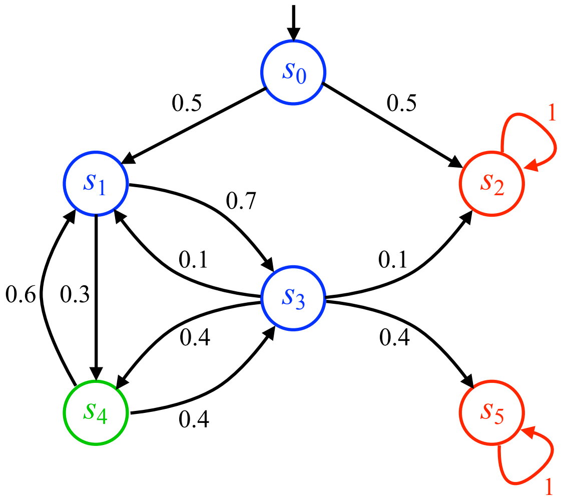
and $B = \{s_4\}$

$\Pr_{s_0}(C \, \mathtt{U}^{\leq 4} \, B)$?

1) Calculate $M^{\mathtt{U}}$

2) Calculate $M^{\mathtt{U}}_{B}$

Constrained reachability



i.e. make states in B absorbing

Let $C = \{s_0, s_1, s_3\}$

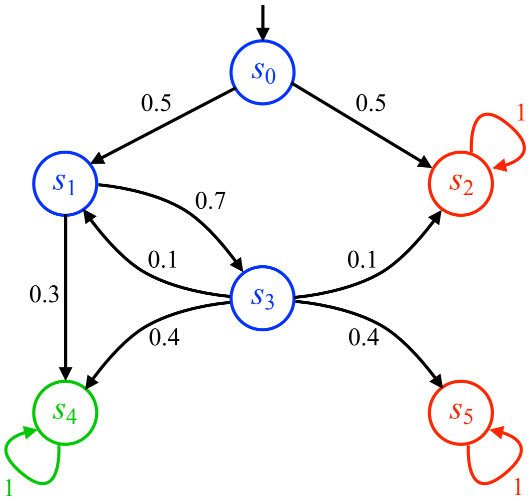
and $B = \{s_4\}$

$\Pr_{s_0}(C \mathtt{U}^{\leq 4} B)$?

1) Calculate $M^{\mathtt{U}}$

2) Calculate $M_B^{\mathtt{U}}$

Constrained reachability



Let $C = \{s_0, s_1, s_3\}$

and $B = \{s_4\}$

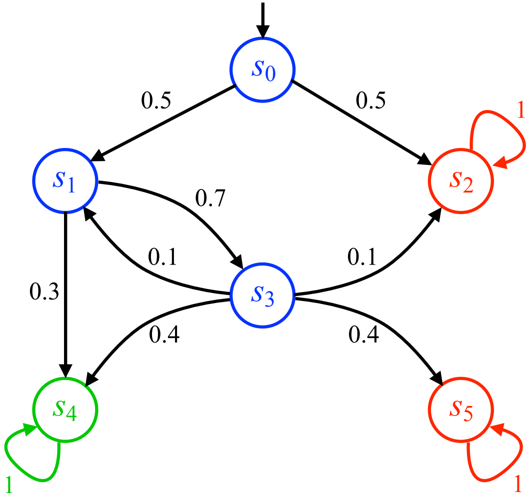
$\Pr_{s_0}(C \,\mathtt{U}^{\leq 4}\, B)$?

1) Calculate $M^{\mathtt{U}}$

2) Calculate $M^{\mathtt{U}}_B$

i.e. make states in B absorbing

Constrained reachability



i.e. make states in B absorbing

Let $C = \{s_0, s_1, s_3\}$

and $B = \{s_4\}$

$\Pr_{s_0}(C \, \mathtt{U}^{\leq 4} \, B)$?

1) Calculate $M^{\mathtt{U}}$

2) Calculate $M^{\mathtt{U}}_B$

3) Calculate $\Pr^{M^{\mathtt{U}}_B}_{s_0}(\Diamond^{=4} B)$

Qualitative properties

Qualitative properties

- These properties deal with extreme probabilities:
  - something happens with probability 1, or
  - something happens with some probability (different from 0)
- We focus on:
  - reachability ($\Diamond B$)
  - constrained reachability ($C \cup B$)
  - repeated reachability ($\Box\Diamond B$) → states in B are visited infinitely often
  - persistence ($\Diamond\Box B$) → reach SCCs that contain only states in B
- All these properties can be verified by doing graph analysis on the underlying graph of the DTMC

Qualitative properties

- These properties deal with extreme probabilities:
  - something happens with probability 1, or
  - something happens with some probability (different from 0)

Dually: something happens with probability 0

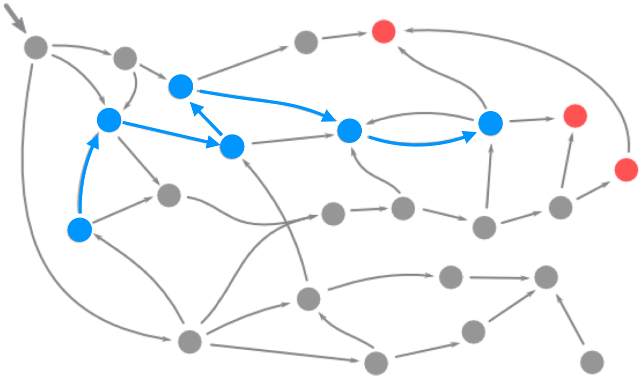
All these properties can be proved measurable

- We focus on:
  - reachability ($\Diamond B$)
  - constrained reachability ($C \cup B$)
  - repeated reachability ($\Box\Diamond B$) → states in B are visited infinitely often
  - persistence ($\Diamond\Box B$) → reach SCCs that contain only states in B
- All these properties can be verified by doing graph analysis on the underlying graph of the DTMC

Reachability (with some probability)

An execution fragment is a sequence $s_0\, s_1\, s_2\, \ldots s_n \in S^*$ such that $\mathbf{P}(s_0\, s_1\, s_2\, \ldots s_n) > 0$, that is, $\mathbf{P}(s_i, s_{i+1}) > 0$ for all $0 \leq i < n$.

$\mathit{Path}_{\mathit{fin}}(s)$ is the set of all execution fragments starting in the state s.



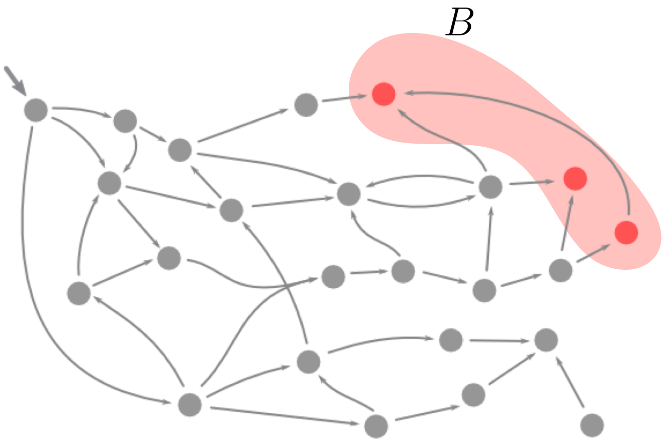
Reachability (with some probability)

An execution fragment is a sequence $s_0\, s_1\, s_2\, \ldots s_n \in S^*$ such that $\mathbf{P}(s_0\, s_1\, s_2\, \ldots s_n) > 0$, that is, $\mathbf{P}(s_i, s_{i+1}) > 0$ for all $0 \leq i < n$.

$\mathit{Path}_{\mathit{fin}}(s)$ is the set of all execution fragments starting in the state s.

The (immediate) predecesors of a set of states $B \subseteq S$ is defined by

$$Pre(B) = \{s \mid \exists t \in B \colon \mathbf{P}(s,t) > 0\}$$



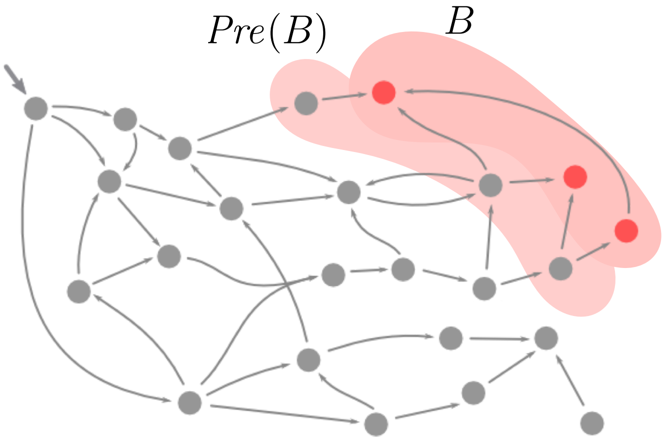
Reachability (with some probability)

An execution fragment is a sequence $s_0\, s_1\, s_2\, \ldots s_n \in S^*$ such that $\mathbf{P}(s_0\, s_1\, s_2\, \ldots s_n) > 0$, that is, $\mathbf{P}(s_i, s_{i+1}) > 0$ for all $0 \leq i < n$.

$\mathit{Path}_{\mathit{fin}}(s)$ is the set of all execution fragments starting in the state s.

The (immediate) predecesors of a set of states $B \subseteq S$ is defined by

$$\mathit{Pre}(B) = \{s \mid \exists t \in B \colon \mathbf{P}(s,t) > 0\}$$



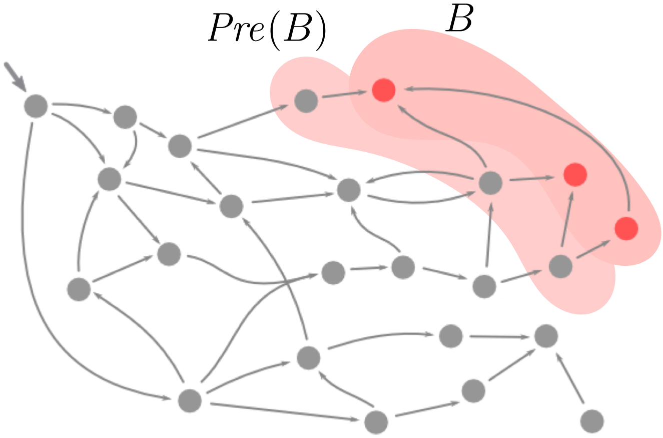
Reachability (with some probability)

An execution fragment is a sequence $s_0\, s_1\, s_2\ \ldots s_n \in S^*$ such that $\mathbf{P}(s_0\, s_1\, s_2\ \ldots s_n) > 0$, that is, $\mathbf{P}(s_i, s_{i+1}) > 0$ for all $0 \leq i < n$.

$\mathit{Path}_{\mathit{fin}}(s)$ is the set of all execution fragments starting in the state s.

The (immediate) predecesors of a set of states $B \subseteq S$ is defined by

$$\mathit{Pre}(B) = \{s \mid \exists t \in B \colon \mathbf{P}(s,t) > 0\}$$



Then, is the set of states reaching B is defined by

$$\mathit{Pre}^*(B) = \bigcup_{i \geq 0} \mathit{Pre}^i(B) = \{s \in S \mid \exists \pi \in \mathit{Path}_{\mathit{fin}}(s) \colon \mathit{last}(\pi) \in B\}$$

Reachability (with some probability)

An execution fragment is a sequence $s_0\, s_1\, s_2\, \ldots s_n \in S^*$ such that $\mathbf{P}(s_0\, s_1\, s_2\, \ldots s_n) > 0$, that is, $\mathbf{P}(s_i, s_{i+1}) > 0$ for all $0 \leq i < n$.

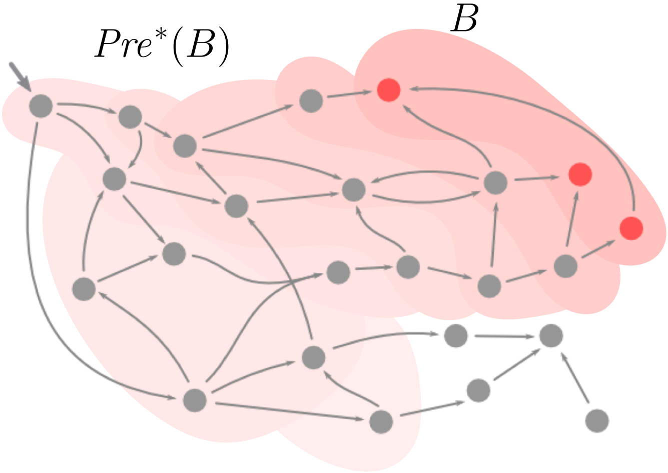
$\mathit{Path}_{\mathit{fin}}(s)$ is the set of all execution fragments starting in the state s.

The (immediate) predecesors of a set of states $B \subseteq S$ is defined by

$$\mathit{Pre}(B) = \{s \mid \exists t \in B \colon \mathbf{P}(s,t) > 0\}$$

Then, is the set of states reaching B is defined by

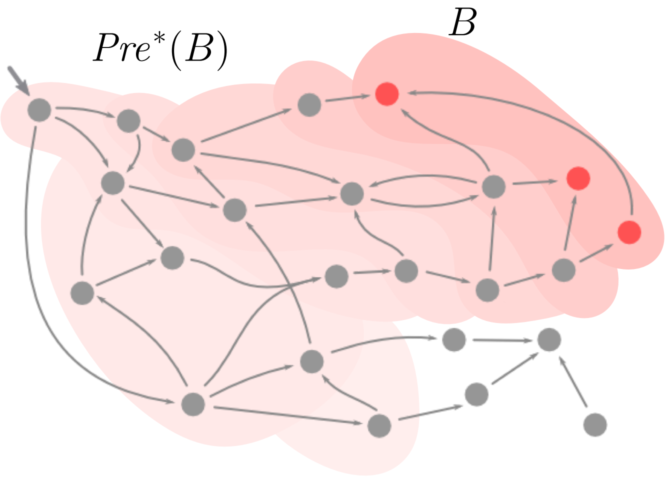
$$\mathit{Pre}^*(B) = \bigcup_{i \geq 0} \mathit{Pre}^i(B) = \{s \in S \mid \exists \pi \in \mathit{Path}_{\mathit{fin}}(s) \colon \mathit{last}(\pi) \in B\}$$



Reachability (with some probability)

An execution fragment is a sequence $s_0\, s_1\, s_2\, \dots s_n \in S^*$ such that $\mathbf{P}(s_0\, s_1\, s_2\, \dots s_n) > 0$, that is, $\mathbf{P}(s_i, s_{i+1}) > 0$ for all $0 \leq i < n$.

$\mathit{Path}_{\mathit{fin}}(s)$ is the set of all execution fragments starting in the state s.



The (immediate) predecesors of a s ed by

$$\mathit{Pre}(B) = \{s \mid \exists t \in B \colon \mathbf{P}(s, t)$$

This equality can be proved by induction from which the theorem follows

Then, is the set of states reaching is defined by

$$\mathit{Pre}^*(B) = \bigcup_{i \geq 0} \mathit{Pre}^i(B) = \{s \in S \mid \exists \pi \in \mathit{Path}_{\mathit{fin}}(s) \colon \mathit{last}(\pi) \in B\}$$

Theorem: $\Pr_s(\Diamond B) > 0$ if and only if $s \in \mathit{Pre}^*(B)$

Reachability (with some probability)

An execution fragment is a sequence $s_0\, s_1\, s_2\, \ldots s_n \in S^*$ such that $\mathbf{P}(s_0\, s_1\, s_2\, \ldots s_n) > 0$, that is, $\mathbf{P}(s_i, s_{i+1}) > 0$ for all $0 \leq i < n$.

$\mathit{Path_{fin}}(s)$ is the set of all execution fragments starting in the state s.

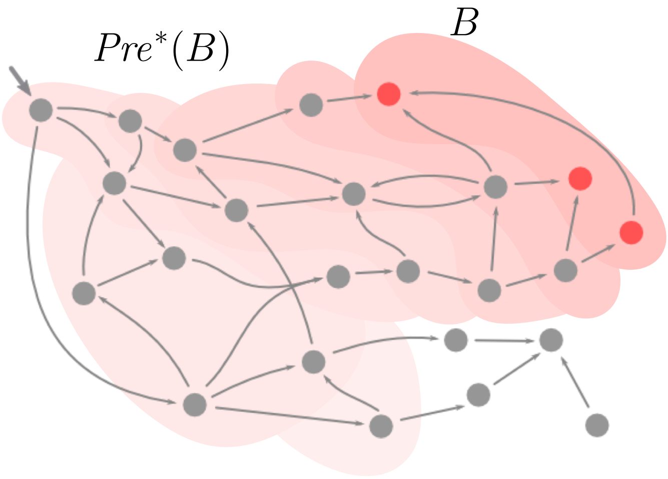
The (immediate) predecesors of a s ed by

$$\mathit{Pre}(B) = \{s \mid \exists t \in B\colon \mathbf{P}(s,t)$$

Then, is the set of states reaching is defined by

$$\mathit{Pre}^*(B) = \bigcup_{i \geq 0} \mathit{Pre}^i(B) = \{s \in S \mid \exists \pi \in \mathit{Path_{fin}}(s)\colon \mathit{last}(\pi) \in B\}$$

This equality can be proved by induction from which the theorem follows



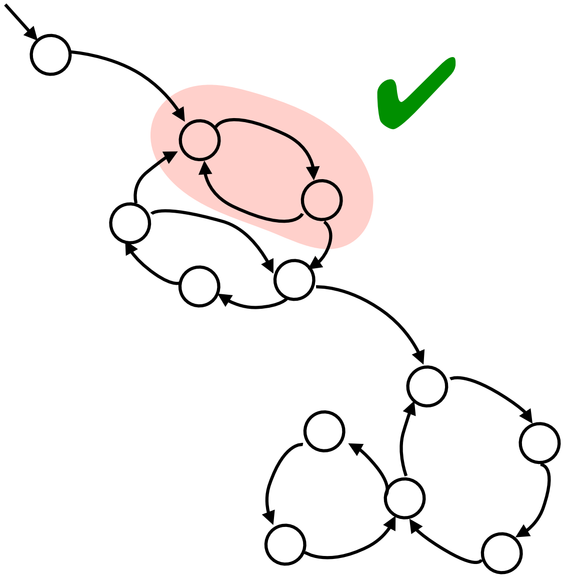
Theorem: $\Pr_s(\Diamond B) > 0$ if and only if $s \in \mathit{Pre}^*(B)$

Computed in linear time

Bottom strongly connected component

Let $M = (S, \mathbf{P}, s_0, AP, L)$ be a DTMC. Then $T \subseteq S$ is

- strongly connected if every pair of states in T is connected with an execution fragment, i.e., $\forall t, u \in T\colon \exists \pi \in Path_{fin}(t)\colon last(\pi) = u$.



Bottom strongly connected component

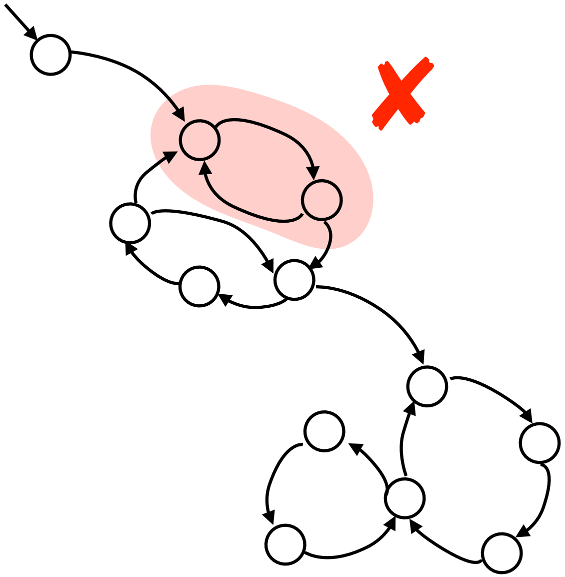
Let $M = (S, \mathbf{P}, s_0, AP, L)$ be a DTMC. Then $T \subseteq S$ is

- strongly connected if every pair of states in T is connected with an execution fragment, i.e., $\forall t, u \in T \colon \exists \pi \in Path_{fin}(t) \colon last(\pi) = u$.

- a strongly connected component (SCC) if it is a maximal strongly connected set, i.e.,

  i. T is strongly connected and

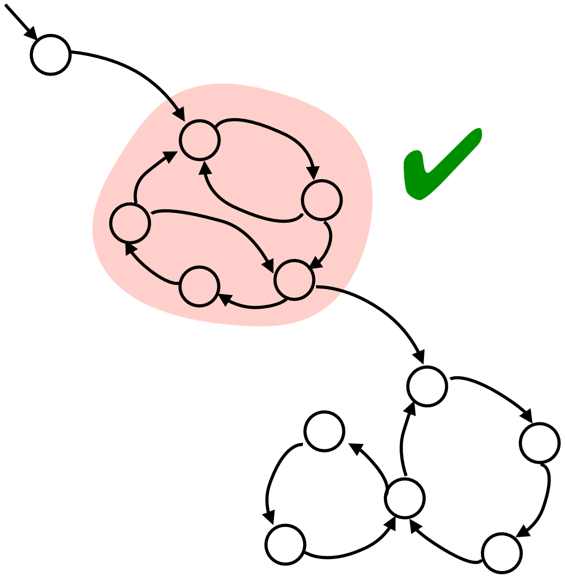
  ii. for every strongly connected T' such that $T \cap T' \neq \varnothing$, $T' \subseteq T$.



Bottom strongly connected component

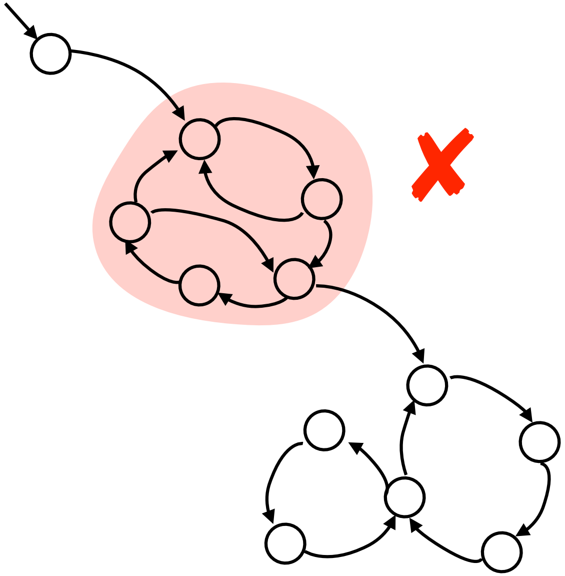
Let $M = (S, \mathbf{P}, s_0, AP, L)$ be a DTMC. Then $T \subseteq S$ is

- strongly connected if every pair of states in T is connected with an execution fragment, i.e., $\forall t, u \in T\colon \exists \pi \in Path_{fin}(t)\colon last(\pi) = u$.
- a strongly connected component (SCC) if it is a maximal strongly connected set, i.e.,
  1. T is strongly connected and
  2. for every strongly connected T' such that $T \cap T' \neq \varnothing$, $T' \subseteq T$.



Bottom strongly connected component

Let $M = (S, \mathbf{P}, s_0, AP, L)$ be a DTMC. Then $T \subseteq S$ is

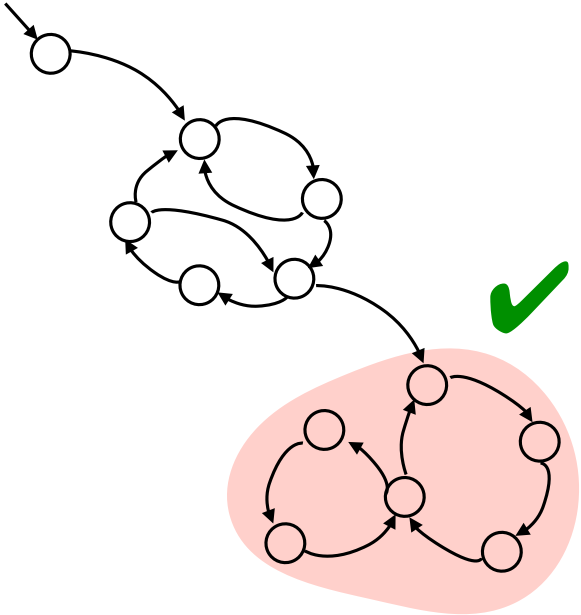


- strongly connected if every pair of states in T is connected with an execution fragment, i.e., $\forall t, u \in T \colon \exists \pi \in \mathit{Path}_{\mathit{fin}}(t) \colon \mathit{last}(\pi) = u$.
- a strongly connected component (SCC) if it is a maximal strongly connected set, i.e.,
  i. T is strongly connected and
  ii. for every strongly connected T' such that $T \cap T' \neq \varnothing$, $T' \subseteq T$.
- a bottom strongly connected component (BSCC) if it is a SCC and no state outside T is reached from T, i.e.,
  i. T is a SCC and
  ii. $\forall t \in T \colon \mathbf{P}(t, S \setminus T) = 0$ (or alternatively, $\mathbf{P}(t, T) = 1$).

Bottom strongly connected component

Let $M = (S, \mathbf{P}, s_0, AP, L)$ be a DTMC. Then $T \subseteq S$ is

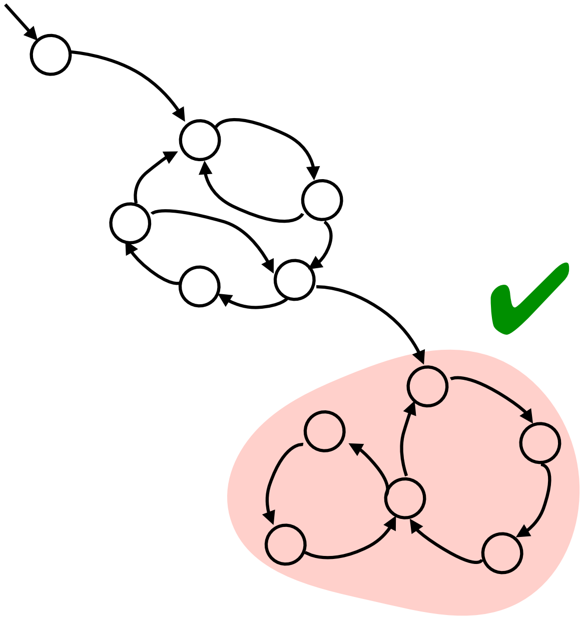
- strongly connected if every pair of states in T is connected with an execution fragment, i.e., $\forall t, u \in T\colon \exists \pi \in \mathit{Path}_{\mathit{fin}}(t)\colon \mathit{last}(\pi) = u$.
- a strongly connected component (SCC) if it is a maximal strongly connected set, i.e.,
  i. T is strongly connected and
  ii. for every strongly connected T' such that $T \cap T' \neq \varnothing$, $T' \subseteq T$.
- a bottom strongly connected component (BSCC) if it is a SCC and no state outside T is reached from T, i.e.,
  i. T is a SCC and
  ii. $\forall t \in T\colon \mathbf{P}(t, S \setminus T) = 0$ (or alternatively, $\mathbf{P}(t, T) = 1$).



Bottom strongly connected component

Let $M = (S, \mathbf{P}, s_0, AP, L)$ be a DTMC. Then $T \subseteq S$ is

- strongly connected if every pair of states in T is connected with an execution fragment, i.e., $\forall t, u \in T \colon \exists \pi \in \mathit{Path}_{\mathit{fin}}(t) \colon \mathit{last}(\pi) = u$.
- a strongly connected component (SCC) if it is a maximal strongly connected set, i.e.,
  i. T is strongly connected and
  ii. for every strongly connected T' such that $T \cap T' \neq \varnothing$, $T' \subseteq T$.
- a bottom strongly connected component (BSCC) if it is a SCC and no state outside T is reached from T, i.e.,
  i. T is a SCC and
  ii. $\forall t \in T \colon \mathbf{P}(t, S \setminus T) = 0$ (or alternatively, $\mathbf{P}(t, T) = 1$).



BSCC
can be computed in
linear time

Limit behavior of Markov chains

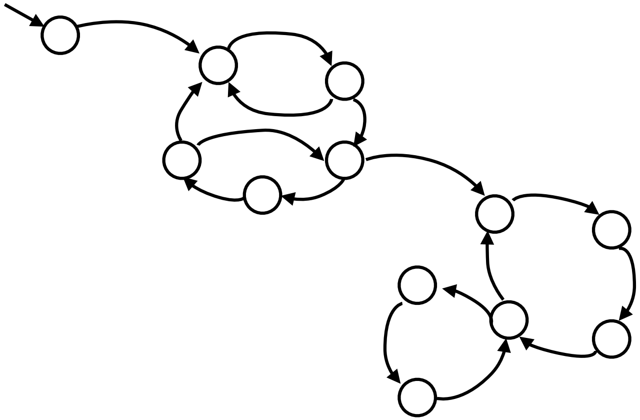
Theorem: For every state s of a finite DTMC M,

$$\Pr_s\left(\{\rho \in \mathit{Path}(s) \mid \mathit{infty}(\rho) \in \mathit{BSCC}(M)\}\right) = 1.$$

$\mathit{Path}(s) \subseteq S^\omega$ is the set of all (infinite) executions of M starting in s, i.e., infinite sequences $s_0\, s_1\, s_2\, s_3 \ldots$ such that $s_0 = s$ and $\mathbf{P}(s_i, s_{i+1}) > 0$ for all $i \geq 0$.

$\mathit{BSCC}(M)$ denotes the set of all BSCC in M.

$\mathit{infty}(\rho) = \{s \mid \overset{\infty}{\exists}\, i \geq 0\colon\, s = \rho(i)\}$ is the set of all states that repeats infinitely often in ρ

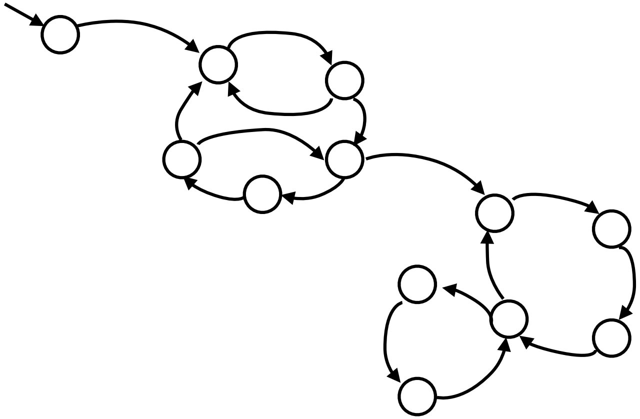


Limit behavior of Markov chains

Theorem: For every state s of a finite DTMC M,

$$\Pr_s(\{\rho \in \mathit{Path}(s) \mid \mathit{infty}(\rho) \in \mathit{BSCC}(M)\}) = 1.$$

In other words:
the probability of getting trapped
in a BSCC is 1

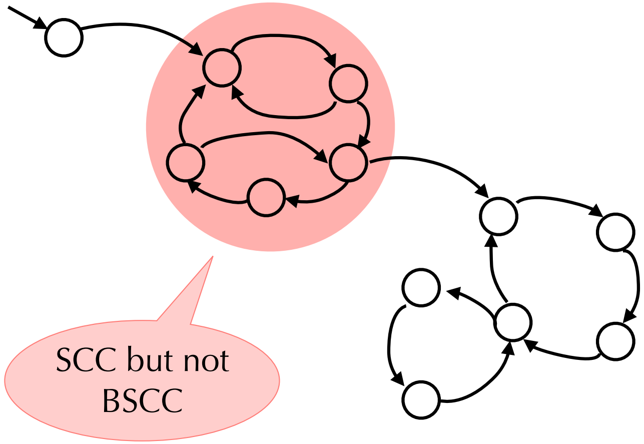


Limit behavior of Markov chains

Theorem: For every state s of a finite DTMC M,

$$\Pr_s\left(\{\rho \in \mathit{Path}(s) \mid \mathit{infty}(\rho) \in \mathit{BSCC}(M)\}\right) = 1.$$

In other words:
the probability of getting trapped
in a BSCC is 1



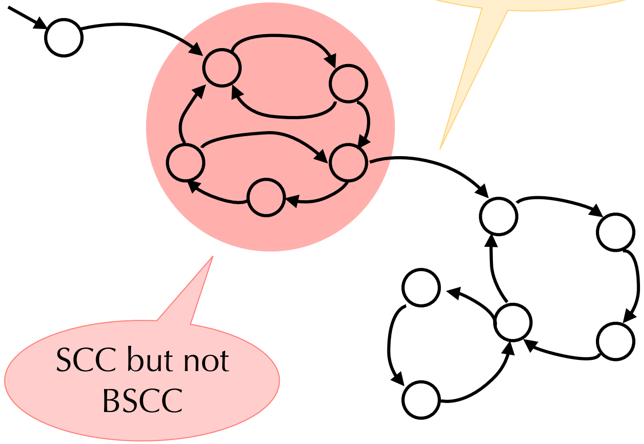
SCC but not
BSCC

Limit behavior of Markov chains

Theorem: For every state s of a finite DTMC M,

$$\Pr_s(\{\rho \in \mathit{Path}(s) \mid \mathit{infty}(\rho) \in \mathit{BSCC}(M)\}) = 1.$$

In other words:
the probability of getting trapped
in a BSCC is 1



There is always
some probability to leave
the SCC

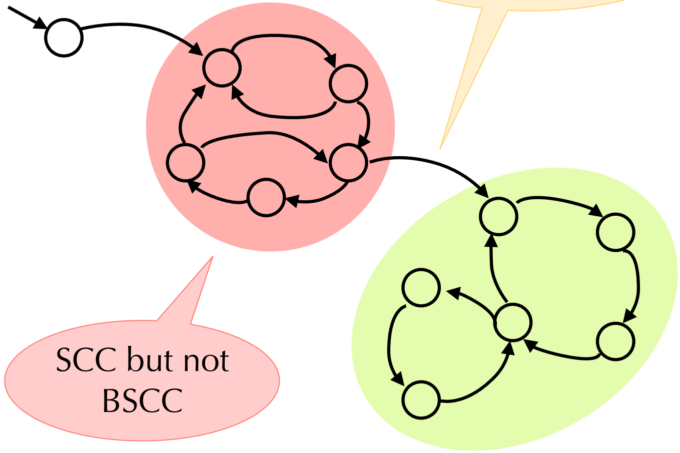
SCC but not
BSCC

Limit behavior of Markov chains

Theorem: For every state s of a finite DTMC M,

$$\Pr_s\left(\{\rho \in \mathit{Path}(s) \mid \mathit{infty}(\rho) \in \mathit{BSCC}(M)\}\right) = 1.$$

In other words:
the probability of getting trapped
in a BSCC is 1



There is always
some probability to leave
the SCC

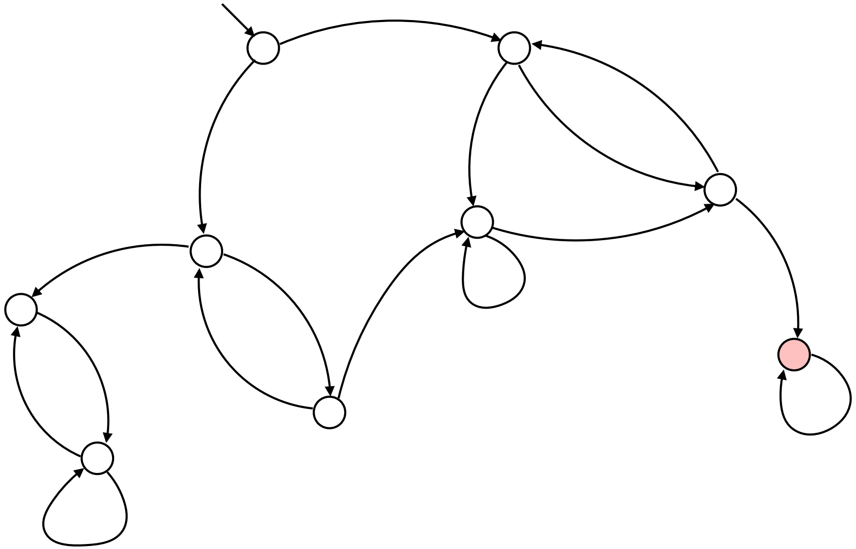
SCC but not
BSCC

BSCC:
you are trapped by
definition!

Almost sure reachability

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash Pre^*(S \backslash Pre^*(B))$$

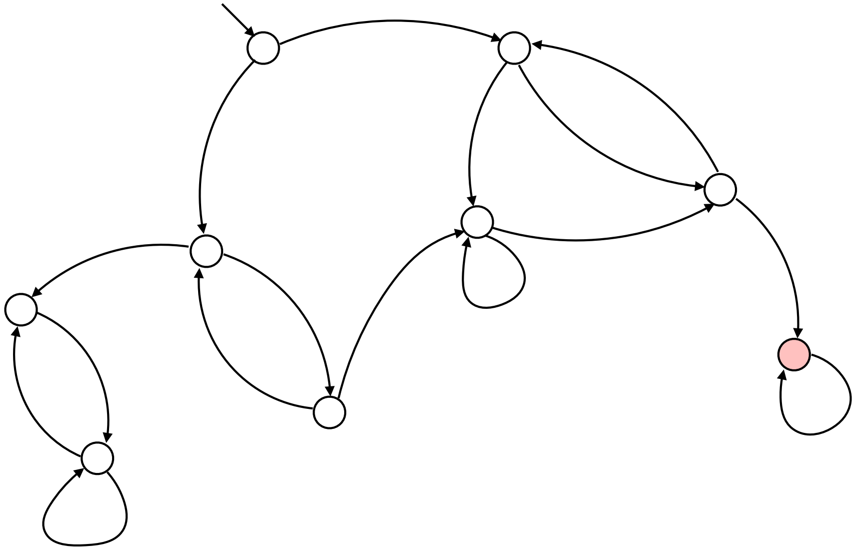


Almost sure reachability

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash Pre^*(S \backslash Pre^*(B))$$

B

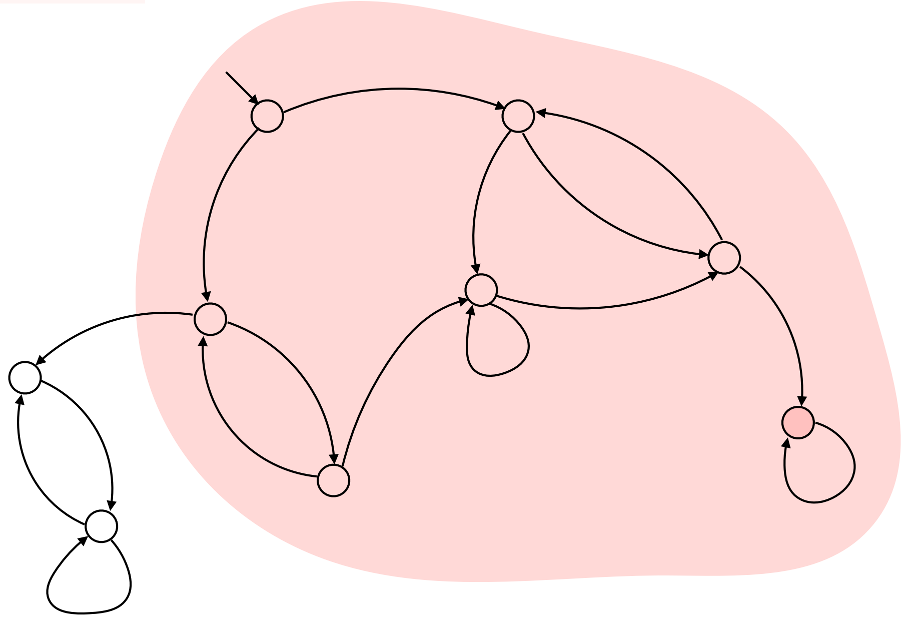


Almost sure reachability

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash Pre^*(S \backslash Pre^*(B))$$

$Pre^*(B)$

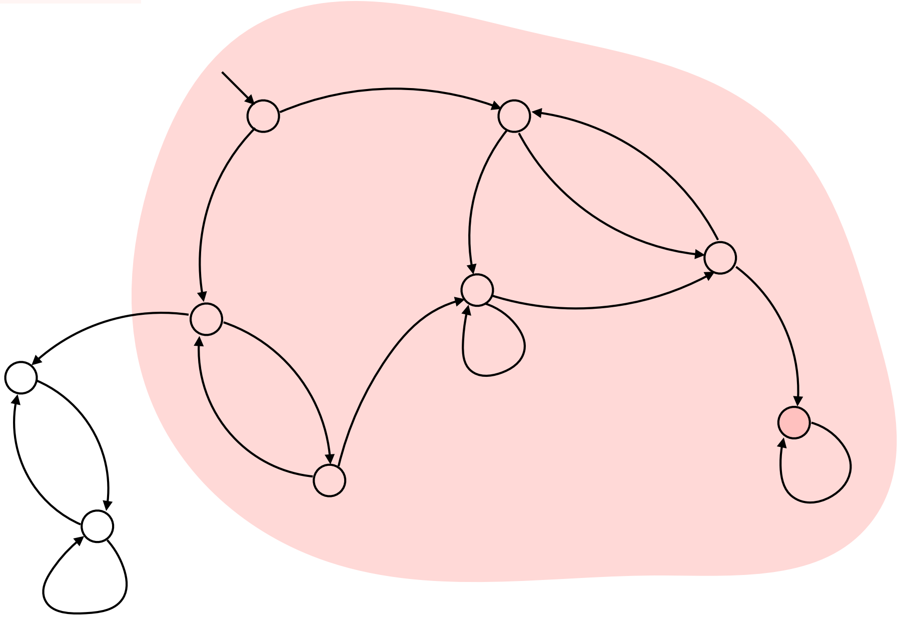


Almost sure reachability

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash Pre^*(S \backslash Pre^*(B))$$

$$\overbrace{\Pr_s(\Diamond B) > 0}^{Pre^*(B)}$$

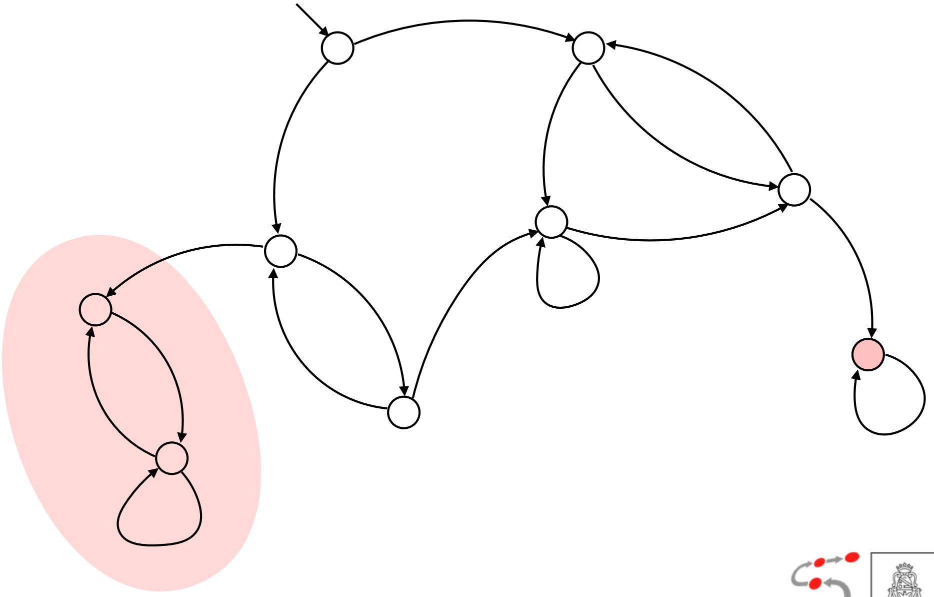


Almost sure reachability

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash Pre^*(S \backslash Pre^*(B))$$

$$S\backslash \underbrace{Pre^*(B)}_{\Pr_s(\Diamond B) > 0}$$



CONICET

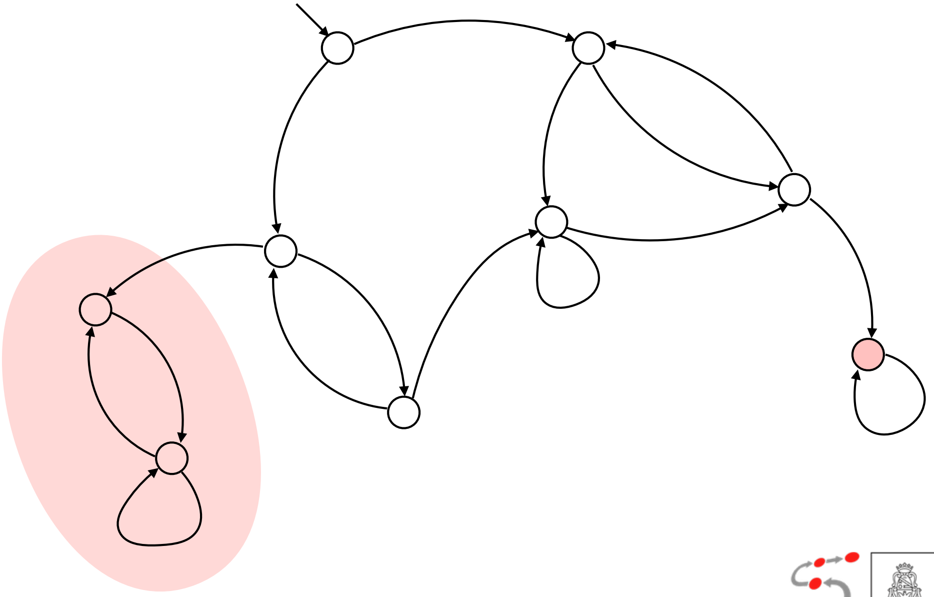
UNC

Almost sure reachability

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash Pre^*(S \backslash Pre^*(B))$$

$$\underbrace{\underbrace{S \backslash Pre^*(B)}_{\Pr_s(\Diamond B) > 0}}_{\Pr_s(\Diamond B) = 0}$$

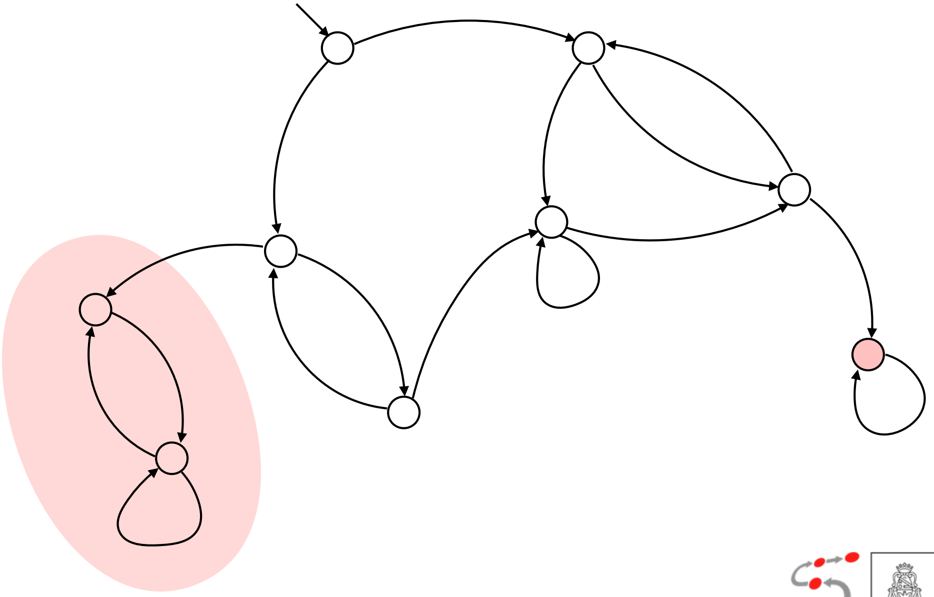


Almost sure reachability

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash Pre^*(S \backslash Pre^*(B))$$

$$\underbrace{S\backslash \underbrace{Pre^*(B)}_{\Pr_s(\Diamond B) > 0}}_{\Pr_s(\neg \Diamond B) = 1}$$

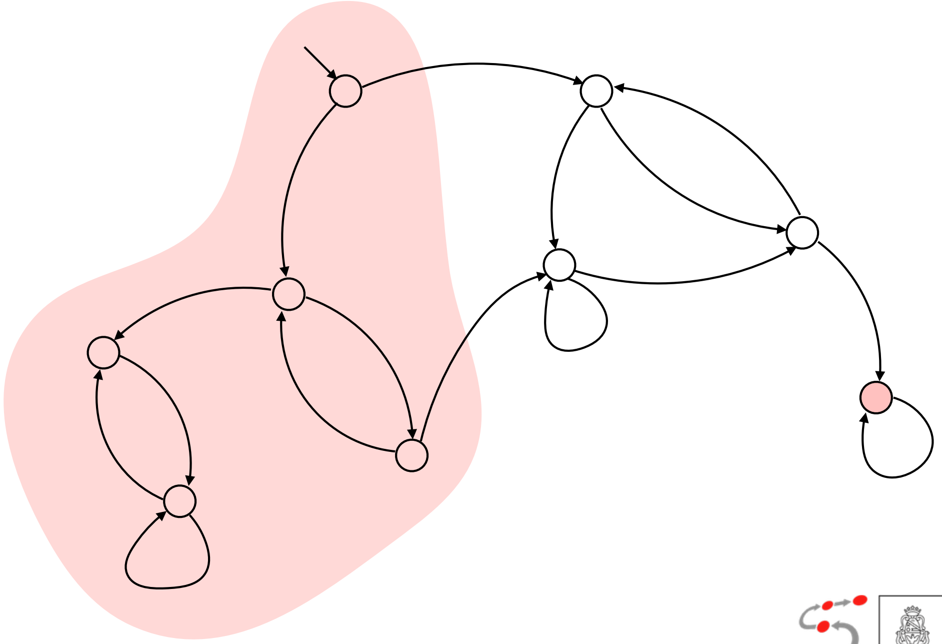


Almost sure reachability

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash Pre^*(S \backslash Pre^*(B))$$

$$Pre^*(\underbrace{S \backslash \underbrace{Pre^*(B)}_{\Pr_s(\Diamond B) > 0}}_{\Pr_s(\neg\Diamond B) = 1})$$

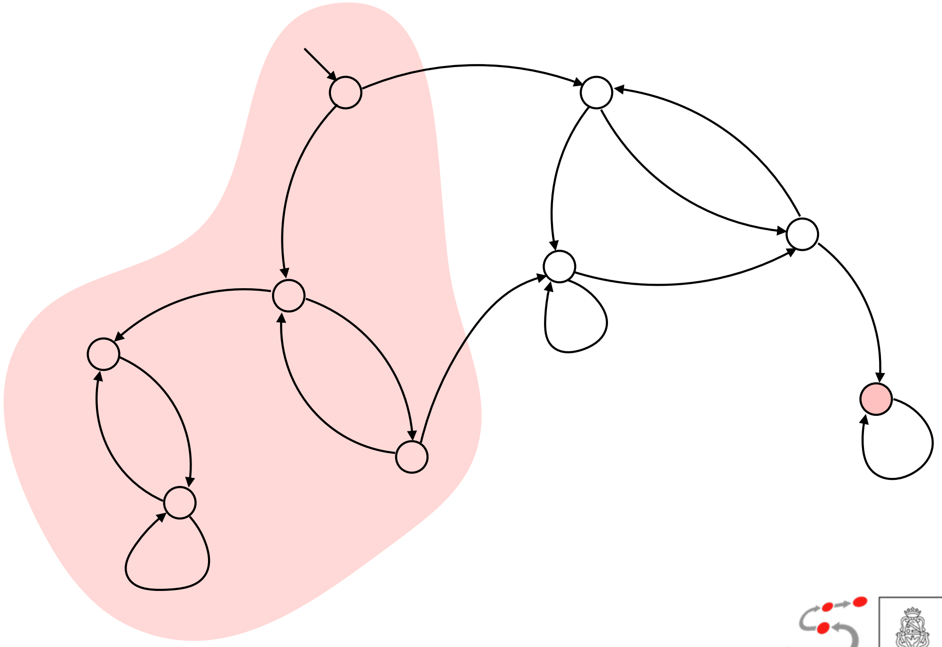


Almost sure reachability

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash \mathit{Pre}^*(S \backslash \mathit{Pre}^*(B))$$

$$\underbrace{\mathit{Pre}^*(\underbrace{S\backslash\underbrace{\mathit{Pre}^*(B)}_{\Pr_s(\Diamond B) > 0}}_{\Pr_s(\neg\Diamond B) = 1})}_{\Pr_s(\neg\Diamond B) > 0}$$

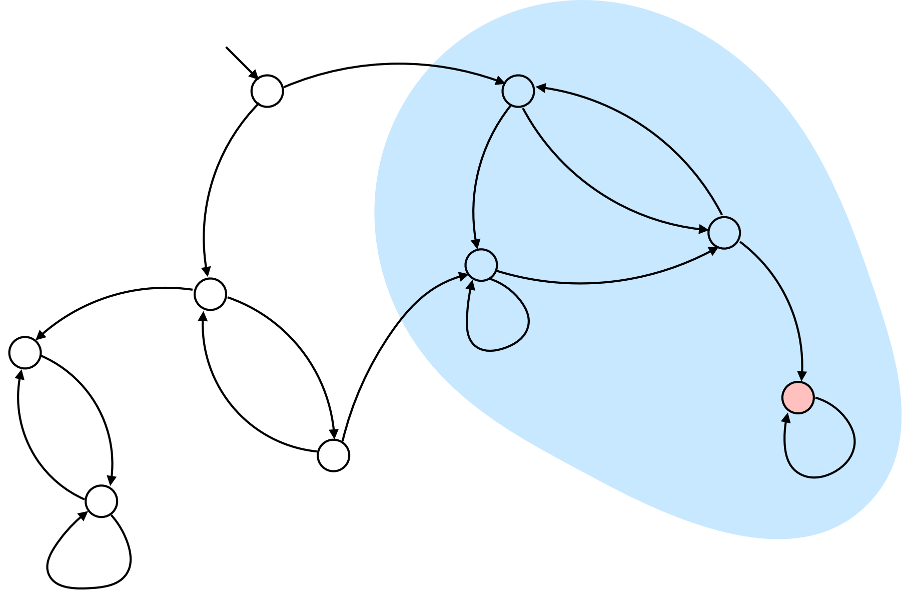


Almost sure reachability

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash Pre^*(S \backslash Pre^*(B))$$

$$S \backslash \underbrace{Pre^*(\underbrace{S \backslash \underbrace{Pre^*(B)}_{\Pr_s(\Diamond B) > 0}}_{\Pr_s(\neg \Diamond B) = 1})}_{\Pr_s(\neg \Diamond B) > 0}$$

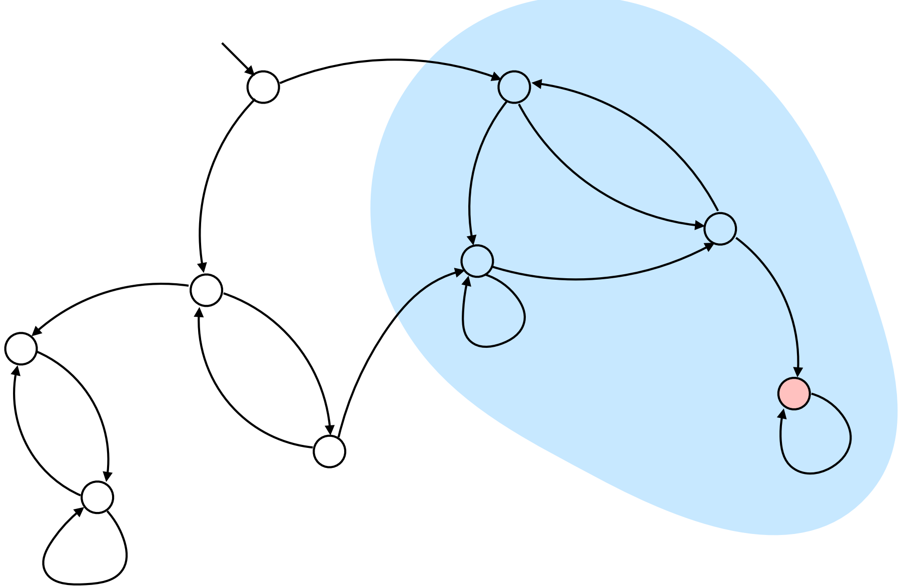


Almost sure reachability

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S\backslash Pre^*(S\backslash Pre^*(B))$$

$$S\backslash Pre^*(S\backslash \underbrace{\underbrace{\underbrace{\underbrace{Pre^*(B))}_{\Pr_s(\Diamond B) > 0}}_{\Pr_s(\neg\Diamond B) = 1}}_{\Pr_s(\neg\Diamond B) > 0}}_{\Pr_s(\neg\Diamond B) = 0}$$

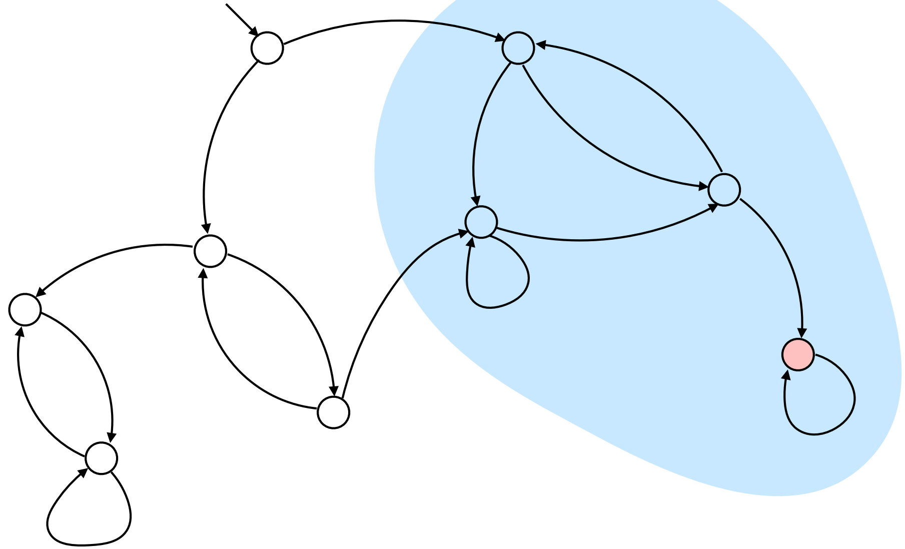


Almost sure reachability

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash Pre^*(S \backslash Pre^*(B))$$

$$\underbrace{S\backslash \underbrace{Pre^*(\underbrace{S\backslash \underbrace{Pre^*(B)}_{\Pr_s(\Diamond B) > 0}}_{\Pr_s(\neg\Diamond B) = 1})}_{\Pr_s(\neg\Diamond B) > 0}}_{\Pr_s(\Diamond B) = 1}$$



Almost sure reachability

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash \mathit{Pre}^*(S \backslash \mathit{Pre}^*(B))$$

Recall:
linear time

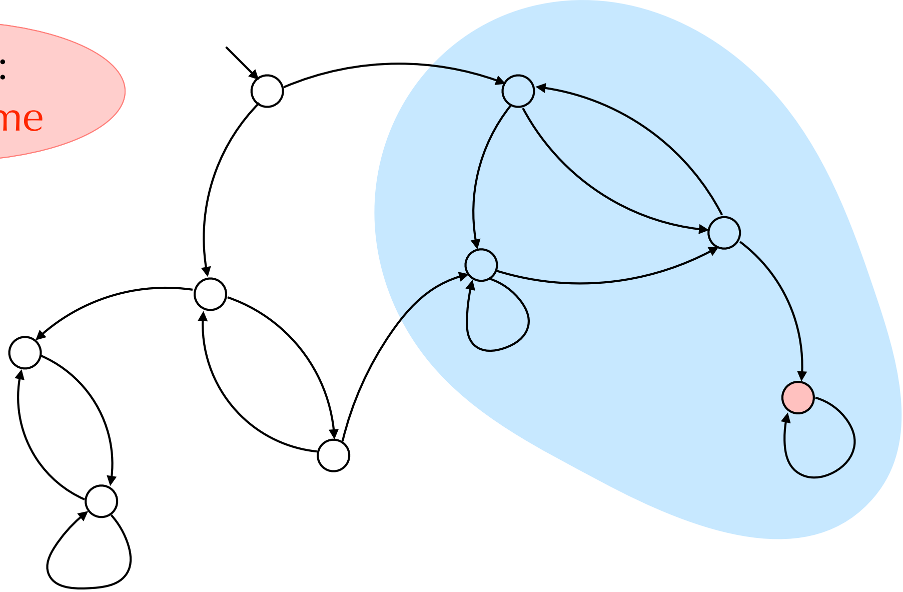
$$S \backslash \mathit{Pre}^*(S \backslash \underbrace{\mathit{Pre}^*(B)})$$

$$\underbrace{\Pr_s(\Diamond B) > 0}$$

$$\underbrace{\Pr_s(\neg\Diamond B) = 1}$$

$$\underbrace{\Pr_s(\neg\Diamond B) > 0}$$

$$\Pr_s(\Diamond B) = 1$$



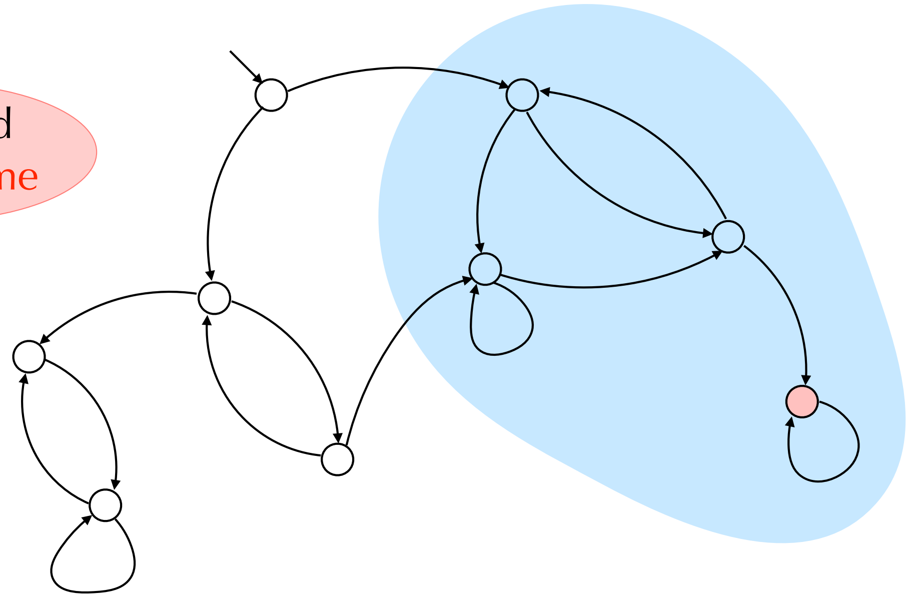
Almost sure reachability

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash Pre^*(S \backslash Pre^*(B))$$

$$\underbrace{S \backslash \underbrace{Pre^*(\underbrace{S \backslash \underbrace{Pre^*(B)}_{\Pr_s(\Diamond B) > 0}}_{\Pr_s(\neg\Diamond B) = 1})}_{\Pr_s(\neg\Diamond B) > 0}}_{\Pr_s(\Diamond B) = 1}$$

Computed in linear time



Almost sure reachability

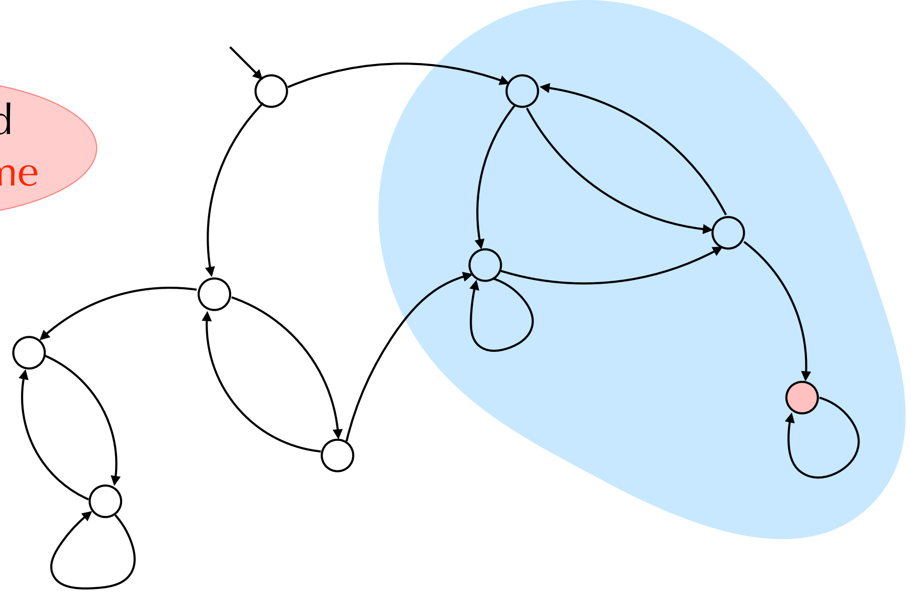
What if B is not absorbing?

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S\backslash Pre^*(S\backslash Pre^*(B))$$

Computed in linear time

$$\underbrace{S\backslash\underbrace{Pre^*(\underbrace{S\backslash\underbrace{Pre^*(B)}_{\Pr_s(\Diamond B) > 0})}_{\Pr_s(\neg\Diamond B) = 1})}_{\Pr_s(\neg\Diamond B) > 0}}_{\Pr_s(\Diamond B) = 1}$$

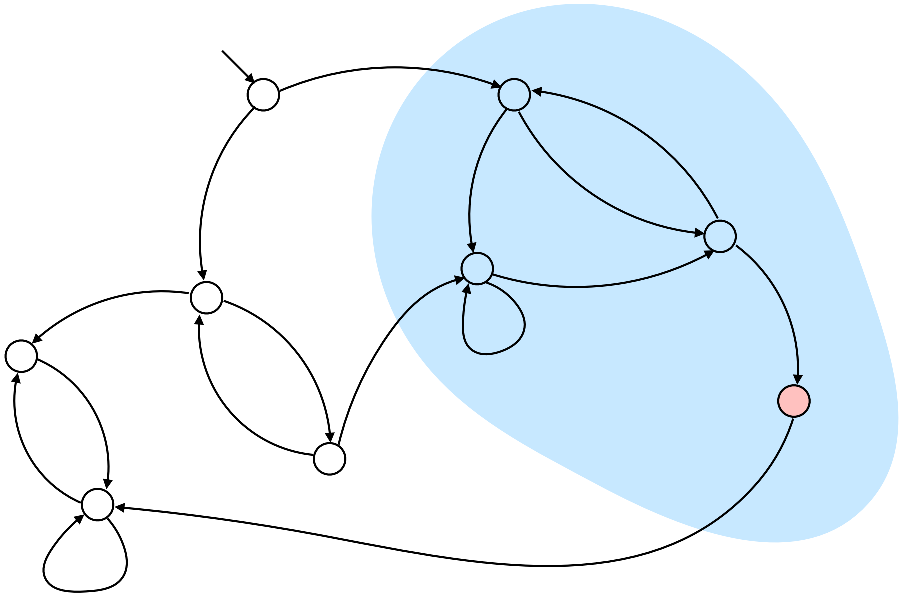


Almost sure reachability

What if B is not absorbing?

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash Pre^*(S \backslash Pre^*(B))$$



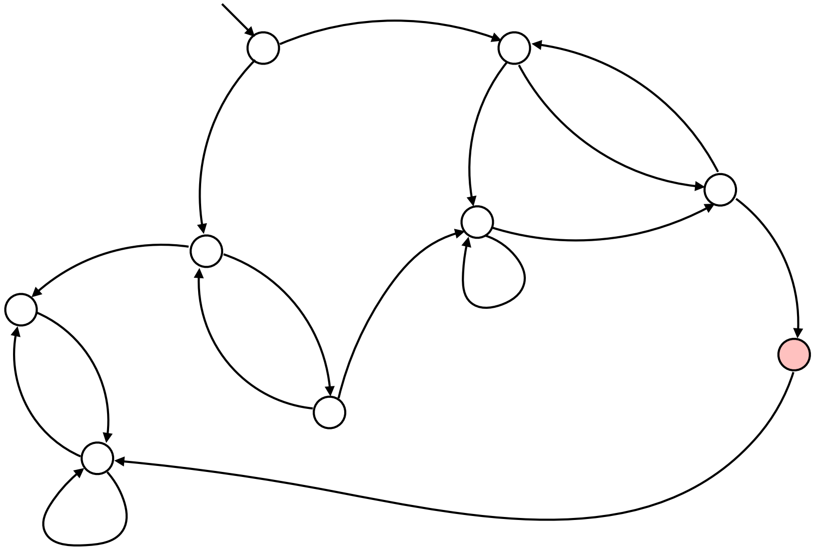
Almost sure reachability

What if B is not absorbing?

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash Pre^*(S \backslash Pre^*(B))$$

B



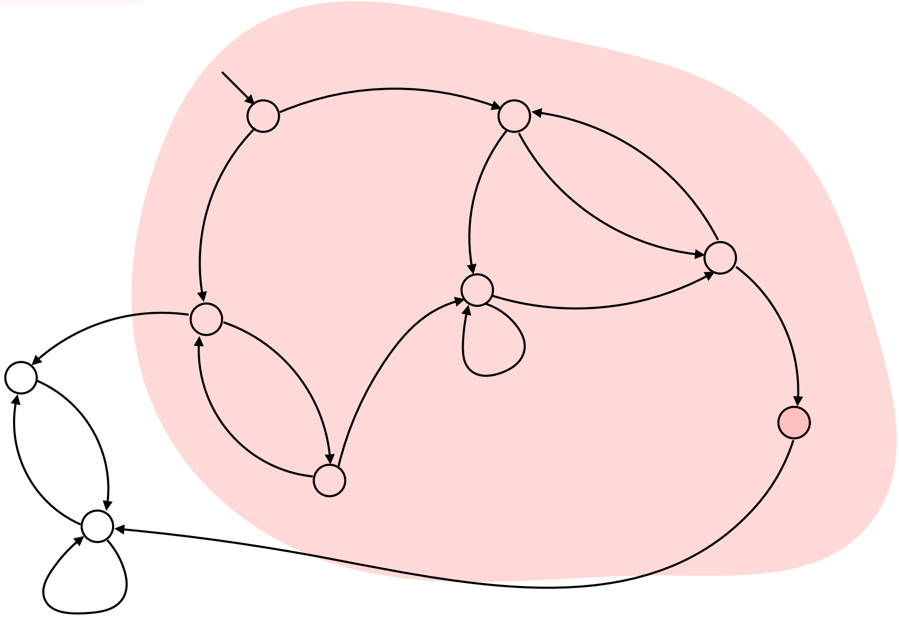
Almost sure reachability

What if B is not absorbing?

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash Pre^*(S \backslash Pre^*(B))$$

$Pre^*(B)$



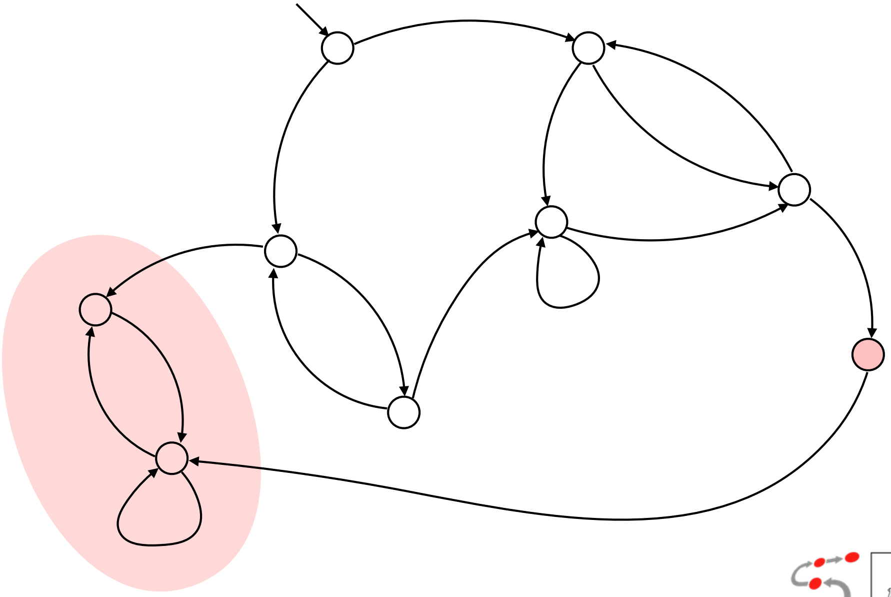
Almost sure reachability

What if B is not absorbing?

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash Pre^*(S \backslash Pre^*(B))$$

$S \backslash Pre^*(B)$



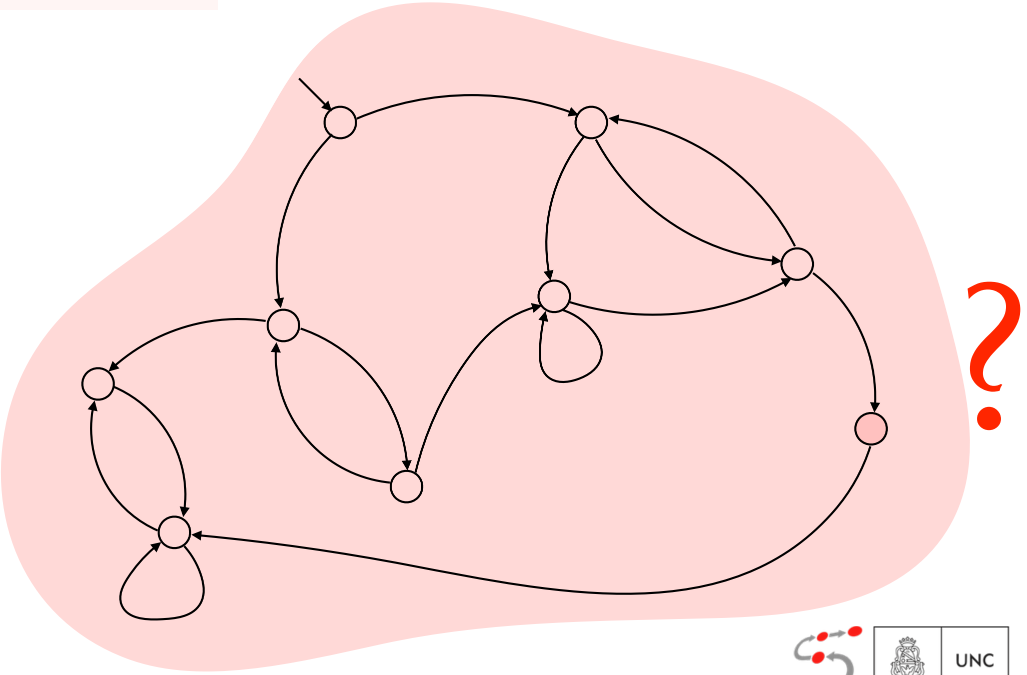
Almost sure reachability

What if B is not absorbing?

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash Pre^*(S \backslash Pre^*(B))$$

$$Pre^*(S \backslash Pre^*(B))$$



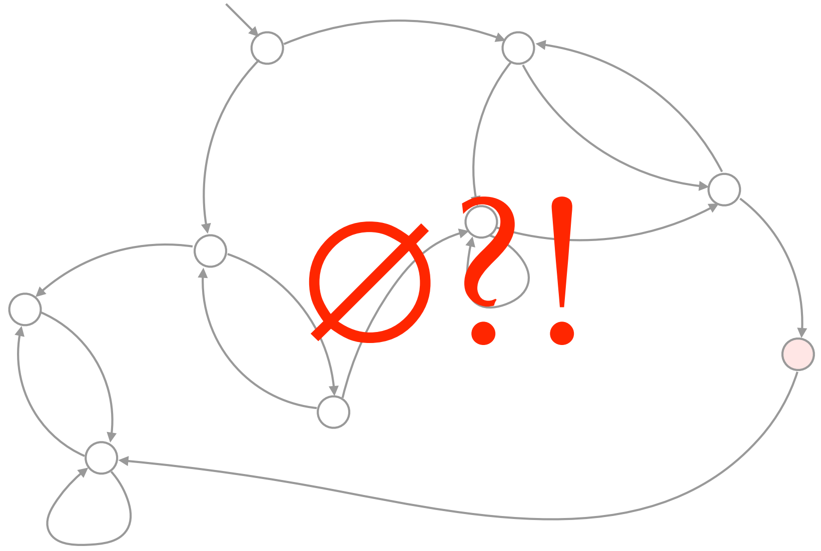
Almost sure reachability

What if B is not absorbing?

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash Pre^*(S \backslash Pre^*(B))$$

$$S \backslash Pre^*(S \backslash Pre^*(B))$$



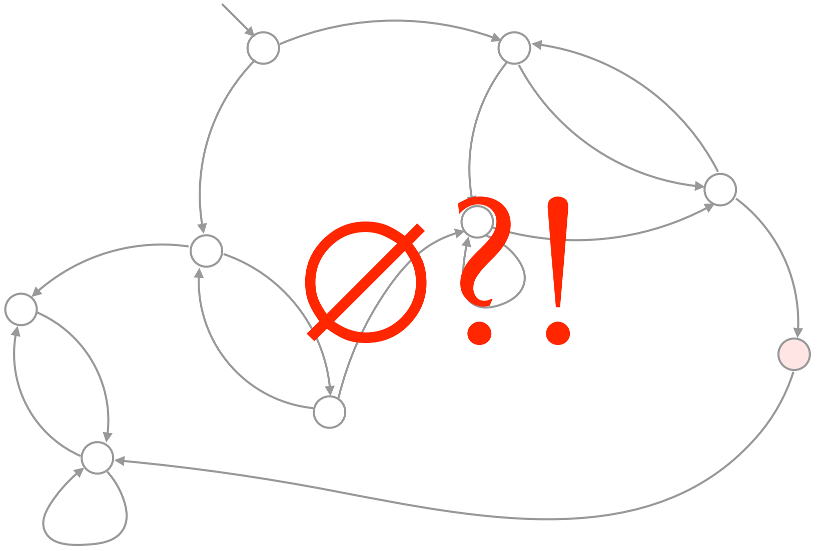
Almost sure reachability

What if B is not absorbing?

Theorem: Let $s \in S$ and $B \subseteq S$ be a set of absorbing states. Then

$$\Pr_s(\Diamond B) = 1 \quad \text{if and ony if} \quad s \in S \backslash Pre^*(S \backslash Pre^*(B))$$

$$S \backslash Pre^*(S \backslash Pre^*(B))$$



Therefore, for the general case, first construct M_B

Qualitative repeated reachability

$\rho \in \Box\Diamond B$ iff $\mathit{infty}(\rho) \cap B \neq \varnothing$

Some state of *B* should repeat infinitely often

Qualitative repeated reachability

$\rho \in \Box\Diamond B$ iff $\mathit{infty}(\rho) \cap B \neq \varnothing$

Some state of *B* should repeat infinitely often

Theorem: Let $s \in S$ and $B \subseteq S$. Then

$\Pr_s(\Box\Diamond B) = 1$ iff for all $T \in \mathit{BSCC}(M)$ reachable from $s \in S, T \cap B \neq \varnothing$

iff $s \in \mathit{Pre}^*(\bigcup\{T \in \mathit{BSCC}(M) \mid T \cap B \neq \varnothing\})$

Qualitative repeated reachability

$\rho \in \Box\Diamond B$ iff $\mathit{infty}(\rho) \cap B \neq \varnothing$

Some state of *B* should repeat infinitely often

Theorem: Let $s \in S$ and $B \subseteq S$. Then

$$\Pr_s(\Box\Diamond B) = 1 \quad \text{iff} \quad \text{for all } T \in \mathit{BSCC}(M) \text{ reachable from } s \in S, T \cap B \neq \varnothing$$

$$\text{iff} \quad s \in \mathit{Pre}^*(\bigcup\{T \in \mathit{BSCC}(M) \mid T \cap B \neq \varnothing\})$$

Follows from the limit behavior of Markov chains

Theorem: For every state s of a finite DTMC M,

$$\Pr_s(\{\rho \in \mathit{Path}(s) \mid \mathit{infty}(\rho) \in \mathit{BSCC}(M)\}) = 1.$$

Qualitative repeated reachability

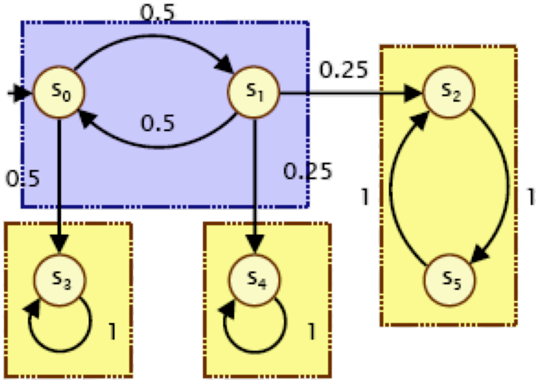
$\rho \in \Box\Diamond B \quad \text{iff} \quad \mathit{infty}(\rho) \cap B \neq \varnothing$

Some state of *B* should repeat infinitely often

Theorem: Let $s \in S$ and $B \subseteq S$. Then

$$\Pr_s(\Box\Diamond B) = 1 \quad \text{iff} \quad \text{for all } T \in \mathit{BSCC}(M) \text{ reachable from } s \in S, T \cap B \neq \varnothing$$

$$\text{iff} \quad s \in \mathit{Pre}^*(\bigcup\{T \in \mathit{BSCC}(M) \mid T \cap B \neq \varnothing\})$$



$$B = \{s_3, s_4, s_5\}$$

Qualitative repeated reachability

$\rho \in \Box\Diamond B$ iff $\mathit{infty}(\rho) \cap B \neq \varnothing$

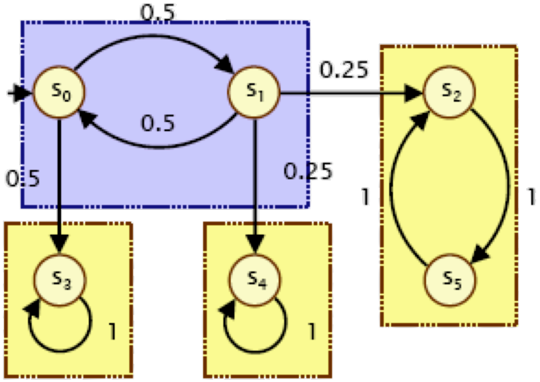
Some state of B should repeat infinitely often

<span style="color:red">Theorem:</span> Let $s \in S$ and $B \subseteq S$. Then

$$\Pr_s(\Box\Diamond B) = 1 \quad \text{iff} \quad \text{for all } T \in \mathit{BSCC}(M) \text{ reachable from } s \in S, T \cap B \neq \varnothing$$

$$\text{iff} \quad s \in \mathit{Pre}^*(\bigcup\{T \in \mathit{BSCC}(M) \mid T \cap B \neq \varnothing\})$$

Computed in linear time



$B = \{s_3, s_4, s_5\}$

Qualitative persistence

$\rho \in \Diamond\Box B \quad \text{iff} \quad \mathit{infty}(\rho) \subseteq B$

Only states from *B* can repeat infinitely often

Qualitative persistence

$\rho \in \Diamond\Box B$ iff $\mathit{infty}(\rho) \subseteq B$

Only states from *B* can repeat infinitely often

Theorem: Let $s \in S$ and $B \subseteq S$. Then

$\Pr_s(\Diamond\Box G) = 1$ iff for all $T \in BSCC(M)$ reachable from $s \in S, T \subseteq B$

iff $s \in Pre^*(\bigcup\{T \in BSCC(M) \mid T \subseteq B\})$

Qualitative persistence

$\rho \in \Diamond\Box B$ iff $\mathit{infty}(\rho) \subseteq B$

Only states from B can repeat infinitely often

Theorem: Let $s \in S$ and $B \subseteq S$. Then

$\Pr_s(\Diamond\Box G) = 1$ iff for all $T \in \mathit{BSCC}(M)$ reachable from $s \in S, T \subseteq B$

iff $s \in \mathit{Pre}^*(\bigcup\{T \in \mathit{BSCC}(M) \mid T \subseteq B\})$

Like before, follows from the limit behavior of Markov chains

CONICET

UNC

Qualitative persistence

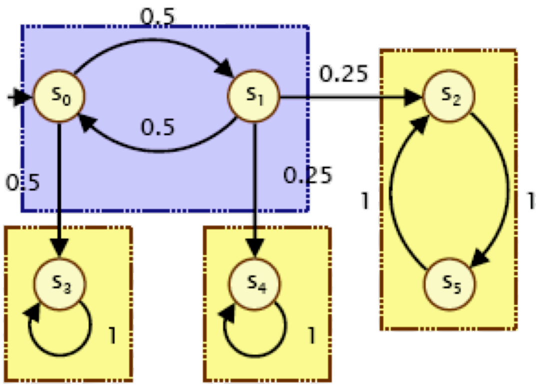
$\rho \in \Diamond\Box B \quad \text{iff} \quad \mathit{infty}(\rho) \subseteq B$

Only states from ***B*** can repeat infinitely often

Theorem: Let $s \in S$ and $B \subseteq S$. Then

$$\mathrm{Pr}_s(\Diamond\Box G) = 1 \quad \text{iff} \quad \text{for all } T \in BSCC(M) \text{ reachable from } s \in S, T \subseteq B$$

$$\text{iff} \quad s \in Pre^*(\bigcup\{T \in BSCC(M) \mid T \subseteq B\})$$



$B = \{s_3, s_4, s_5\}$

Qualitative persistence

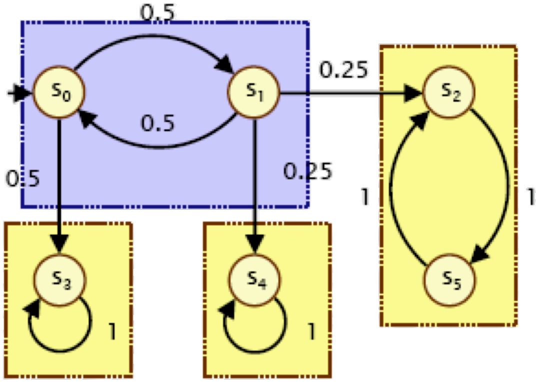
$\rho \in \Diamond\Box B \quad \text{iff} \quad \mathit{infty}(\rho) \subseteq B$

Only states from ***B*** can repeat infinitely often

Theorem: Let $s \in S$ and $B \subseteq S$. Then

$$\Pr_s(\Diamond\Box G) = 1 \qquad \text{iff} \qquad \text{for all } T \in \mathit{BSCC}(M) \text{ reachable from } s \in S, T \subseteq B$$

$$\text{iff} \qquad s \in \mathit{Pre}^*(\bigcup\{T \in \mathit{BSCC}(M) \mid T \subseteq B\})$$



$\xcancel{B = \{s_3, s_4, s_5\}}$

Qualitative persistence

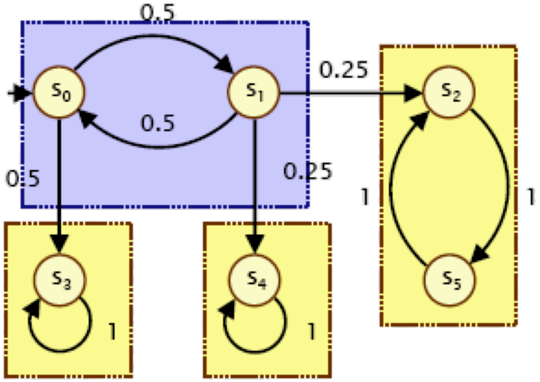
$\rho \in \Diamond\Box B$ iff $\mathit{infty}(\rho) \subseteq B$

Only states from B can repeat infinitely often

Theorem: Let $s \in S$ and $B \subseteq S$. Then

$$\Pr_s(\Diamond\Box G) = 1 \quad \text{iff} \quad \text{for all } T \in \mathit{BSCC}(M) \text{ reachable from } s \in S, T \subseteq B$$

$$\text{iff} \quad s \in \mathit{Pre}^*(\bigcup\{T \in \mathit{BSCC}(M) \mid T \subseteq B\})$$



$\xcancel{B = \{s_3, s_4, s_5\}}$

$B = \{s_3, s_4, s_5, s_6\}$ ✓

Qualitative persistence

$\rho \in \Diamond\Box B \quad \text{iff} \quad \mathit{infty}(\rho) \subseteq B$

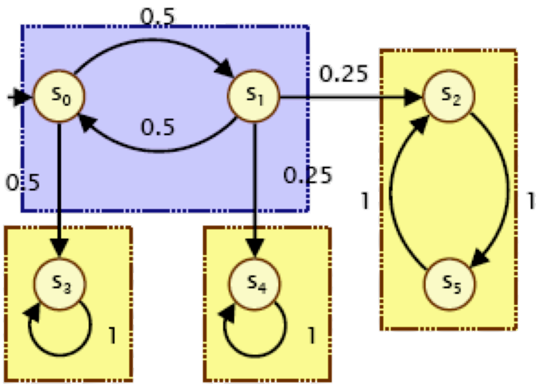
Only states from B can repeat infinitely often

Theorem: Let $s \in S$ and $B \subseteq S$. Then

$$\Pr_s(\Diamond\Box G) = 1 \quad \text{iff} \quad \text{for all } T \in BSCC(M) \text{ reachable from } s \in S, T \subseteq B$$

$$\text{iff} \quad s \in Pre^*(\bigcup\{T \in BSCC(M) \mid T \subseteq B\})$$

Computed in linear time



~~$B = \{s_3, s_4, s_5\}$~~

$B = \{s_3, s_4, s_5, s_6\}$ ✔

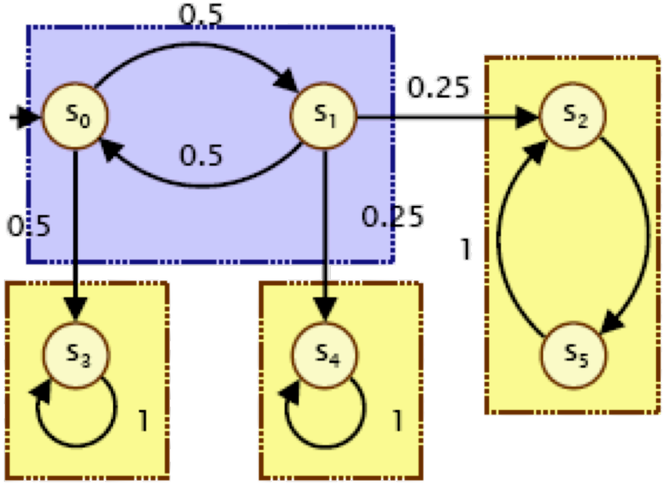
More quantitative properties

Quantitative repeated reachability

Theorem: Let $s \in S$ and $B \subseteq S$. Then

$$\Pr_s(\Box\Diamond B) = \Pr_s(\Diamond U)$$

where $U = \bigcup\{T \in BSCC(M) \mid T \cap B \neq \varnothing\}$.



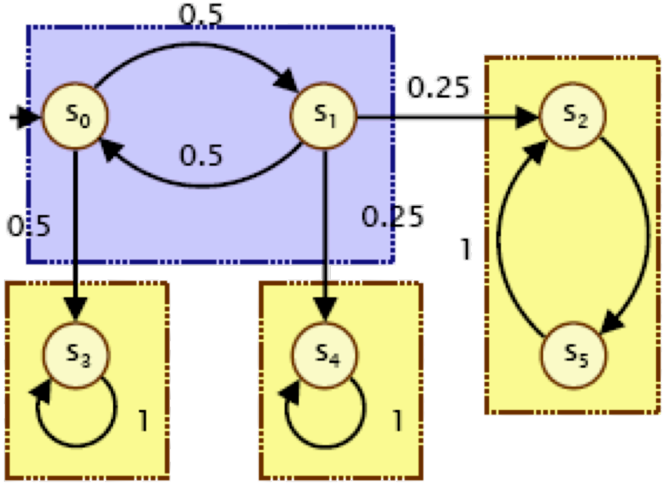
$$B = \{s_4, s_5\}$$

Quantitative repeated reachability

Theorem: Let $s \in S$ and $B \subseteq S$. Then

$$\Pr_s(\Box\Diamond B) = \Pr_s(\Diamond U)$$

where $U = \bigcup\{T \in BSCC(M) \mid T \cap B \neq \varnothing\}$.



- ❖ Compute U (linear time)

$B = \{s_4, s_5\}$

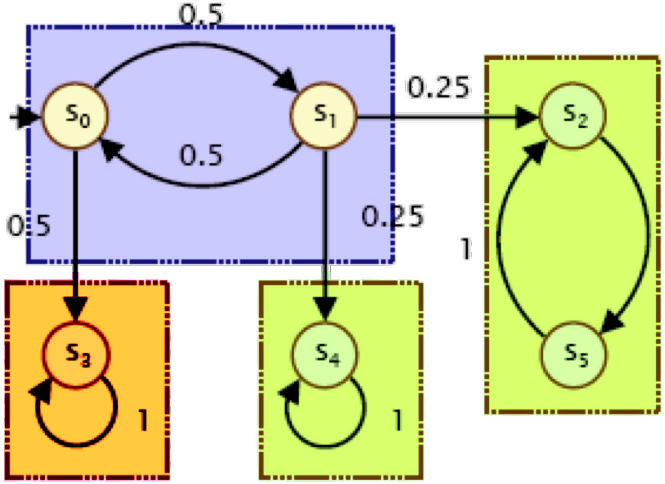
Quantitative repeated reachability

Theorem: Let $s \in S$ and $B \subseteq S$. Then

$$\Pr_s(\Box\Diamond B) = \Pr_s(\Diamond U)$$

where $U = \bigcup\{T \in BSCC(M) \mid T \cap B \neq \varnothing\}$.

❖ Compute U (linear time)



$$B = \{s_4, s_5\}$$

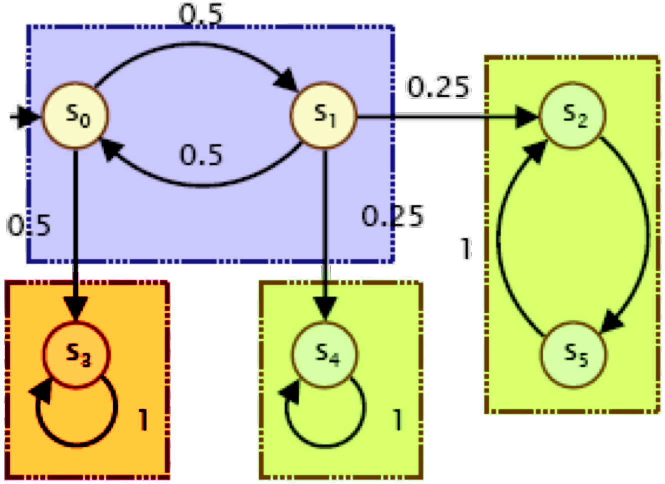
$$U = \{s_2, s_4, s_5\}$$

Quantitative repeated reachability

Theorem: Let $s \in S$ and $B \subseteq S$. Then

$$\Pr_s(\Box\Diamond B) = \Pr_s(\Diamond U)$$

where $U = \bigcup\{T \in BSCC(M) \mid T \cap B \neq \varnothing\}$.



- Compute U (linear time)
- Compute $\Pr_s(\Diamond U)$ (polynomial time)

$$B = \{s_4, s_5\}$$

$$U = \{s_2, s_4, s_5\}$$

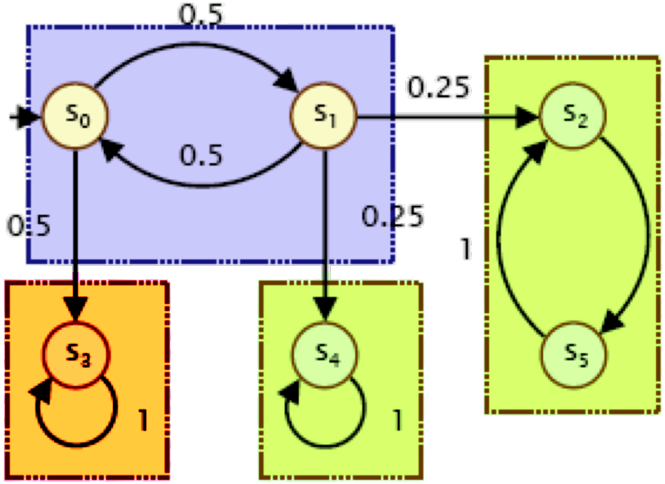
Computed in polynomial time

Quantitative repeated reachability

Theorem: Let $s \in S$ and $B \subseteq S$. Then

$$\Pr_s(\Box\Diamond B) = \Pr_s(\Diamond U)$$

where $U = \bigcup\{T \in BSCC(M) \mid T \cap B \neq \varnothing\}$.



- Compute U (linear time)
- Compute $\Pr_s(\Diamond U)$ (polynomial time)

$$B = \{s_4, s_5\}$$

$$U = \{s_2, s_4, s_5\}$$

CONICET

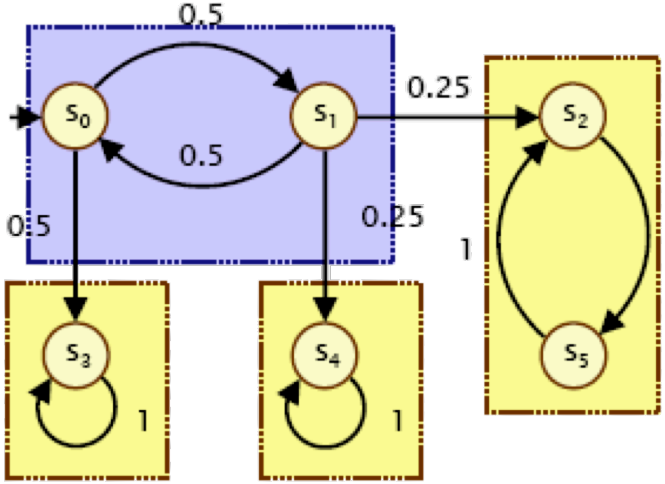
UNC

Quantitative persistence

Theorem: Let $s \in S$ and $B \subseteq S$. Then

$$\Pr_s(\Diamond\Box B) = \Pr_s(\Diamond U)$$

where $U = \bigcup\{T \in BSCC(M) \mid T \subseteq B\}$.



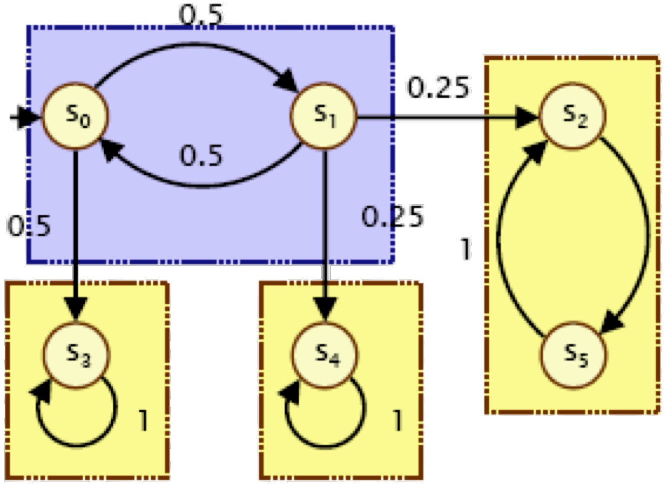
$$B = \{s_4, s_5\}$$

Quantitative persistence

Theorem: Let $s \in S$ and $B \subseteq S$. Then

$$\Pr_s(\Diamond\Box B) = \Pr_s(\Diamond U)$$

where $U = \bigcup\{T \in BSCC(M) \mid T \subseteq B\}$.



- Compute U

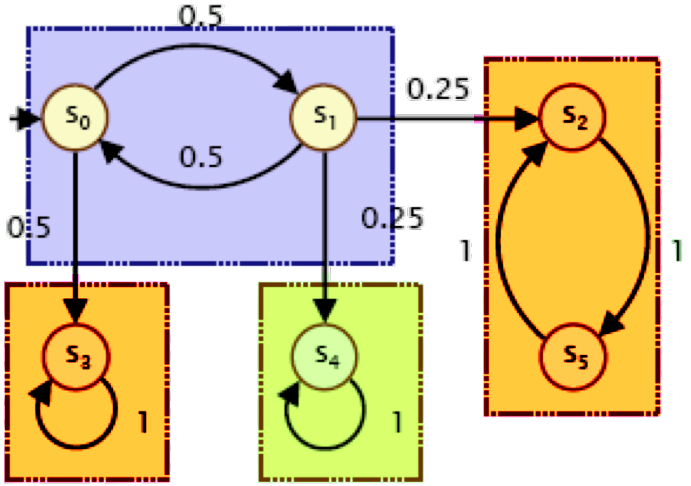
$$B = \{s_4, s_5\}$$

Quantitative persistence

Theorem: Let $s \in S$ and $B \subseteq S$. Then

$$\Pr_s(\Diamond\Box B) = \Pr_s(\Diamond U)$$

where $U = \bigcup\{T \in BSCC(M) \mid T \subseteq B\}$.



- Compute U

$$B = \{s_4, s_5\}$$

$$U = \{s_4\}$$

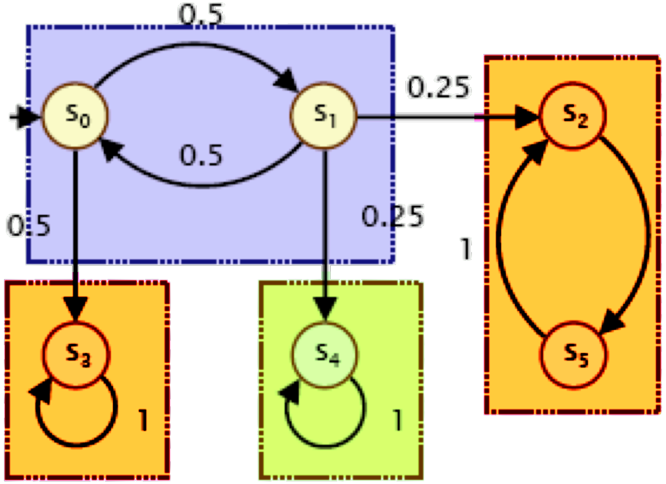
Computed in polynomial time

Quantitative persistence

Theorem: Let $s \in S$ and $B \subseteq S$. Then

$$\Pr_s(\Diamond\Box B) = \Pr_s(\Diamond U)$$

where $U = \bigcup\{T \in BSCC(M) \mid T \subseteq B\}$.



- Compute U
- Compute $\Pr_s(\Diamond U)$

$B = \{s_4, s_5\}$

$U = \{s_4\}$

ω-regular properties

- Can be expressed with ω-automata such as Büchi automata, Rabin automata, Strett automata, etc.
- Repeated reachability and persistence are central, since, e.g., the Rabin acceptance condition of can be expressed as properties of the form:

$$\bigvee_{i\in I}(\Diamond\Box\neg G_i \wedge \Box\Diamond H_i)$$

- The verification of ω-properties proceed by
  i. obtaining the synchronous product of the DTMC with the deterministic Rabin automata (DRA) of the property, and
  ii. calculating the reachability property of a set U very much like for repeated reachability and persistence.

ω-regular properties

Though polynomial w.r.t. the DTMC and the DRA, the DRA normally grows exponentially large w.r.t. the ω-property expressed in e.g. LTL

- Can be expressed with ω-automata such as Büchi automata, automata, etc.
- Repeated reachability and persistence are central, since, e.g., th abin acceptance condition of can be expressed as properties of the form:

$$\bigvee_{i\in I}(\Diamond\Box\neg G_i \wedge \Box\Diamond H_i)$$

- The verification of ω-properties proceed by
  1. obtaining the synchronous product of the DTMC with the deterministic Rabin automata (DRA) of the property, and
  2. calculating the reachability property of a set U very much like for repeated reachability and persistence.

PCTL

PCTL: Probabilistic Computational Tree Logic

- Syntax

$$\begin{array}{lcl} \Phi & = & \textit{true} \;\mid\; p \;\mid\; \neg\Phi \;\mid\; \Phi_1 \wedge \Phi_2 \;\mid\; \mathtt{P}_{\bowtie a}(\phi) \\ \phi & = & \bigcirc\Phi \;\mid\; \Phi_1 \,\mathtt{U}\, \Phi_2 \;\mid\; \Phi_1 \,\mathtt{U}^{\leq n}\, \Phi_2 \end{array}$$

state formulas

path formulas

where

- $p \in AP$ is an atomic proposition, and
- $\bowtie \in \{<, \leq, \geq, >\}$ and $a \in \mathbb{R}$.

PCTL: Probabilistic Computational Tree Logic

- Syntax

$$\Phi \;=\; \textit{true} \;\mid\; p \;\mid\; \neg\Phi \;\mid\; \Phi_1 \wedge \Phi_2 \;\mid\; \mathrm{P}_{\bowtie a}(\phi)$$

$$\phi \;=\; \bigcirc\Phi \;\mid\; \Phi_1 \,\mathtt{U}\, \Phi_2 \;\mid\; \Phi_1 \,\mathtt{U}^{\leq n}\, \Phi_2$$

state formulas

path formulas

where

- $p \in AP$ is an atomic proposition, and
- $\bowtie \in \{<, \leq, \geq, >\}$ and $a \in \mathbb{R}$.

- Some abbreviations:

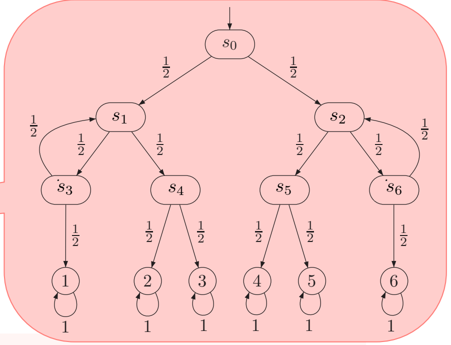
$$\mathrm{P}_{(a,b]}(\phi) \;\equiv\; \mathrm{P}_{>a}(\phi) \wedge \mathrm{P}_{\leq b}(\phi)$$

$$\mathrm{P}_{\bowtie a}(\Diamond\Phi) \;\equiv\; \mathrm{P}_{\bowtie a}(\textit{true}\,\mathtt{U}\,\Phi) \qquad \mathrm{P}_{\bowtie a}(\Diamond^{\leq n}\Phi) \;\equiv\; \mathrm{P}_{\bowtie a}(\textit{true}\,\mathtt{U}^{\leq n}\,\Phi)$$

$$\mathrm{P}_{\leq a}(\Box\Phi) \;\equiv\; \mathrm{P}_{\geq 1-a}(\Diamond\neg\Phi) \qquad \mathrm{P}_{>a}(\Box^{\leq n}\Phi) \;\equiv\; \mathrm{P}_{<1-a}(\Diamond^{\leq n}\neg\Phi)$$

in addition to the boolean abbreviations

Some examples

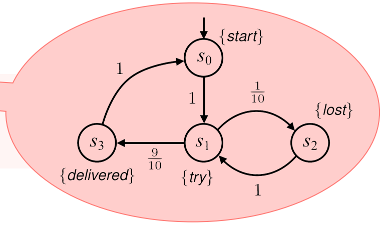


- On the “die with a coin” example:

$$\mathrm{P}_{=\frac{1}{6}}(\Diamond 1) \ \wedge\ \mathrm{P}_{=\frac{1}{6}}(\Diamond 2) \ \wedge\ \mathrm{P}_{=\frac{1}{6}}(\Diamond 3) \ \wedge\ \mathrm{P}_{=\frac{1}{6}}(\Diamond 4) \ \wedge\ \mathrm{P}_{=\frac{1}{6}}(\Diamond 5) \ \wedge\ \mathrm{P}_{=\frac{1}{6}}(\Diamond 6)$$

“Each of the six sides will eventually appear with 1/6 probability”

- On the “toy protocol”:



$$\mathrm{P}_{=1}(\Diamond \mathit{delivered})$$

“The message is almost surely delivered”

$$\mathrm{P}_{=1}\left(\Box\left(\mathit{start} \Rightarrow \mathrm{P}_{\geq 0.99}(\Diamond^{\leq 4}\mathit{delivered})\right)\right)$$

“Almost surely always each time a communication is started, the message is eventually delivered in at most 4 steps with probability 0.99”

Semantics of PCTL

A PCTL formula Φ holds in state $s \in S$ of a DTMC M, denoted by $s \models \Phi$, whenever:

state formulas

$s \models p$ iff $p \in L(s)$

$s \models \neg\Phi$ iff $s \not\models \Phi$

$s \models \Phi_1 \wedge \Phi_2$ iff $s \models \Phi_1$ and $s \models \Phi_2$

$s \models \mathtt{P}_{\bowtie a}(\phi)$ iff $\mathrm{Pr}(s \models \phi) \bowtie a$

where $\mathrm{Pr}(s \models \phi) = \mathrm{Pr}_s(\{\rho \in \mathit{Path}(s) \mid \rho \models \phi\})$ and

path formulas

$\rho \models \bigcirc\Phi$ iff $\rho(1) \models \Phi$

$\rho \models \Phi \,\mathtt{U}\, \Psi$ iff exists $j \geq 0$ s.t. $\rho(j) \models \Psi$ and for all $0 \leq k < j, \rho(k) \models \Phi$

$\rho \models \Phi \,\mathtt{U}^{\leq n}\, \Psi$ iff exists $0 \leq j \leq n$ s.t. $\rho(j) \models \Psi$ and for all $0 \leq k < j, \rho(k) \models \Phi$

Algorithm for PCTL model checking

```
fun $Sat(\Phi)$ {
    // input: a PCTL (state) formula $\Phi$
    // output: $\{s \in S \mid s \models \Phi\}$
    case {  $\Phi \in AP$                return  $\{s \in S \mid \Phi \in L(s)\}$
            $\Phi \equiv \neg\Psi$              return  $S \setminus Sat(\Psi)$
            $\Phi \equiv \Psi_1 \wedge \Psi_2$          return  $Sat(\Psi_1) \cap Sat(\Psi_2)$
            $\Phi \equiv \mathtt{P}_J(\phi)$           return  $\{s \in S \mid Prob(s, \phi) \in J\}$
    }
}

fun $Prob(s, \phi)$ {
    // input: a state $s$ and a path formula $\phi$
    // output: $\Pr_s(s \models \phi)$
    case {  $\phi \equiv \bigcirc\Phi$               return  $\left(\mathbf{P} \cdot \mathbf{1}_{Sat(\Phi)}\right)(s)$
            $\phi \equiv \Phi \ \mathtt{U}\ \Psi$            let $B = Sat(\Psi)$;  let $C = Sat(\Phi)$
                                 return  $\Pr_s(C \ \mathtt{U}\ B)$          // constrained reachability
            $\phi \equiv \Phi \ \mathtt{U}^{\leq n}\ \Psi$         let $B = Sat(\Psi)$;  let $C = Sat(\Phi)$
                                 return  $\Pr_s(C \ \mathtt{U}^{\leq n}\ B)$      // bounded constrained reachability
    }
}
```

$Prob(\ \cdot\ , \phi)$ is calculated as a matrix

Polynomial on the size of M
Linear on the size of Φ
Linear on the largest n

Markov Decision Processes

The need of non-determinism

- Parallel composition / distributed components:
  - relative probabilities of events occurring in different physical locations may be hard to estimate.
- Sub-specification:
  - many probabilities may be unknown at modeling time
- Abstraction:
  - models are intentional abstractions of the system under study
- Control synthesis and planning:
  - sub-specification is intentional to synthesize optimal decisions

Markov Decision Processes (MDP)

A MDP is a structure

$$(S, Act, \mathbf{P}, s_0, AP, L)$$

where

- S is a finite set of states, where $s_0 \in S$ is the initial state,
- Act is a finite set of actions,
- $\mathbf{P} : S \times Act \times S \to [0,1]$ is the probabilistic transition function, such that, for every $s \in S$, and $\alpha \in Act$, $\sum_{s' \in S} \mathbf{P}(s, \alpha, s') \in \{0, 1\}$, and
- $L : S \to \mathscr{P}(AP)$ is a labelling function, where AP is a a set of atomic propositions.

If $Act = \{\alpha\}$, the MDP is a DTMC

Markov Decision Processes (MDP)

A MDP is a structure

$$(S, Act, \mathbf{P}, s_0, AP, L)$$

where

- S is a finite set of states, where $s_0 \in S$ is the initial state,
- Act is a finite set of actions,
- $\mathbf{P} : S \times Act \times S \to [0,1]$ is the probabilistic transition function, such that, for every $s \in S$, and $\alpha \in Act$, $\sum_{s' \in S} \mathbf{P}(s, \alpha, s') \in \{0,1\}$, and
- $L : S \to \mathscr{P}(AP)$ is a labelling function, where AP is a a set of atomic propositions.

$\mathbf{P}(s, \alpha, s')$ is the probability to move to state s' conditioned to the system being at state s and action α being selected

α is enabled in s if $\sum_{s' \in S} \mathbf{P}(s, \alpha, s') = 1$

$Act(s)$ is the set of all actions enabled in s

At least one action should be enabled in every state

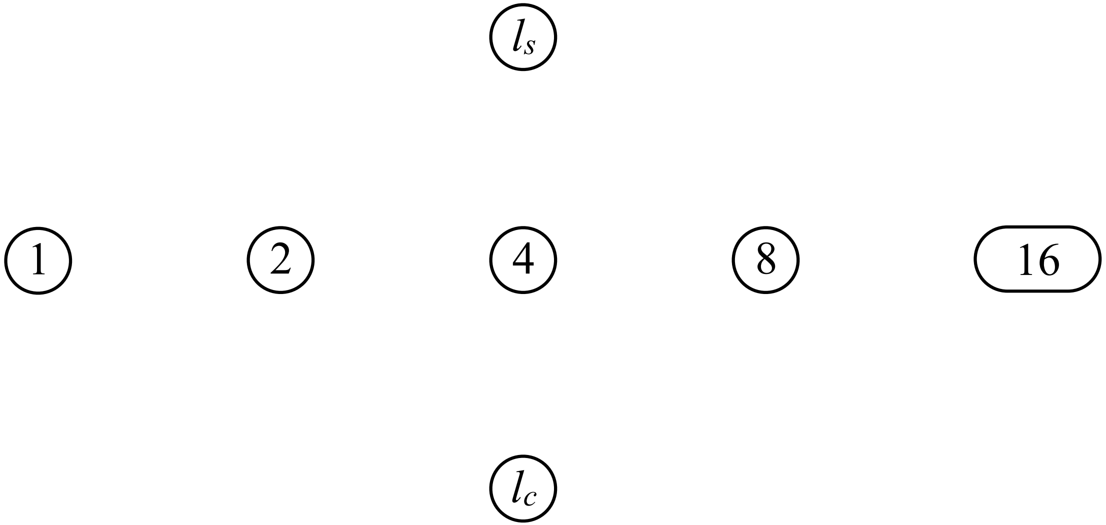
CONICET

UNC

Financial decisions

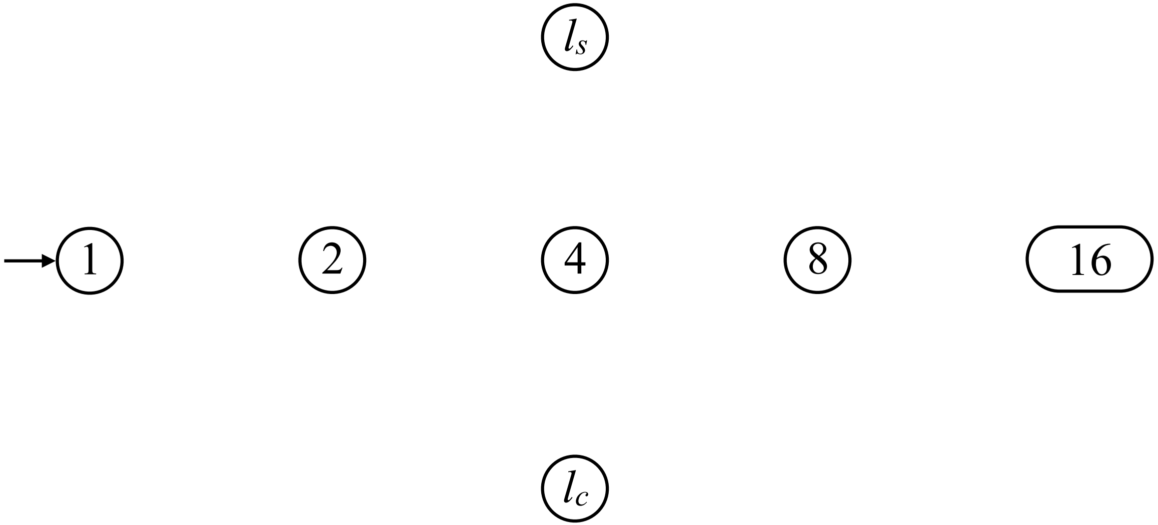
$$(S, Act, \mathbf{P}, s_0, AP, L)$$

Financial decisions



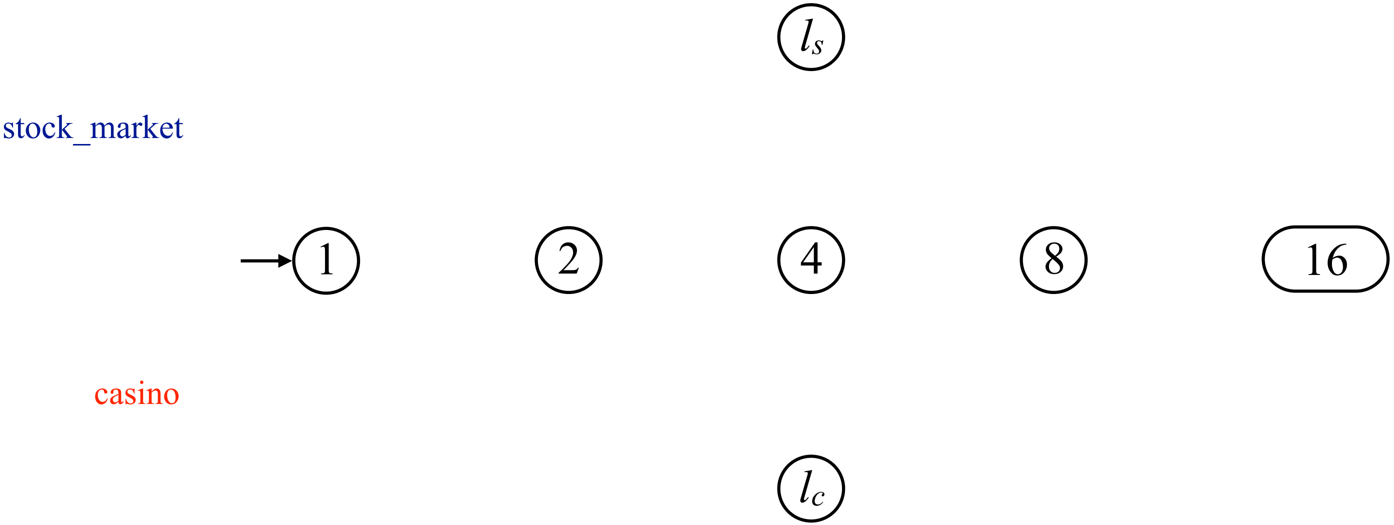
$$(S, Act, \mathbf{P}, s_0, AP, L)$$

Financial decisions



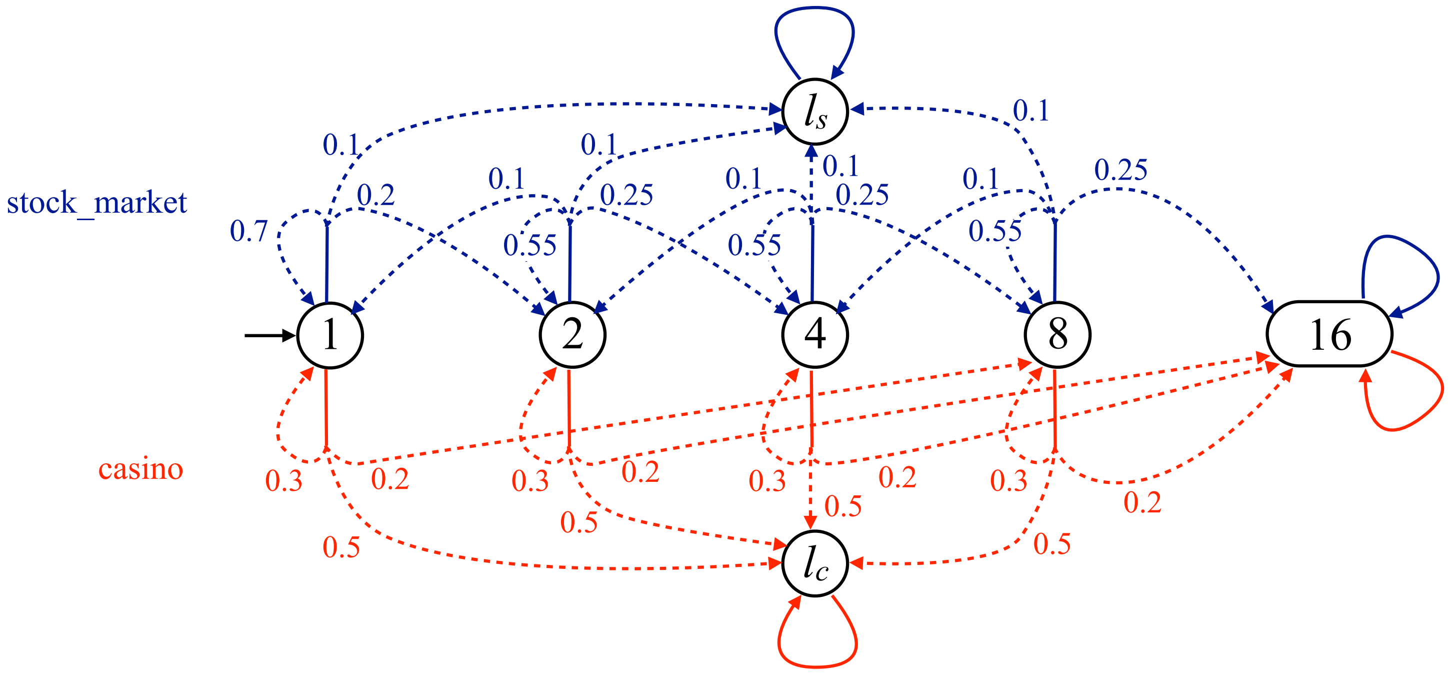
$$(S, Act, \mathbf{P}, s_0, AP, L)$$

Financial decisions



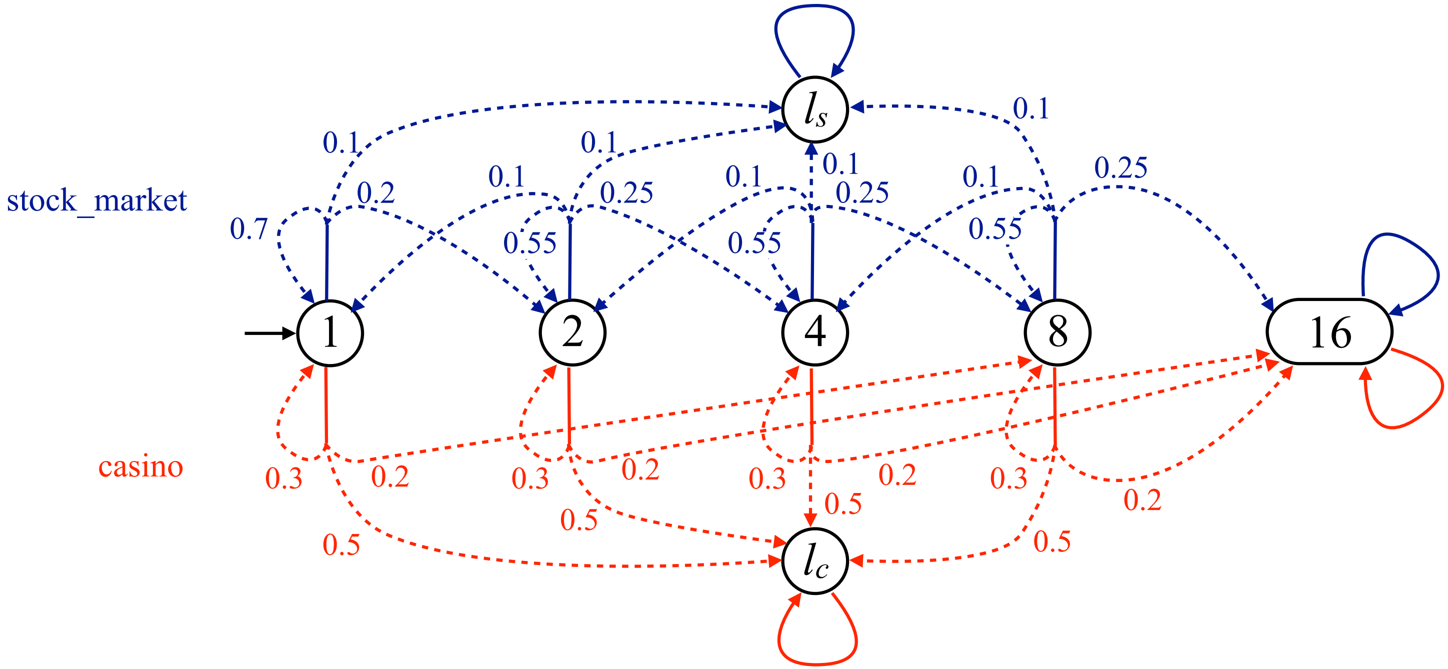
$$(S, Act, \mathbf{P}, s_0, AP, L)$$

Financial decisions



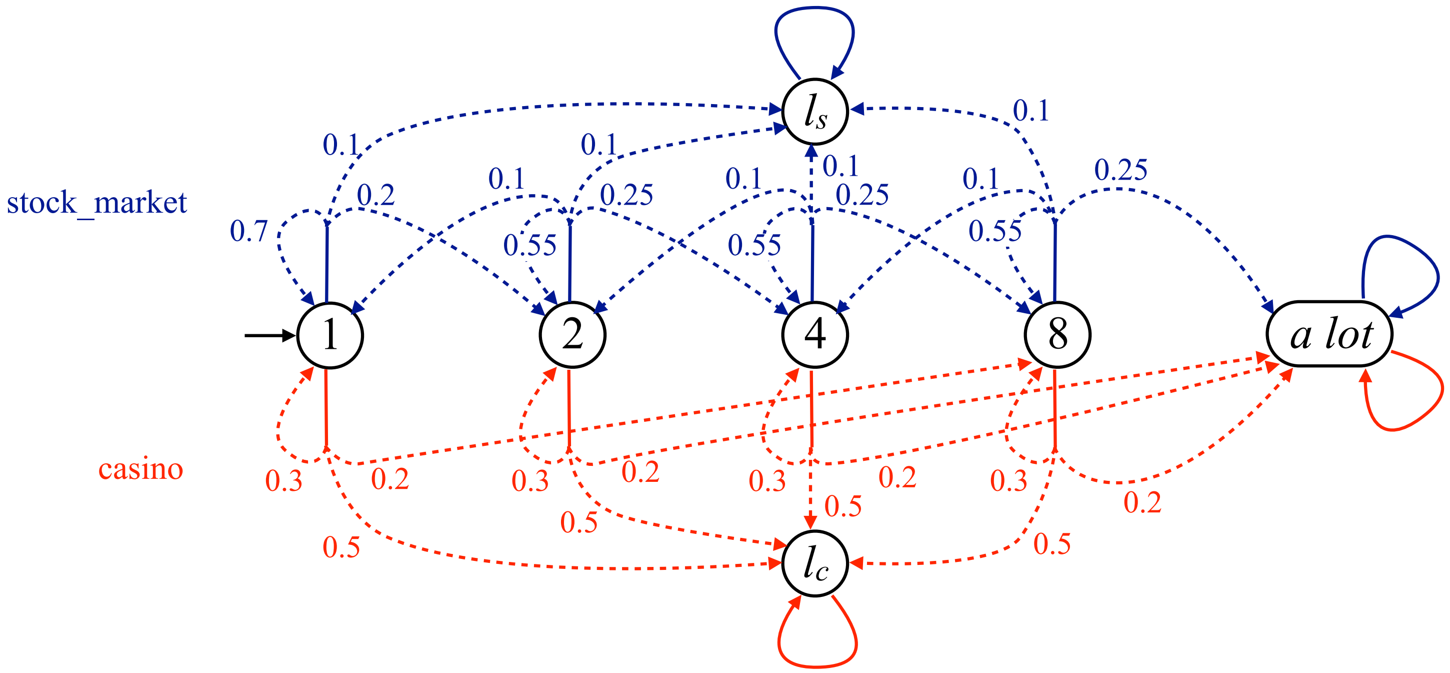
$$(S, Act, \mathbf{P}, s_0, AP, L)$$

Financial decisions



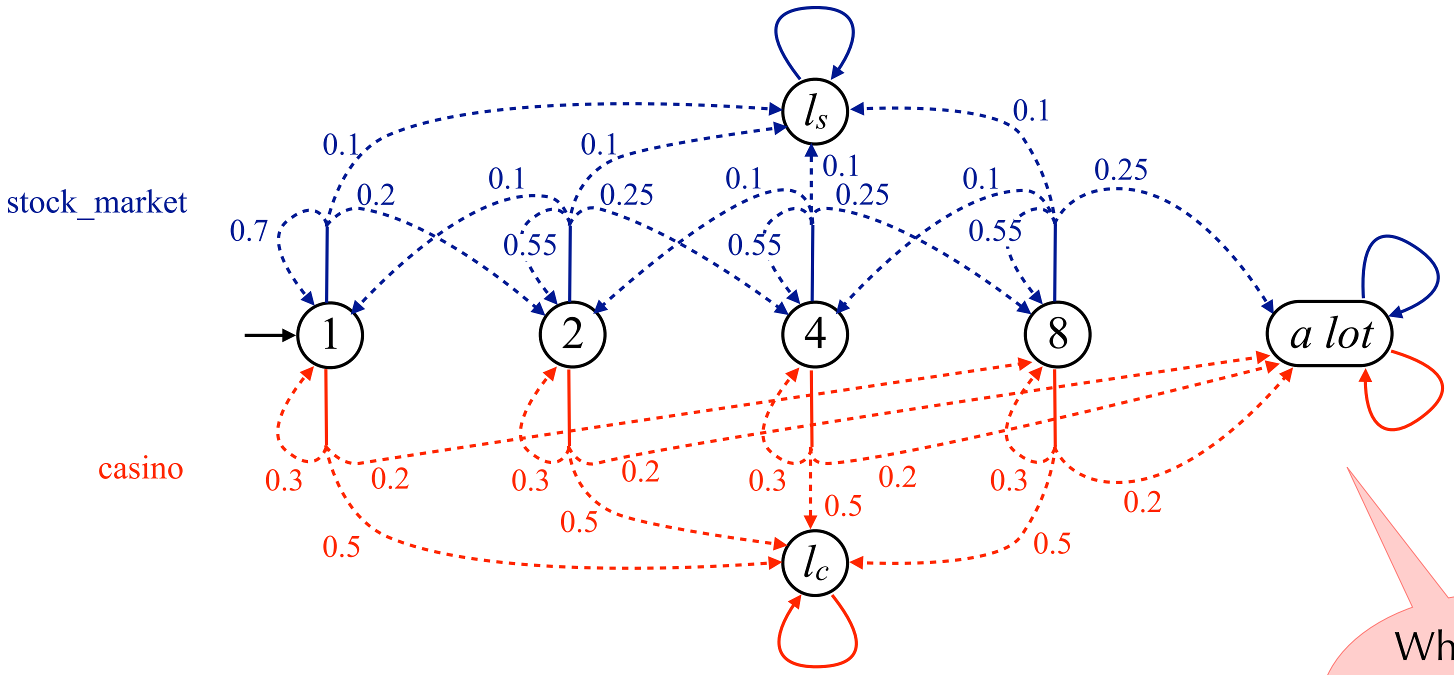
$$(S, Act, \mathbf{P}, s_0, AP, L)$$

Financial decisions



$$(S, Act, \mathbf{P}, s_0, AP, L)$$

Financial decisions

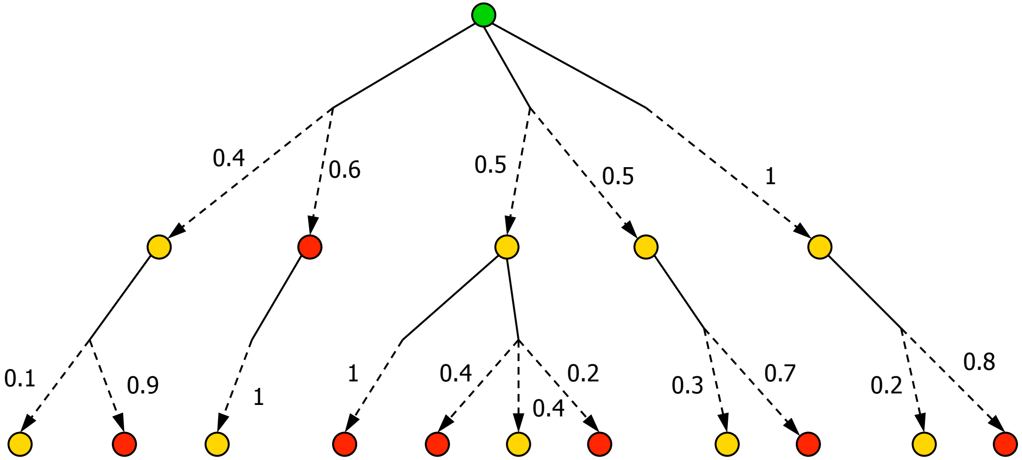


$(S, Act, \mathbf{P}, s_0, AP, L)$

What is the probability of $\Diamond$ *"a lot"*?

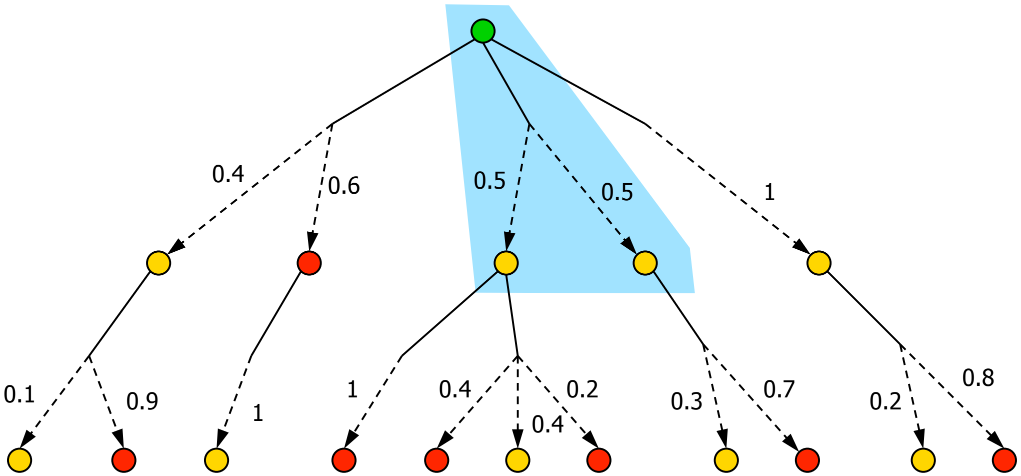
Resolving the non-determinism

- To compute the probabilities in a MDP, non-determinism needs to be resolved
- Schedulers (also adversaries or policies) are functions that select the next action based on the past execution.



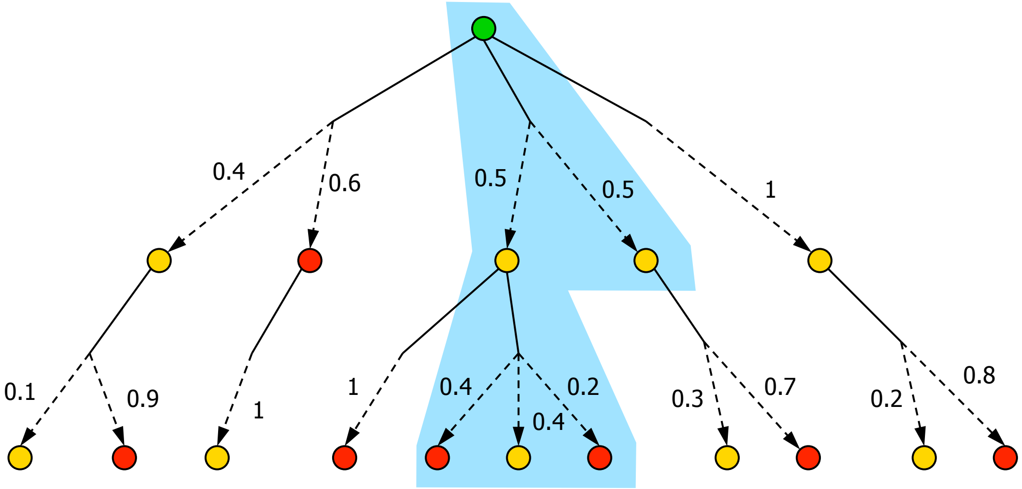
Resolving the non-determinism

- To compute the probabilities in a MDP, non-determinism needs to be resolved
- Schedulers (also adversaries or policies) are functions that select the next action based on the past execution.



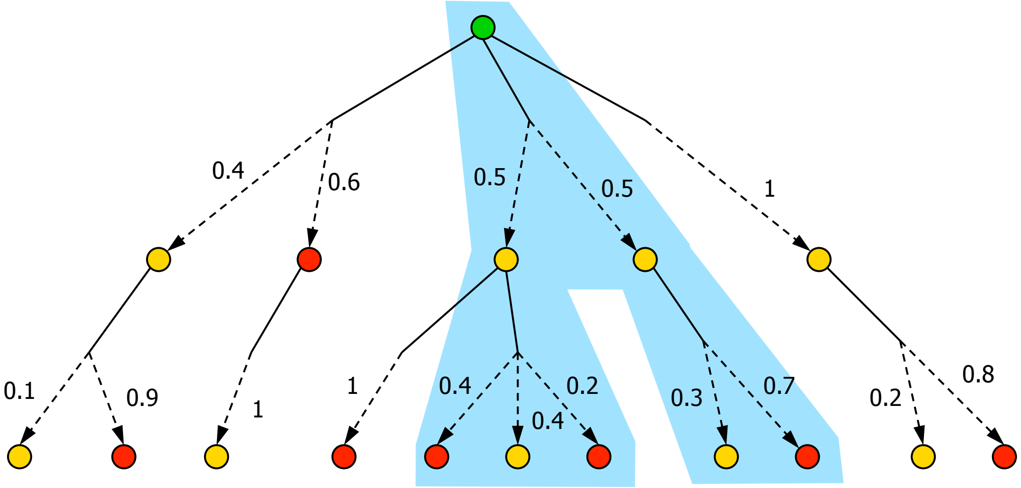
Resolving the non-determinism

- To compute the probabilities in a MDP, non-determinism needs to be resolved
- Schedulers (also adversaries or policies) are functions that select the next action based on the past execution.



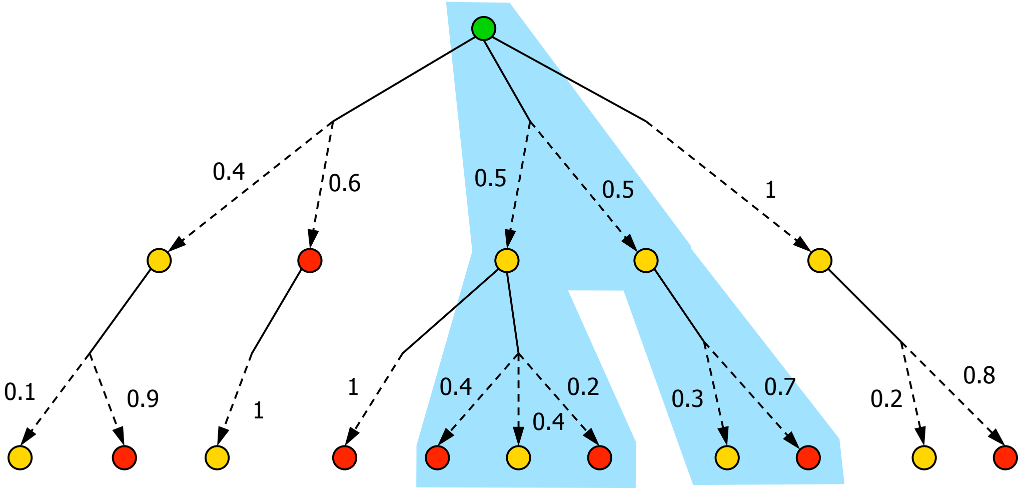
Resolving the non-determinism

- To compute the probabilities in a MDP, non-determinism needs to be resolved
- Schedulers (also adversaries or policies) are functions that select the next action based on the past execution.



Resolving the non-determinism

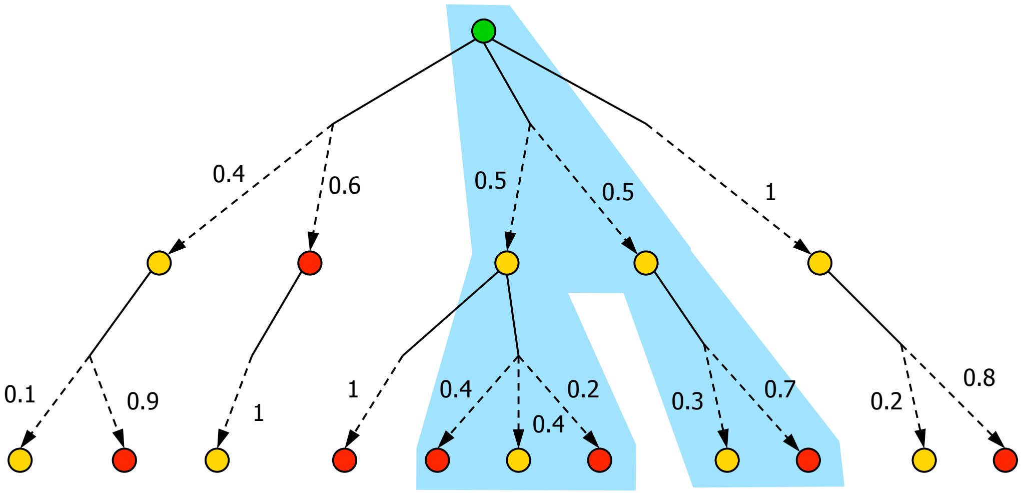
- To compute the probabilities in a MDP, non-determinism needs to be resolved
- Schedulers (also adversaries or policies) are functions that select the next action based on the past execution.



A scheduler defines a (maybe infinite) DTMC

Resolving the non-determinism

- To compute the probabilities in a MDP, non-determinism needs to be resolved
- Schedulers (also adversaries or policies) are functions that select the next action based on the past execution.



A scheduler defines a (maybe infinite) DTMC

A scheduler can also chose with randomness

Schedulers

Let $\mathcal{M} = (S, Act, \mathbf{P}, s_0, AP, L)$ be a MDP.

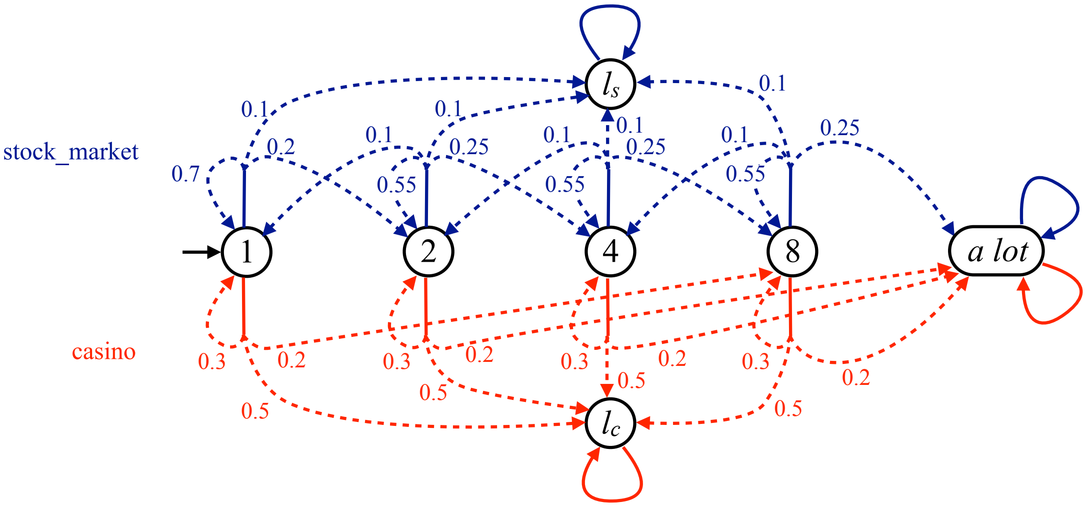
A scheduler is a funciton $\mathfrak{S} : S^+ \to Act \to [0,1]$ such that

1. $\mathfrak{S}(s_0\, s_1 \ldots s_n)$ is a probability distribution on Act, i.e., $\sum_{\alpha \in Act} \mathfrak{S}(s_0\, s_1 \ldots s_n)(\alpha) = 1$, and
2. if $\mathfrak{S}(s_0\, s_1 \ldots s_n)(\alpha) > 0$, then $\alpha \in Act(s_n)$.

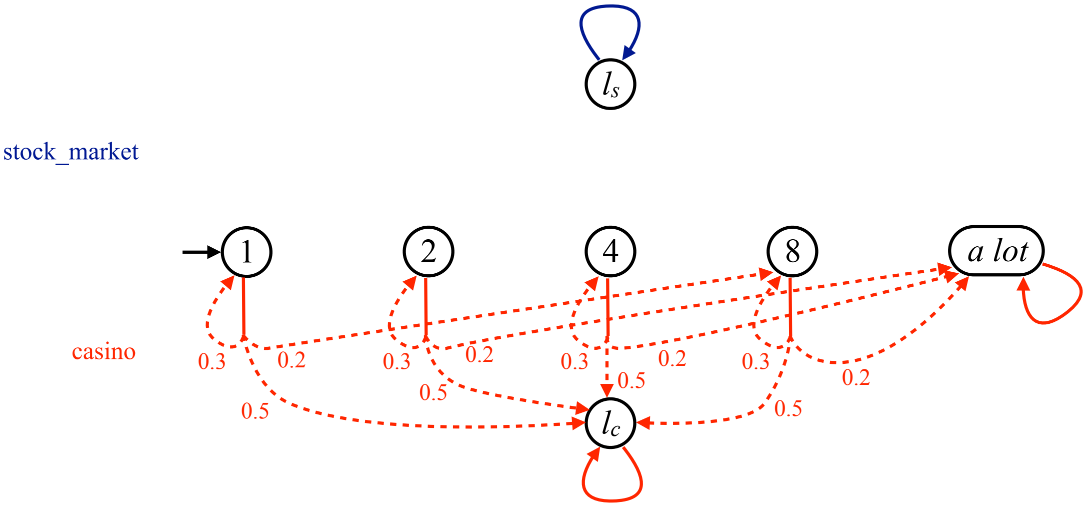
A scheduler $\mathfrak{S}$ induces the DTMC $\mathcal{M}_{\mathfrak{S}} = (S^+, \mathbf{P}_{\mathfrak{S}}, s_0, AP, L')$ where

- $\mathbf{P}_{\mathfrak{S}}(s_0\, s_1 \ldots s_n,\ s_0\, s_1 \ldots s_n\, s_{n+1}) = \sum_{\alpha \in Act} \mathfrak{S}(s_0\, s_1 \ldots s_n)(\alpha) \cdot \mathbf{P}(s_n, \alpha, s_{n+1})$
- $L'(s_0\, s_1 \ldots s_n) = L(s_n)$

DTMC induced by a scheduler



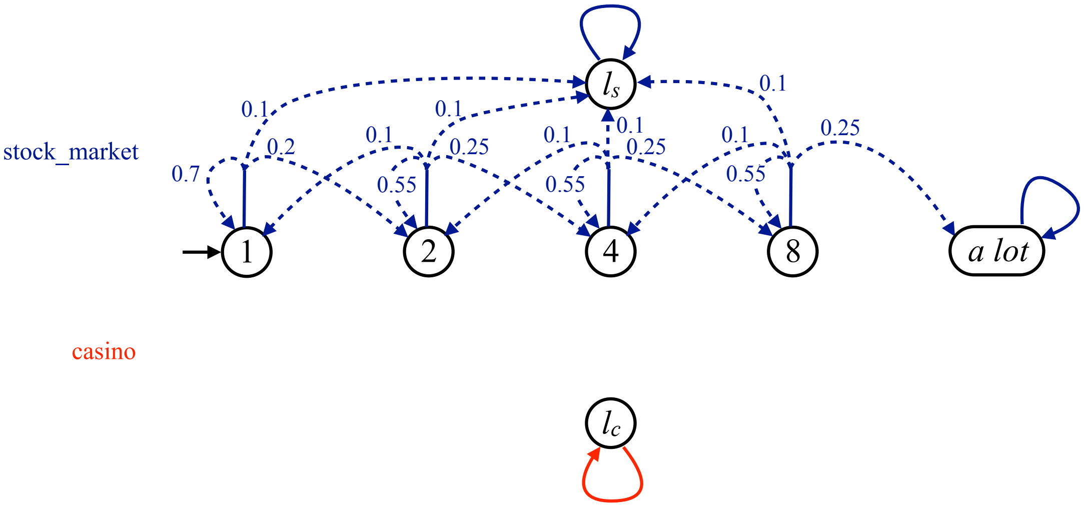
DTMC induced by a scheduler



$\mathfrak{S}$ always chooses casino

$\Pr^{\mathfrak{S}}(① \models \Diamond\text{“}a\ lot\text{”}) \approx 0.0816$

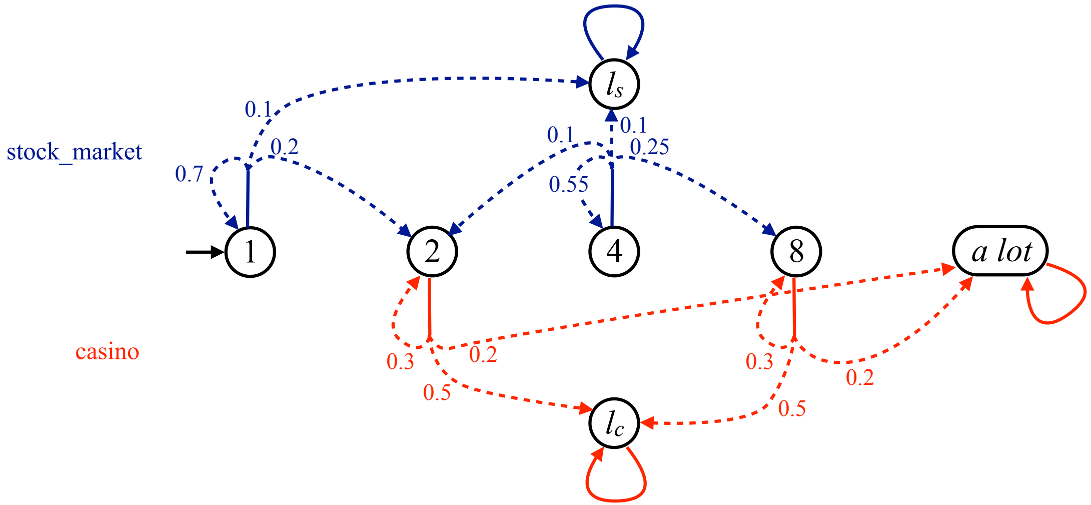
DTMC induced by a scheduler



$\mathfrak{S}$ always chooses casino $\qquad \Pr^{\mathfrak{S}}(① \models \Diamond\text{“}a\ lot\text{”}) \approx 0.0816$

$\mathfrak{S}$ always chooses stock_market $\qquad \Pr^{\mathfrak{S}}(① \models \Diamond\text{“}a\ lot\text{”}) \approx 0.0443$

DTMC induced by a scheduler

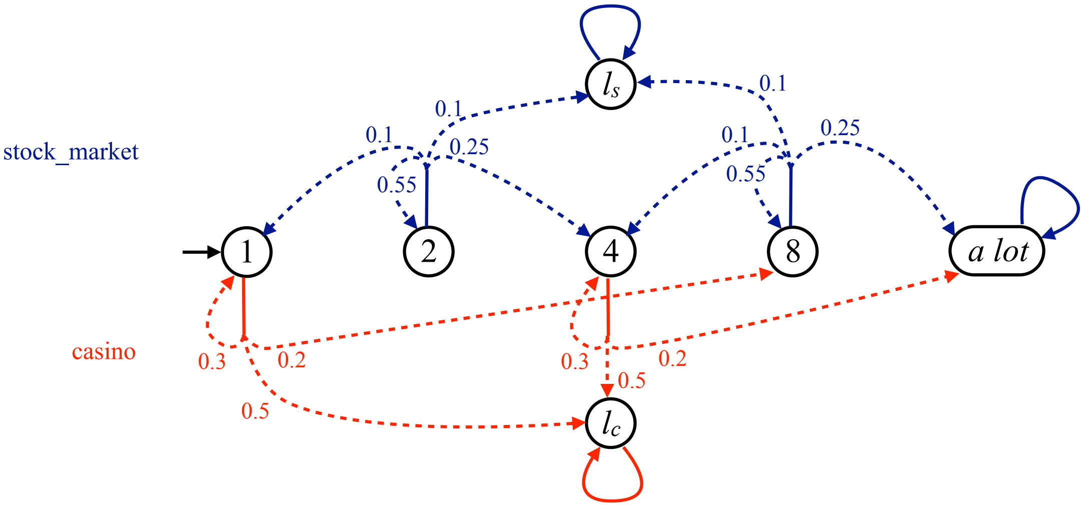


$\mathfrak{S}$ always chooses casino $\quad \Pr^{\mathfrak{S}}(\textcircled{1} \models \Diamond\text{“}a\ lot\text{”}) \approx 0.0816$

$\mathfrak{S}$ always chooses stock_market $\quad \Pr^{\mathfrak{S}}(\textcircled{1} \models \Diamond\text{“}a\ lot\text{”}) \approx 0.0443$

$\mathfrak{S}$ chooses stock_market on ① and ④ and casino otherwise $\quad \Pr^{\mathfrak{S}}(\textcircled{1} \models \Diamond\text{“}a\ lot\text{”}) \approx 0.1504$

DTMC induced by a scheduler



$\mathfrak{S}$ always chooses casino $\qquad \mathrm{Pr}^{\mathfrak{S}}(\textcircled{1} \models \Diamond\text{“}\mathit{a\ lot}\text{”}) \approx 0.0816$

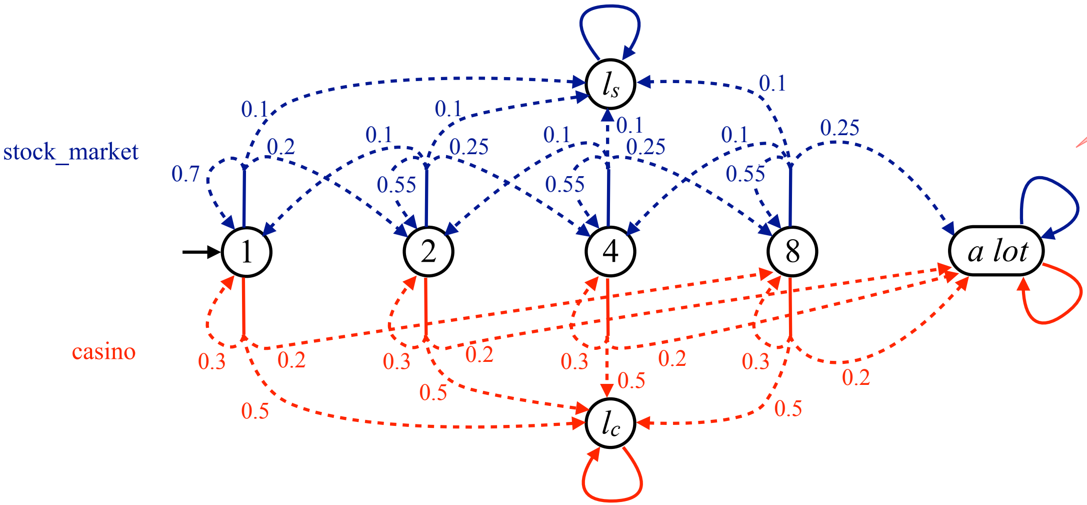
$\mathfrak{S}$ always chooses stock_market $\qquad \mathrm{Pr}^{\mathfrak{S}}(\textcircled{1} \models \Diamond\text{“}\mathit{a\ lot}\text{”}) \approx 0.0443$

$\mathfrak{S}$ chooses stock_market on ① and ④ and casino otherwise $\qquad \mathrm{Pr}^{\mathfrak{S}}(\textcircled{1} \models \Diamond\text{“}\mathit{a\ lot}\text{”}) \approx 0.1504$

$\mathfrak{S}$ chooses on the other way around $\qquad \mathrm{Pr}^{\mathfrak{S}}(\textcircled{1} \models \Diamond\text{“}\mathit{a\ lot}\text{”}) \approx 0.1332$

DTMC induced by a scheduler

But then,…
what is the probability
of $\Diamond$ *“a lot”* ??!!



$\mathfrak{S}$ always chooses casino $\qquad \Pr^{\mathfrak{S}}(① \models \Diamond\text{“}a\ lot\text{”}) \approx 0.0816$

$\mathfrak{S}$ always chooses stock_market $\qquad \Pr^{\mathfrak{S}}(① \models \Diamond\text{“}a\ lot\text{”}) \approx 0.0443$

$\mathfrak{S}$ chooses stock_market on ① and ④ and casino otherwise $\qquad \Pr^{\mathfrak{S}}(① \models \Diamond\text{“}a\ lot\text{”}) \approx 0.1504$

$\mathfrak{S}$ chooses on the other way around $\qquad \Pr^{\mathfrak{S}}(① \models \Diamond\text{“}a\ lot\text{”}) \approx 0.1332$

Supremum and infimum probabilities

- There are uncountably many resolutions
- Only the best or worst bound for the probability can guarantee the satisfaction of a property, e.g:
  - an error occurs with probability less than 0.001
  - a message is transmitted successfully with probability over 0.95
- Therefore, if Φ is the property of interest, we search for

$$\mathrm{Pr}^{\max}(s \models \Phi) \;\triangleq\; \sup_{\mathfrak{S}} \mathrm{Pr}^{\mathfrak{S}}(s \models \Phi), \quad \text{and}$$

$$\mathrm{Pr}^{\min}(s \models \Phi) \;\triangleq\; \inf_{\mathfrak{S}} \mathrm{Pr}^{\mathfrak{S}}(s \models \Phi)$$

Supremum and infimum probabilities

- There are uncountably many resolutions
- Only the best or worst bound for the probability can guarantee the satisfaction of a property, e.g:
  - an error occurs with probability less than 0.001
  - a message is transmitted successfully with probability over 0.95
- Therefore, if Φ is the property of interest, we search for

How can we calculate this?

$$\mathrm{Pr}^{\max}(s \models \Phi) \triangleq \sup_{\mathfrak{S}} \mathrm{Pr}^{\mathfrak{S}}(s \models \Phi), \quad \text{and}$$

$$\mathrm{Pr}^{\min}(s \models \Phi) \triangleq \inf_{\mathfrak{S}} \mathrm{Pr}^{\mathfrak{S}}(s \models \Phi)$$

Type of schedulers

A scheduler $\mathfrak{S}$ is:

deterministic:

if for all $s_0\, s_1 \ldots s_n$, $\mathfrak{S}(s_0\, s_1 \ldots s_n)(\alpha) = 1$ for some $\alpha \in \mathit{Act}$

memoryless:

if for all $s_0\, s_1 \ldots s_n$, $\mathfrak{S}(s_0\, s_1 \ldots s_n) = \mathfrak{S}(s_n)$

memoryless and deterministic:

if it is memoryless and deterministic at the same time ☺

CONICET

UNC

Type of schedulers

A scheduler $\mathfrak{S}$ is:

deterministic:

if for all $s_0\, s_1 \ldots s_n$, $\mathfrak{S}(s_0\, s_1 \ldots s_n)(\alpha) = 1$ for some $\alpha \in Act$

memoryless:

if for all $s_0\, s_1 \ldots s_n$, $\mathfrak{S}(s_0\, s_1 \ldots s_n) = \mathfrak{S}(s_n)$

memoryless and deterministic:

if it is memoryless and deterministic at the same time ☺

There are only finitely many of these

CONICET

UNC

Quantitative reachability

Theorem:

Let $B \subseteq S$. Then:

- There exists a memoryless and deterministic scheduler $\mathfrak{S}^{\max}$ such that

$$\Pr{}^{\mathfrak{S}^{\max}}(s \models \Diamond B) \;=\; \Pr{}^{\max}(s \models \Diamond B)$$

- There exists a memoryless and deterministic scheduler $\mathfrak{S}^{\min}$ such that

$$\Pr{}^{\mathfrak{S}^{\min}}(s \models \Diamond B) \;=\; \Pr{}^{\min}(s \models \Diamond B)$$

Quantitative reachability

Not any property!
only reachability

Theorem:

Let $B \subseteq S$. Then:

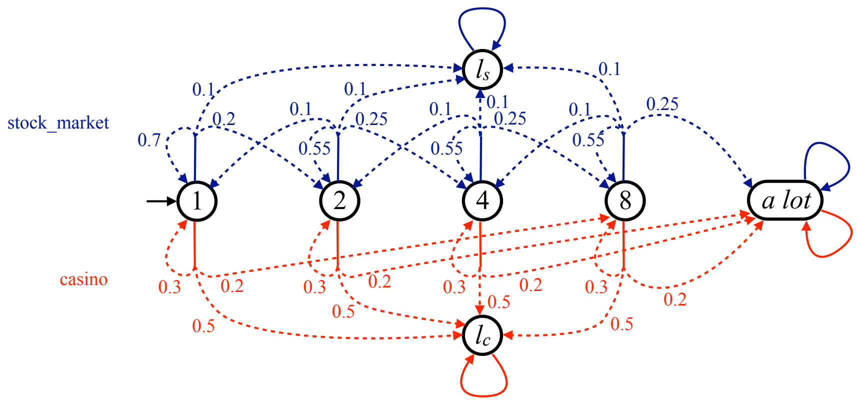
- There exists a memoryless and deterministic scheduler $\mathfrak{S}^{\max}$ such that

$$\Pr^{\mathfrak{S}^{\max}}(s \models \Diamond B) \;=\; \Pr^{\max}(s \models \Diamond B)$$

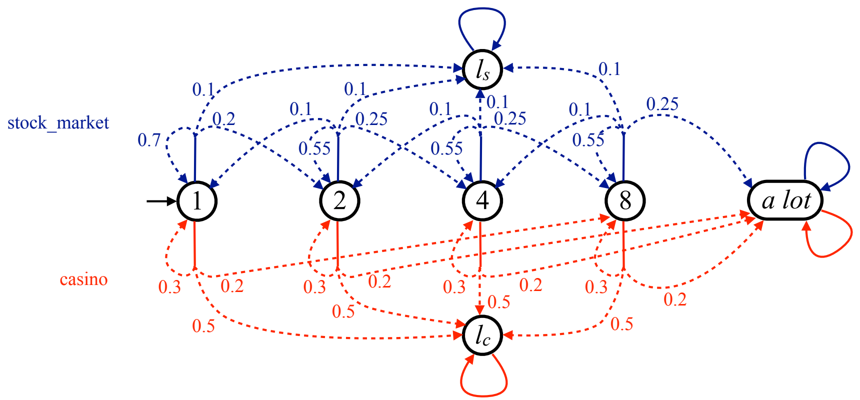
- There exists a memoryless and deterministic scheduler $\mathfrak{S}^{\min}$ such that

$$\Pr^{\mathfrak{S}^{\min}}(s \models \Diamond B) \;=\; \Pr^{\min}(s \models \Diamond B)$$

Quantitative reachability



Quantitative reachability

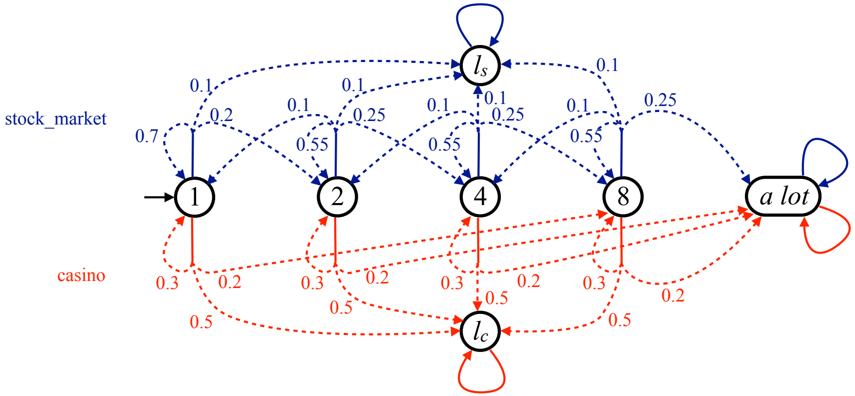


P_s^+ is abbreviates

$\mathrm{Pr}^{\max}(s \models \Diamond \text{“}a\ lot\text{”})$

$$P^+_{l_s} = P^+_{l_c} = 0$$

Quantitative reachability

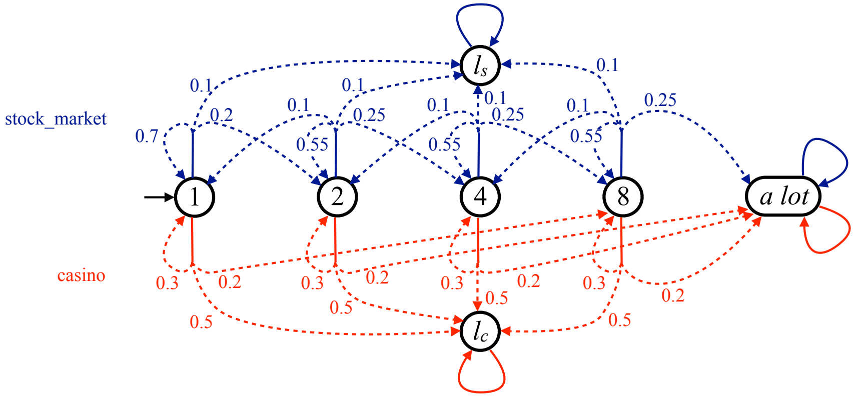


P_s^+ is abbreviates $\Pr^{\max}(s \models \Diamond \text{“}a\ lot\text{”})$

$$P_{l_s}^+ = P_{l_c}^+ = 0$$

$$P_{al}^+ = 1$$

Quantitative reachability



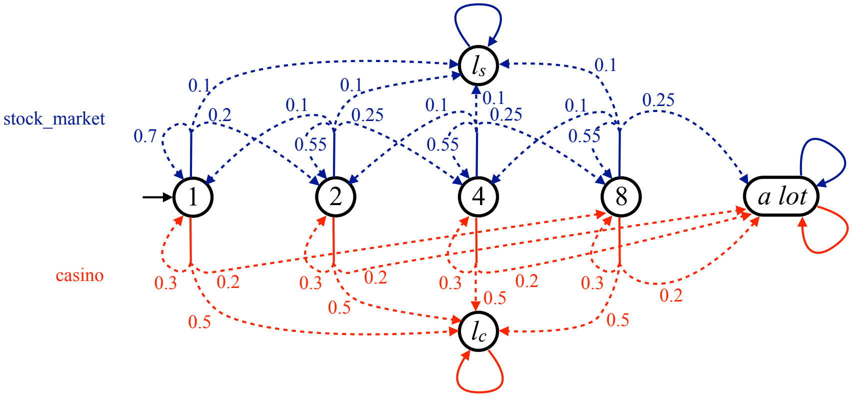
P^+_s is abbreviates $\Pr^{\max}(s \models \Diamond\text{“}a\ lot\text{”})$

$$P^+_{l_s} = P^+_{l_c} = 0$$

$$P^+_{al} = 1$$

$$P^+_1 =$$

Quantitative reachability



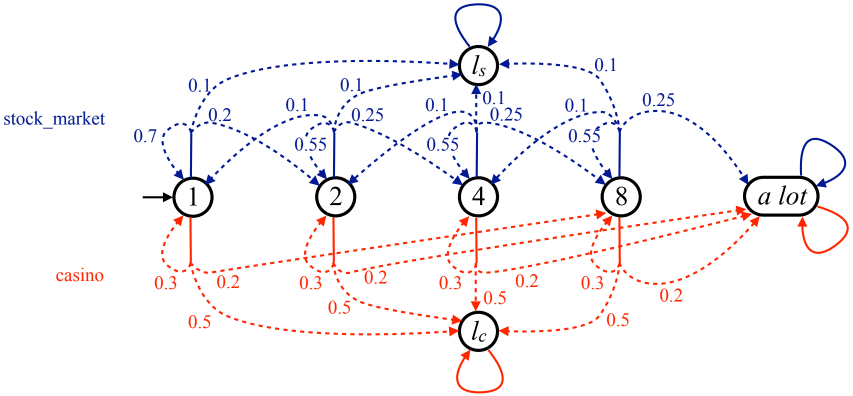
P^+_s is abbreviates $\mathrm{Pr}^{\max}(s \models \Diamond\text{“}a\ lot\text{”})$

$$P^+_{l_s} = P^+_{l_c} = 0$$

$$P^+_{al} = 1$$

$$P^+_1 = 0.7\, P^+_1 + 0.2\, P^+_2 + 0.1\, P^+_{l_s}$$

Quantitative reachability



P_s^+ is abbreviates $\Pr^{\max}(s \models \Diamond \text{“}a\ lot\text{''})$

$$P_{l_s}^+ = P_{l_c}^+ = 0$$

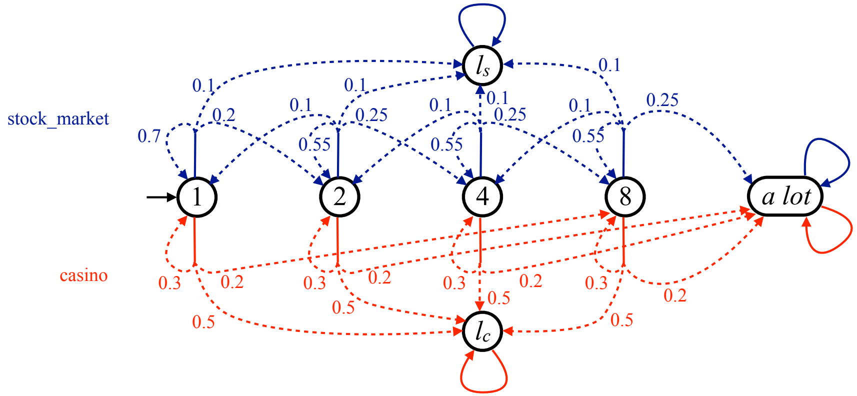
$$P_{al}^+ = 1$$

$$P_1^+ = \qquad 0.3\,P_1^+ + 0.2\,P_8^+ + 0.5\,P_{l_c}^+$$

CONICET

UNC

Quantitative reachability



P_s^+ is abbreviates

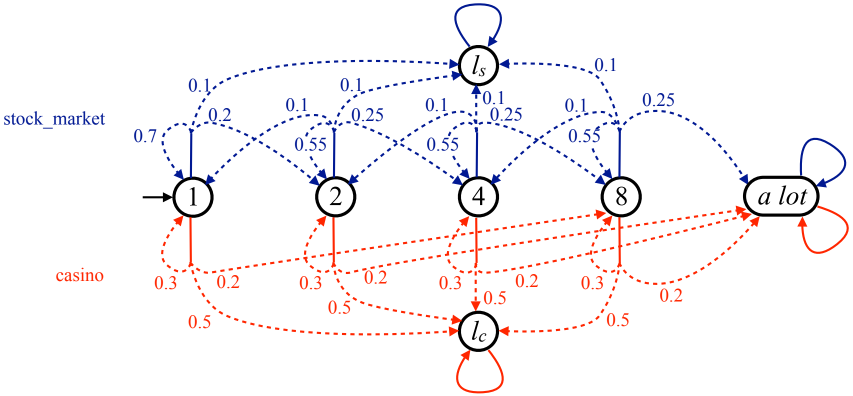
$\Pr^{\max}(s \models \Diamond\text{“}a\ lot\text{”})$

$$P_{l_s}^+ = P_{l_c}^+ = 0$$

$$P_{al}^+ = 1$$

$$P_1^+ = \max\left(\, 0.7\, P_1^+ + 0.2\, P_2^+ + 0.1\, P_{l_s}^+ \,,\; 0.3\, P_1^+ + 0.2\, P_8^+ + 0.5\, P_{l_c}^+ \,\right)$$

Quantitative reachability



P_s^+ is abbreviates

$\mathrm{Pr}^{\max}(s \models \Diamond\text{“}a\ lot\text{”})$

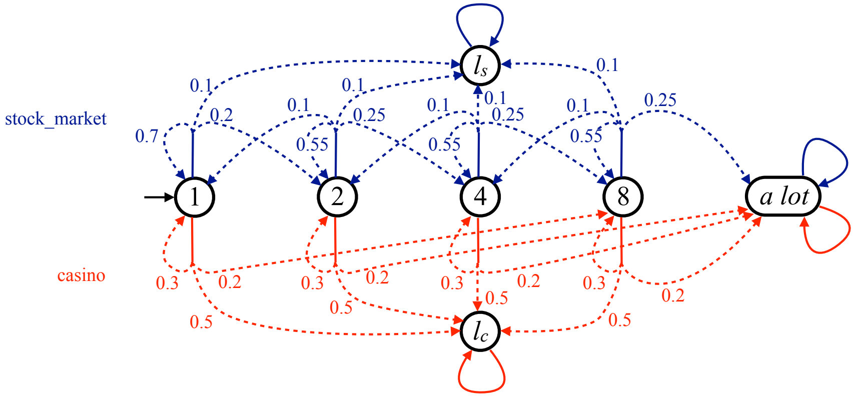
$$P_{l_s}^+ = P_{l_c}^+ = 0$$

$$P_{al}^+ = 1$$

$$P_1^+ = \max\left(0.7\,P_1^+ + 0.2\,P_2^+ + 0.1\,P_{l_s}^+ \,,\; 0.3\,P_1^+ + 0.2\,P_8^+ + 0.5\,P_{l_c}^+ \right)$$

$$P_2^+ = \max\left(0.55\,P_2^+ + 0.25\,P_4^+ + 0.1\,P_1^+ + 0.1\,P_{ls}^+ \,,\; 0.3\,P_2^+ + 0.2\,P_{al}^+ + 0.5\,P_{l+c}^+ \right)$$

Quantitative reachability



P_s^+ is abbreviates

$\mathrm{Pr}^{\max}(s \models \Diamond\text{“}a\ lot\text{”})$

$$P^+_{l_s} = P^+_{l_c} = 0$$

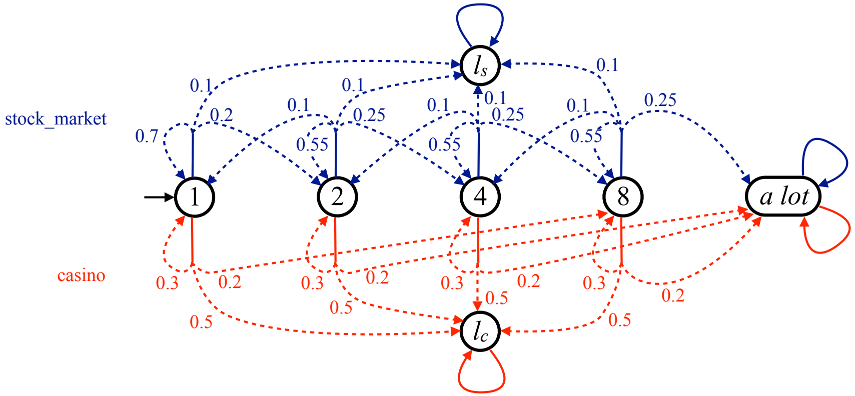
$$P^+_{al} = 1$$

$$P^+_1 = \max\left(0.7\, P^+_1 + 0.2\, P^+_2 + 0.1\, P^+_{l_s} \;,\; 0.3\, P^+_1 + 0.2\, P^+_8 + 0.5\, P^+_{l_c} \right)$$

$$P^+_2 = \max\left(0.55\, P^+_2 + 0.25\, P^+_4 + 0.1\, P^+_1 + 0.1\, P^+_{ls} \;,\; 0.3\, P^+_2 + 0.2\, P^+_{al} + 0.5\, P^+_{l+c} \right)$$

$$P^+_3 = \max\left(0.55\, P^+_4 + 0.25\, P^+_8 + 0.1\, P^+_2 + 0.1\, P^+_{ls} \;,\; 0.3\, P^+_4 + 0.2\, P^+_{al} + 0.5\, P^+_{l+c} \right)$$

Quantitative reachability



P_s^+ is abbreviates

$\Pr^{\max}(s \models \Diamond\text{“}a\ lot\text{”})$

$$P^+_{l_s} = P^+_{l_c} = 0$$

$$P^+_{al} = 1$$

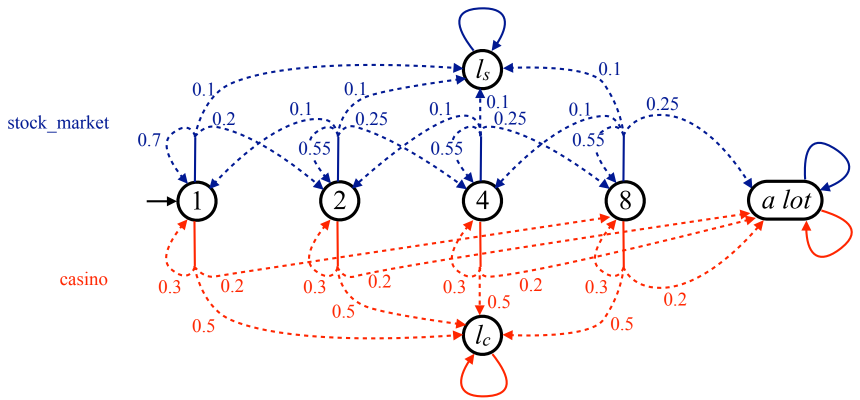
$$P^+_1 = \max\left(\,0.7\,P^+_1 + 0.2\,P^+_2 + 0.1\,P^+_{l_s}\;,\;0.3\,P^+_1 + 0.2\,P^+_8 + 0.5\,P^+_{l_c}\,\right)$$

$$P^+_2 = \max\left(\,0.55\,P^+_2 + 0.25\,P^+_4 + 0.1\,P^+_1 + 0.1\,P^+_{ls}\;,\;0.3\,P^+_2 + 0.2\,P^+_{al} + 0.5\,P^+_{l+c}\,\right)$$

$$P^+_3 = \max\left(\,0.55\,P^+_4 + 0.25\,P^+_8 + 0.1\,P^+_2 + 0.1\,P^+_{ls}\;,\;0.3\,P^+_4 + 0.2\,P^+_{al} + 0.5\,P^+_{l+c}\,\right)$$

$$P^+_4 = \max\left(\,0.55\,P^+_8 + 0.25\,P^+_{al} + 0.1\,P^+_4 + 0.1\,P^+_{ls}\;,\;0.3\,P^+_8 + 0.2\,P^+_{al} + 0.5\,P^+_{l+c}\,\right)$$

Quantitative reachability



$$\mathrm{Pr}^{\max}(\textcircled{1} \models \Diamond \text{“}a\ lot\text{”}) \;\approx\; 0.1905$$

and the (memoryless and determinstic) scheduler $\mathfrak{S}$ that maximizes it is

$\mathfrak{S}(\textcircled{1}) = \text{stock\_market}$ $\mathfrak{S}(\textcircled{4}) = \text{stock\_market}$

$\mathfrak{S}(\textcircled{2}) = \text{casino}$ $\mathfrak{S}(\textcircled{8}) = \text{stock\_market}$

Quantitative reachability (max)

Theorem:

The family of values $\{\mathbf{x}_s\}_{s\in S}$ with $\mathbf{x}_s = \mathrm{Pr}^{\max}(s \models \Diamond B)$ is the unique solution to the following equation system:

$$
\begin{aligned}
x_s &= 1 && \text{if } s \in B \\
x_s &= 0 && \text{if } \mathrm{Pr}^{\max}(s \models \Diamond B) = 0 \\
x_s &= \max\left\{\textstyle\sum_{t\in S} \mathbf{P}(s,\alpha,t)\cdot x_t \mid \alpha \in \mathit{Act}(s)\right\} && \text{if } \mathrm{Pr}^{\max}(s \models \Diamond B) > 0 \text{ and } s \notin B
\end{aligned}
$$

Quantitative reachability (max)

Theorem:

The family of values $\{\mathbf{x}_s\}_{s\in S}$ with $\mathbf{x}_s = \mathrm{Pr}^{\max}(s \models \Diamond B)$ is the unique solution to the following equation system:

$$\begin{aligned}
x_s &= 1 && \text{if } s \in B \\
x_s &= 0 && \text{if } \mathrm{Pr}^{\max}(s \models \Diamond B) = 0 \\
x_s &= \max\left\{\textstyle\sum_{t\in S} \mathbf{P}(s,\alpha,t)\cdot x_t \mid \alpha \in Act(s)\right\} && \text{if } \mathrm{Pr}^{\max}(s \models \Diamond B) > 0 \text{ and } s \notin B
\end{aligned}$$

The Bellman equations can be computed with a fixed-point iteration

… but how can the conditions be calculated?

UNC

Qualitative reachability (max)

Lemma: Let $\mathcal{M} = (S, Act, \mathbf{P}, s_0, AP, L)$ be a MDP and let $B \subseteq S$ be a set of absorbing states. Then, for $s \in S$,

❖ $\Pr^{\max}(s \models \Diamond B) > 0 \quad \text{iff} \quad s \in \exists Pre^*(B)$

❖ $\Pr^{\max}(s \models \Diamond B) = 0 \quad \text{iff} \quad s \in S \backslash \exists Pre^*(B)$

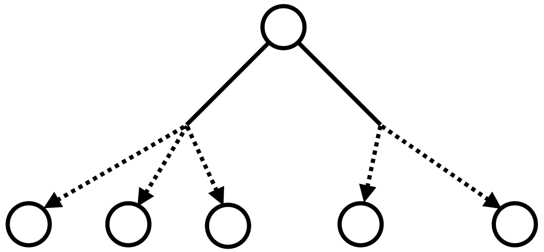
❖ $\Pr^{\max}(s \models \Diamond B) < 1 \quad \text{iff} \quad s \in \forall Pre^*(S \backslash \exists Pre^*(B))$

❖ $\Pr^{\max}(s \models \Diamond B) = 1 \quad \text{iff} \quad s \in S \backslash \forall Pre^*(S \backslash \exists Pre^*(B))$

where

$$\exists Pre(C) \triangleq \{s \in S \mid \exists \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\}$$

$$\forall Pre(C) \triangleq \{s \in S \mid \forall \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\}$$



Qualitative reachability (max)

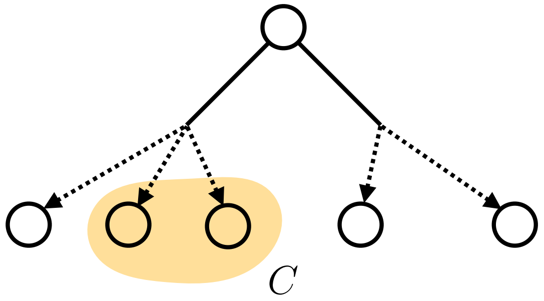
Lemma: Let $\mathcal{M} = (S, Act, \mathbf{P}, s_0, AP, L)$ be a MDP and let $B \subseteq S$ be a set of absorbing states. Then, for $s \in S$,

- $\Pr^{\max}(s \models \Diamond B) > 0 \quad \text{iff} \quad s \in \exists Pre^*(B)$
- $\Pr^{\max}(s \models \Diamond B) = 0 \quad \text{iff} \quad s \in S \backslash \exists Pre^*(B)$
- $\Pr^{\max}(s \models \Diamond B) < 1 \quad \text{iff} \quad s \in \forall Pre^*(S \backslash \exists Pre^*(B))$
- $\Pr^{\max}(s \models \Diamond B) = 1 \quad \text{iff} \quad s \in S \backslash \forall Pre^*(S \backslash \exists Pre^*(B))$

where

$$\exists Pre(C) \triangleq \{s \in S \mid \exists \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\}$$

$$\forall Pre(C) \triangleq \{s \in S \mid \forall \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\}$$



Qualitative reachability (max)

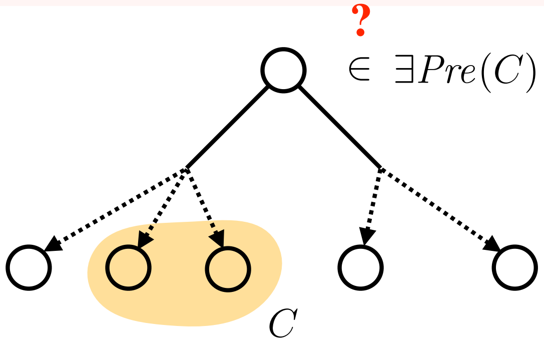
Lemma: Let $\mathcal{M} = (S, Act, \mathbf{P}, s_0, AP, L)$ be a MDP and let $B \subseteq S$ be a set of absorbing states. Then, for $s \in S$,

- $\Pr^{\max}(s \models \Diamond B) > 0 \quad \text{iff} \quad s \in \exists Pre^*(B)$
- $\Pr^{\max}(s \models \Diamond B) = 0 \quad \text{iff} \quad s \in S \backslash \exists Pre^*(B)$
- $\Pr^{\max}(s \models \Diamond B) < 1 \quad \text{iff} \quad s \in \forall Pre^*(S \backslash \exists Pre^*(B))$
- $\Pr^{\max}(s \models \Diamond B) = 1 \quad \text{iff} \quad s \in S \backslash \forall Pre^*(S \backslash \exists Pre^*(B))$

where

$$\exists Pre(C) \triangleq \{s \in S \mid \exists \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\}$$

$$\forall Pre(C) \triangleq \{s \in S \mid \forall \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\}$$



Qualitative reachability (max)

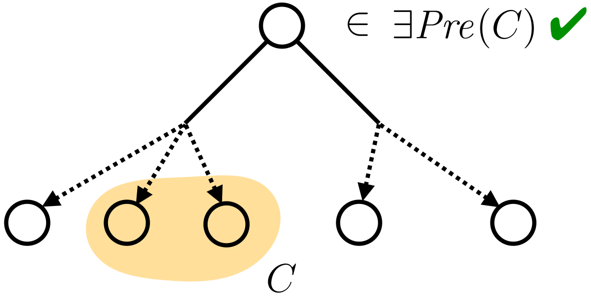
Lemma: Let $\mathcal{M} = (S, Act, \mathbf{P}, s_0, AP, L)$ be a MDP and let $B \subseteq S$ be a set of absorbing states. Then, for $s \in S$,

- $\Pr^{\max}(s \models \Diamond B) > 0$ iff $s \in \exists Pre^*(B)$
- $\Pr^{\max}(s \models \Diamond B) = 0$ iff $s \in S \backslash \exists Pre^*(B)$
- $\Pr^{\max}(s \models \Diamond B) < 1$ iff $s \in \forall Pre^*(S \backslash \exists Pre^*(B))$
- $\Pr^{\max}(s \models \Diamond B) = 1$ iff $s \in S \backslash \forall Pre^*(S \backslash \exists Pre^*(B))$

where

$$\exists Pre(C) \triangleq \{s \in S \mid \exists \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\}$$

$$\forall Pre(C) \triangleq \{s \in S \mid \forall \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\}$$



CONICET

UNC

Qualitative reachability (max)

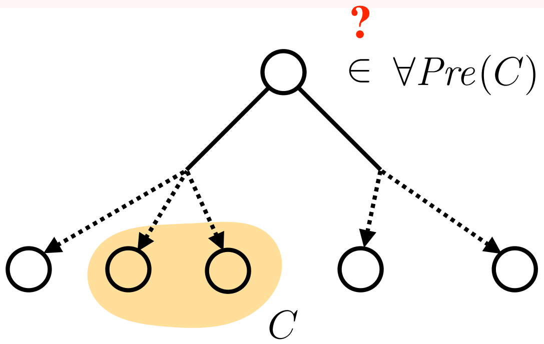
Lemma: Let $\mathcal{M} = (S, Act, \mathbf{P}, s_0, AP, L)$ be a MDP and let $B \subseteq S$ be a set of absorbing states.
Then, for $s \in S$,

- $\Pr^{\max}(s \models \Diamond B) > 0$ iff $s \in \exists Pre^*(B)$
- $\Pr^{\max}(s \models \Diamond B) = 0$ iff $s \in S \setminus \exists Pre^*(B)$
- $\Pr^{\max}(s \models \Diamond B) < 1$ iff $s \in \forall Pre^*(S \setminus \exists Pre^*(B))$
- $\Pr^{\max}(s \models \Diamond B) = 1$ iff $s \in S \setminus \forall Pre^*(S \setminus \exists Pre^*(B))$

where

$$\exists Pre(C) \triangleq \{s \in S \mid \exists \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\}$$

$$\forall Pre(C) \triangleq \{s \in S \mid \forall \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\}$$



Qualitative reachability (max)

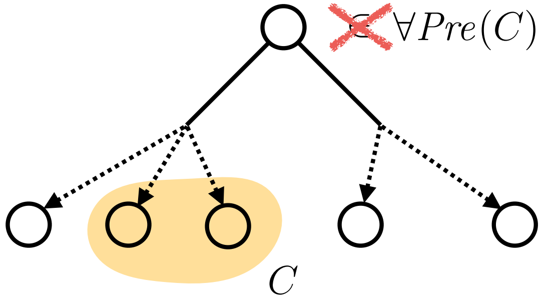
Lemma: Let $\mathcal{M} = (S, Act, \mathbf{P}, s_0, AP, L)$ be a MDP and let $B \subseteq S$ be a set of absorbing states. Then, for $s \in S$,

- $\mathrm{Pr}^{\max}(s \models \Diamond B) > 0$ iff $s \in \exists Pre^*(B)$
- $\mathrm{Pr}^{\max}(s \models \Diamond B) = 0$ iff $s \in S \backslash \exists Pre^*(B)$
- $\mathrm{Pr}^{\max}(s \models \Diamond B) < 1$ iff $s \in \forall Pre^*(S \backslash \exists Pre^*(B))$
- $\mathrm{Pr}^{\max}(s \models \Diamond B) = 1$ iff $s \in S \backslash \forall Pre^*(S \backslash \exists Pre^*(B))$

where

$$\exists Pre(C) \triangleq \{s \in S \mid \exists \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\}$$

$$\forall Pre(C) \triangleq \{s \in S \mid \forall \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\}$$



Qualitative reachability (max)

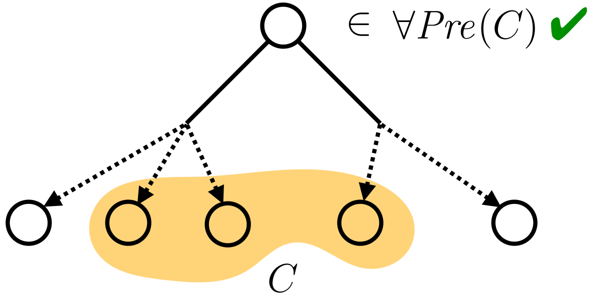
Lemma: Let $\mathcal{M} = (S, Act, \mathbf{P}, s_0, AP, L)$ be a MDP and let $B \subseteq S$ be a set of absorbing states. Then, for $s \in S$,

- $\Pr^{\max}(s \models \Diamond B) > 0 \quad \text{iff} \quad s \in \exists Pre^*(B)$
- $\Pr^{\max}(s \models \Diamond B) = 0 \quad \text{iff} \quad s \in S \backslash \exists Pre^*(B)$
- $\Pr^{\max}(s \models \Diamond B) < 1 \quad \text{iff} \quad s \in \forall Pre^*(S \backslash \exists Pre^*(B))$
- $\Pr^{\max}(s \models \Diamond B) = 1 \quad \text{iff} \quad s \in S \backslash \forall Pre^*(S \backslash \exists Pre^*(B))$

where

$$\exists Pre(C) \triangleq \{s \in S \mid \exists \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\}$$

$$\forall Pre(C) \triangleq \{s \in S \mid \forall \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\}$$



Qualitative reachability (max)

Lemma: Let $\mathcal{M} = (S, Act, \mathbf{P}, s_0, AP, L)$ be a MDP and let $B \subseteq S$ be a set of absorbing states. Then, for $s \in S$,

- $\Pr^{\max}(s \models \Diamond B) > 0$ iff $s \in \exists Pre^*(B)$
- $\Pr^{\max}(s \models \Diamond B) = 0$ iff $s \in S \backslash \exists Pre^*(B)$
- $\Pr^{\max}(s \models \Diamond B) < 1$ iff $s \in \forall Pre^*(S \backslash \exists Pre^*(B))$
- $\Pr^{\max}(s \models \Diamond B) = 1$ iff $s \in S \backslash \forall Pre^*(S \backslash \exists Pre^*(B))$

where

$$\exists Pre(C) \triangleq \{s \in S \mid \exists \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\} \qquad \exists Pre^*(C) \triangleq \bigcup_{n \geq 0} \exists Pre^n(C)$$

$$\forall Pre(C) \triangleq \{s \in S \mid \forall \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\} \qquad \forall Pre^*(C) \triangleq \bigcup_{n \geq 0} \forall Pre^n(C)$$

Qualitative reachability (max)

Lemma: Let $\mathcal{M} = (S, Act, \mathbf{P}, s_0, AP, L)$ be a MDP and let $B \subseteq S$ be a set of absorbing states. Then, for $s \in S$,

- $\Pr^{\max}(s \models \Diamond B) > 0 \quad \text{iff} \quad s \in \exists Pre^*(B)$
- $\Pr^{\max}(s \models \Diamond B) = 0 \quad \text{iff} \quad s \in S \backslash \exists Pre^*(B)$
- $\Pr^{\max}(s \models \Diamond B) < 1 \quad \text{iff} \quad s \in \forall Pre^*(S \backslash \exists Pre^*(B))$
- $\Pr^{\max}(s \models \Diamond B) = 1 \quad \text{iff} \quad s \in S \backslash \forall Pre^*(S \backslash \exists Pre^*(B))$

$\mathcal{O}(size(\mathcal{M}))$

where

$$\exists Pre(C) \triangleq \{s \in S \mid \exists \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\} \qquad \exists Pre^*(C) \triangleq \textstyle\bigcup_{n \geq 0} \exists Pre^n(C)$$

$$\forall Pre(C) \triangleq \{s \in S \mid \forall \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\} \qquad \forall Pre^*(C) \triangleq \textstyle\bigcup_{n \geq 0} \forall Pre^n(C)$$

Qualitative reachability (max)

Lemma: Let $\mathcal{M} = (S, Act, \mathbf{P}, s_0, AP, L)$ be a MDP and let $B \subseteq S$ be a set of absorbing states. Then, for $s \in S$,

- $\Pr^{\max}(s \models \Diamond B) > 0 \quad \text{iff} \quad s \in \exists Pre^*(B)$
- $\Pr^{\max}(s \models \Diamond B) = 0 \quad \text{iff} \quad s \in S \setminus \exists Pre^*(B)$
- $\Pr^{\max}(s \models \Diamond B) < 1 \quad \text{iff} \quad s \in \forall Pre^*(S \setminus \exists Pre^*(B))$
- $\Pr^{\max}(s \models \Diamond B) = 1 \quad \text{iff} \quad s \in S \setminus \forall Pre^*(S \setminus \exists Pre^*(B))$

$\mathcal{O}(size(\mathcal{M}))$

$\mathcal{O}(size(\mathcal{M})^2)$

where

$$\exists Pre(C) \triangleq \{s \in S \mid \exists \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\} \qquad \exists Pre^*(C) \triangleq \bigcup_{n \geq 0} \exists Pre^n(C)$$

$$\forall Pre(C) \triangleq \{s \in S \mid \forall \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\} \qquad \forall Pre^*(C) \triangleq \bigcup_{n \geq 0} \forall Pre^n(C)$$

Qualitative reachability (max

For the general case,
first make states in *B* absorbing
then apply the corresponding
algorithm

Lemma: Let $\mathcal{M} = (S, Act, \mathbf{P}, s_0, AP, L)$ be a MDP and let $B \subseteq S$ be a set of absorbing states.

Then, for $s \in S$,

- $\Pr^{\max}(s \models \Diamond B) > 0$ iff $s \in \exists Pre^*(B)$
- $\Pr^{\max}(s \models \Diamond B) = 0$ iff $s \in S \backslash \exists Pre^*(B)$
- $\Pr^{\max}(s \models \Diamond B) < 1$ iff $s \in \forall Pre^*(S \backslash \exists Pre^*(B))$
- $\Pr^{\max}(s \models \Diamond B) = 1$ iff $s \in S \backslash \forall Pre^*(S \backslash \exists Pre^*(B))$

$\mathcal{O}(size(\mathcal{M}))$

Actually
achieved with a
different algorithm*

$\mathcal{O}(size(\mathcal{M})^2)$

where

$$\exists Pre(C) \triangleq \{s \in S \mid \exists \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\} \qquad \exists Pre^*(C) \triangleq \bigcup_{n \geq 0} \exists Pre^n(C)$$

$$\forall Pre(C) \triangleq \{s \in S \mid \forall \alpha \in Act(s) : \mathbf{P}(s, \alpha, C) > 0\} \qquad \forall Pre^*(C) \triangleq \bigcup_{n \geq 0} \forall Pre^n(C)$$

* See Algorithm 45 in [Baier & Katoen]

Quantitative reachability (max)

Theorem:

The family of values $\{\mathbf{x}_s\}_{s\in S}$ with $\mathbf{x}_s = \Pr^{\max}(s \models \Diamond B)$ is the unique solution to the following equation system:

$$
\begin{array}{ll}
x_s = 1 & \text{if } s \in B \\
x_s = 0 & \text{if } \Pr^{\max}(s \models \Diamond B) = 0 \\
x_s = \max\left\{\sum_{t\in S} \mathbf{P}(s,\alpha,t)\cdot x_t \mid \alpha \in \mathit{Act}(s)\right\} & \text{if } \Pr^{\max}(s \models \Diamond B) > 0 \text{ and } s \notin B
\end{array}
$$

Quantitative reachability (max)

Theorem:

The family of values $\{\mathbf{x}_s\}_{s\in S}$ with $\mathbf{x}_s = \Pr^{\max}(s \models \Diamond B)$ is the unique solution to the following equation system:

$$
\begin{array}{ll}
x_s = 1 & \text{if } s \in S^{\max}_{=1} \\
x_s = 0 & \text{if } s \in S^{\max}_{=0} \\
x_s = \max\left\{\sum_{t\in S}\mathbf{P}(s,\alpha,t)\cdot x_t \mid \alpha \in Act(s)\right\} & \text{if } s \in S^{\max}_{>0}\backslash S^{\max}_{=1}
\end{array}
$$

Quantitative reachability (max)

Theorem:

The family of values $\{\mathbf{x}_s\}_{s\in S}$ with $\mathbf{x}_s = \mathrm{Pr}^{\max}(s \models \Diamond B)$ is the unique solution to the following equation system:

$$
\begin{aligned}
x_s &= 1 && \text{if } s \in S^{\max}_{=1} \\
x_s &= 0 && \text{if } s \in S^{\max}_{=0} \\
x_s &= \max\left\{\textstyle\sum_{t\in S} \mathbf{P}(s,\alpha,t)\cdot x_t \mid \alpha \in \mathit{Act}(s)\right\} && \text{if } s \in S^{\max}_{>0} \backslash S^{\max}_{=1}
\end{aligned}
$$

First make states in *B* absorbing

$$
\begin{aligned}
S^{\max}_{=1} &= S\backslash\forall \mathit{Pre}^*(S\backslash\exists \mathit{Pre}^*(B)) \\
S^{\max}_{=0} &= S\backslash\exists \mathit{Pre}^*(B) \\
S^{\max}_{>0} &= \exists \mathit{Pre}^*(B)
\end{aligned}
$$

Quantitative reachability (max)

Value iteration algorithm

```
for all $s \in S^{\max}_{=1}$,  $x^{(0)}_s = 1$
for all $s \notin S^{\max}_{=1}$,  $x^{(0)}_s = 0$
$i = 0$
repeat
    $i = i + 1$
    for all $s \in S^{\max}_{=1}$,  $x^{(i)}_s = 1$
    for all $s \in S^{\max}_{=0}$,  $x^{(i)}_s = 0$
    for all $s \in S^{\max}_{>0} \backslash S^{\max}_{=1}$,
        $x^{(i)}_s = \max \left\{ \sum_{t \in S} \mathbf{P}(s, \alpha, t) \cdot x^{(i-1)}_t \mid \alpha \in Act(s) \right\}$
until $\left( \max_{s \in S} |x^{(i)}_s - x^{(i-1)}_s| < \varepsilon \right)$
```

a consequece of $x_s = \lim_{i \to \infty} x^{(i)}_s$

Normally very small, e.g. 10^{-6}

Quantitative reachability (max)

Value iteration algorithm

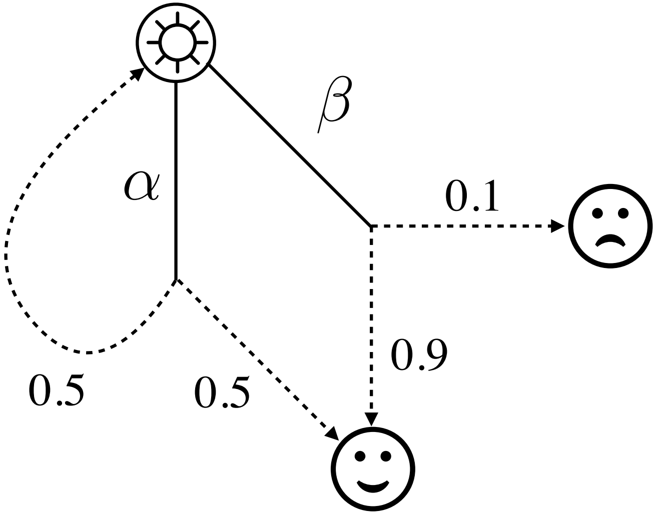
```
for all $s \in S^{\max}_{=1}$,  $x_s^{(0)} = 1$
for all $s \notin S^{\max}_{=1}$,  $x_s^{(0)} = 0$
$i = 0$
repeat
    $i = i + 1$
    for all $s \in S^{\max}_{=1}$,  $x_s^{(i)} = 1$
    for all $s \in S^{\max}_{=0}$,  $x_s^{(i)} = 0$
    for all $s \in S^{\max}_{>0} \setminus S^{\max}_{=1}$,
        $x_s^{(i)} = \max \left\{ \sum_{t \in S} \mathbf{P}(s, \alpha, t) \cdot x_t^{(i-1)} \mid \alpha \in Act(s) \right\}$
until $\left( \max_{s \in S} |x_s^{(i)} - x_s^{(i-1)}| < \varepsilon \right)$
```

a consequece of $x_s = \lim_{i \to \infty} x_s^{(i)}$

What about $\Pr^{\max}(\Diamond^{=n} B)$ and $\Pr^{\max}(\Diamond^{\leq n} B)$?

Normally very small, e.g. 10^{-6}

Quantitative bounded reachability

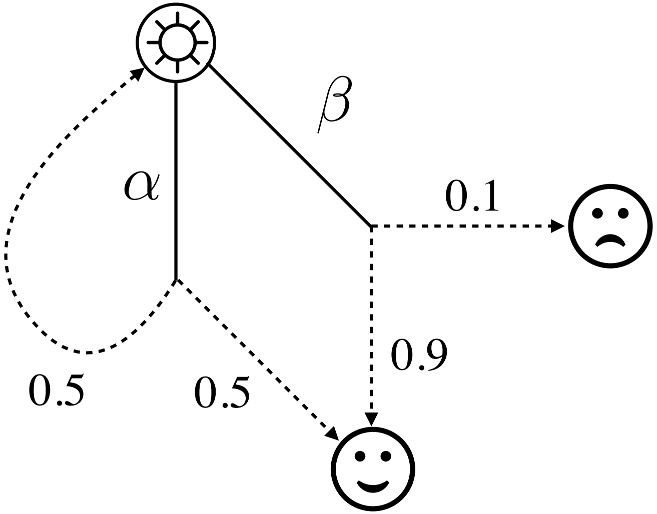


- Only two memoryless deterministic schedulers:

$$\mathfrak{S}_1(\text{☼}) = \alpha \qquad \mathfrak{S}_2(\text{☼}) = \beta$$

$$\Pr^{\mathfrak{S}_1}(\Diamond^{\leq 2}\text{☺}) = 0.875 \qquad \Pr^{\mathfrak{S}_2}(\Diamond^{\leq 2}\text{☺}) = 0.9$$

Quantitative bounded reachability



- Only two memoryless deterministic schedulers:

$$\mathfrak{S}_1(\text{☼}) = \alpha \qquad \mathfrak{S}_2(\text{☼}) = \beta$$

$$\Pr^{\mathfrak{S}_1}(\Diamond^{\leq 2}\text{☺}) = 0.875 \qquad \Pr^{\mathfrak{S}_2}(\Diamond^{\leq 2}\text{☺}) = 0.9$$

- However $\Pr^{\max}(\Diamond^{\leq 2}\text{☺}) = 0.975$ with

$$\mathfrak{S}(\text{☼}) = \alpha \quad \mathfrak{S}(\text{☼☼}) = \alpha \quad \mathfrak{S}(\text{☼☼☼}) = \beta$$

Memoryless deterministic schedulers are not sufficient

Quantitative bounded reachability (max)

```
for all $s \in S^{\max}_{=1}$,  $x_s^{(0)} = 1$
for all $s \notin S^{\max}_{=1}$,  $x_s^{(0)} = 0$
$i = 0$
repeat
    $i = i + 1$
    for all $s \in S^{\max}_{=1}$,  $x_s^{(i)} = 1$
    for all $s \in S^{\max}_{=0}$,  $x_s^{(i)} = 0$
    for all $s \in S^{\max}_{>0} \backslash S^{\max}_{=1}$,
        $x_s^{(i)} = \max \left\{ \sum_{t \in S} \mathbf{P}(s, \alpha, t) \cdot x_t^{(i-1)} \mid \alpha \in Act(s) \right\}$
until $\left( \max_{s \in S} |x_s^{(i)} - x_s^{(i-1)}| < \varepsilon \right)$
```

Algorithm for quantitative reachability

CONICET

UNC

Quantitative bounded reachability (max)

```
for all $s \in B$,      $x_s^{(0)} = 1$
for all $s \notin B$,      $x_s^{(0)} = 0$
$i = 0$
repeat
    $i = i + 1$
    for all $s \in B$,      $x_s^{(i)} = 1$
    for all $s \in S^{\max}_{=0}$,   $x_s^{(i)} = 0$
    for all $s \in S^{\max}_{>0} \backslash B$,
        $x_s^{(i)} = \max \left\{ \sum_{t \in S} \mathbf{P}(s, \alpha, t) \cdot x_t^{(i-1)} \mid \alpha \in Act(s) \right\}$
until $(i = n)$
```

Computes

$\mathrm{Pr}^{\max}(\Diamond^{=n} B)$

To compute $\mathrm{Pr}^{\max}(\Diamond^{\leq n} B)$

first make states in B absorbing

then apply this algorithm

Exactly n times

Qualitative reachability (min)

Lemma: Let $B \subseteq S$ be a set of absorbing states. Then, for $s \in S$,

- $\Pr^{\min}(s \models \Diamond B) > 0 \quad \text{iff} \quad s \in \forall Pre^*(B)$
- $\Pr^{\min}(s \models \Diamond B) = 0 \quad \text{iff} \quad s \in S \backslash \forall Pre^*(B)$
- $\Pr^{\min}(s \models \Diamond B) < 1 \quad \text{iff} \quad s \in \exists Pre^*(S \backslash \forall Pre^*(B))$
- $\Pr^{\min}(s \models \Diamond B) = 1 \quad \text{iff} \quad s \in S \backslash \exists Pre^*(S \backslash \forall Pre^*(B))$

Note the inversion of $\forall$ and $\exists$ respect to max qualitative reachability

Qualitative reachability (min)

Lemma: Let $B \subseteq S$ be a set of absorbing states. Then, for $s \in S$,

$$\left.\begin{array}{l}\Pr^{\min}(s \models \Diamond B) > 0 \quad \text{iff} \quad s \in \forall Pre^*(B) \\ \Pr^{\min}(s \models \Diamond B) = 0 \quad \text{iff} \quad s \in S \backslash \forall Pre^*(B)\end{array}\right\}$$

$\mathcal{O}(size(\mathcal{M}))$

$$\left.\begin{array}{l}\Pr^{\min}(s \models \Diamond B) < 1 \quad \text{iff} \quad s \in \exists Pre^*(S \backslash \forall Pre^*(B)) \\ \Pr^{\min}(s \models \Diamond B) = 1 \quad \text{iff} \quad s \in S \backslash \exists Pre^*(S \backslash \forall Pre^*(B))\end{array}\right\}$$

$\mathcal{O}(size(\mathcal{M}))$

Note the inversion of $\forall$ and $\exists$ respect to max qualitative reachability

Qualitative reachability (min

For the general case, first make states in B absorbing then apply the corresponding algorithm

Lemma: Let $B \subseteq S$ be a set of absorbing states. Then, for $s \in S$,

- $\Pr^{\min}(s \models \Diamond B) > 0 \quad \text{iff} \quad s \in \forall Pre^*(B)$
- $\Pr^{\min}(s \models \Diamond B) = 0 \quad \text{iff} \quad s \in S \backslash \forall Pre^*(B)$
- $\Pr^{\min}(s \models \Diamond B) < 1 \quad \text{iff} \quad s \in \exists Pre^*(S \backslash \forall Pre^*(B))$
- $\Pr^{\min}(s \models \Diamond B) = 1 \quad \text{iff} \quad s \in S \backslash \exists Pre^*(S \backslash \forall Pre^*(B))$

$\mathcal{O}(size(\mathcal{M}))$

$\mathcal{O}(size(\mathcal{M}))$

Note the inversion of $\forall$ and $\exists$ respect to max qualitative reachability

Actually achieved with a different algorithm*

[*] See Algorithm 46 in [Baier & Katoen]

Quantitative reachability (min)

Theorem:

The family of values $\{\mathbf{x}_s\}_{s\in S}$ with $\mathbf{x}_s = \mathrm{Pr}^{\min}(s \models \Diamond B)$ is the unique solution to the following equation system:

$$
\begin{array}{ll}
x_s = 1 & \text{if } s \in B \\
x_s = 0 & \text{if } \mathrm{Pr}^{\min}(s \models \Diamond B) = 0 \\
x_s = \min\left\{\sum_{t\in S} \mathbf{P}(s,\alpha,t)\cdot x_t \mid \alpha \in Act(s)\right\} & \text{if } \mathrm{Pr}^{\min}(s \models \Diamond B) > 0 \text{ and } s \notin B
\end{array}
$$

Quantitative reachability (min)

Theorem:

The family of values $\{\mathbf{x}_s\}_{s\in S}$ with $\mathbf{x}_s = \mathrm{Pr}^{\min}(s \models \Diamond B)$ is the unique solution to the following equation system:

$$
\begin{array}{ll}
x_s = 1 & \text{if } s \in S^{\min}_{=1} \\
x_s = 0 & \text{if } s \in S^{\min}_{=0} \\
x_s = \min\left\{\sum_{t\in S} \mathbf{P}(s,\alpha,t)\cdot x_t \mid \alpha \in Act(s)\right\} & \text{if } s \in S^{\min}_{>0} \setminus S^{\min}_{=1}
\end{array}
$$

UNC

Quantitative reachability (min)

Value iteration algorithm

Algorithm for quantitative reachability

```
for all $s \in S^{\min}_{=1}$,  $x^{(0)}_s = 1$
for all $s \notin S^{\min}_{=1}$,  $x^{(0)}_s = 0$
$i = 0$
repeat
    $i = i + 1$
    for all $s \in S^{\min}_{=1}$,  $x^{(i)}_s = 1$
    for all $s \in S^{\min}_{=0}$,  $x^{(i)}_s = 0$
    for all $s \in S^{\min}_{>0} \backslash S^{\max}_{=1}$,
        $x^{(i)}_s = \min \left\{ \sum_{t \in S} \mathbf{P}(s, \alpha, t) \cdot x^{(i-1)}_t \mid \alpha \in Act(s) \right\}$
until $\left( \max_{s \in S} |x^{(i)}_s - x^{(i-1)}_s| < \varepsilon \right)$
```

CONICET

UNC

Quantitative bounded reachability (min)

```
for all $s \in B,\ x_s^{(0)} = 1$
for all $s \notin B,\ x_s^{(0)} = 0$
$i = 0$
repeat
    $i = i + 1$
    for all $s \in B,\ x_s^{(i)} = 1$
    for all $s \in S^{\min}_{=0},\ x_s^{(i)} = 0$
    for all $s \in S^{\min}_{>0} \backslash B,$
        $x_s^{(i)} = \min \left\{ \sum_{t \in S} \mathbf{P}(s, \alpha, t) \cdot x_t^{(i-1)} \mid \alpha \in Act(s) \right\}$
until $(i = n)$
```

Computes $\Pr^{\min}(\Diamond^{=n} B)$

To compute $\Pr^{\min}(\Diamond^{\leq n} B)$ first make states in B absorbing then apply this algorithm

Exactly n times

CONICET

UNC

Quantitative reachability

- We gave approximating algorithms (value iteration) to calculate quantitative reachability (max or min)

- However, the exact values can be computed by solving a linear programming problem

- Therefore, quantitative reachability (max or min) can be computed in polynomial time

Constrained reachability

To compute

$$\begin{array}{lll} \Pr^{\max}(s \models C \,\mathtt{U}\, B) & \Pr^{\max}(s \models C \,\mathtt{U}^{\leq n}\, B) & \Pr^{\max}(s \models C \,\mathtt{U}\, B) = 1 \\ \Pr^{\min}(s \models C \,\mathtt{U}\, B) & \Pr^{\min}(s \models C \,\mathtt{U}^{\leq n}\, B) & \Pr^{\min}(s \models C \,\mathtt{U}\, B) = 1 \end{array} \qquad \text{etc.}$$

in a MDP $\mathcal{M}$ do:

1. Obtain $\mathcal{M}_{\mathtt{U}}$ from $\mathcal{M}$ by making states in $S\backslash(C \cup B)$ absorbing.
2. Apply the algorithm in $\mathcal{M}_{\mathtt{U}}$ to verify the reachability property $s \models \Diamond B$.

PCTL in MDP

A PCTL formula Φ holds in state $s \in S$ of a MDP $\mathcal{M}$, denoted by $s \models \Phi$, whenever:

state formulas

	$s \models p$	iff	$p \in L(s)$
	$s \models \neg\Phi$	iff	$s \not\models \Phi$
	$s \models \Phi_1 \wedge \Phi_2$	iff	$s \models \Phi_1$ and $s \models \Phi_2$
	$s \models \mathtt{P}_{\bowtie a}(\phi)$	iff	❓

path formulas

	$\rho \models \bigcirc\Phi$	iff	$\rho(1) \models \Phi$
	$\rho \models \Phi \,\mathtt{U}\, \Psi$	iff	exists $j \geq 0$ s.t. $\rho(j) \models \Psi$ and for all $0 \leq k < j, \rho(k) \models \Phi$
	$\rho \models \Phi \,\mathtt{U}^{\leq n}\, \Psi$	iff	exists $0 \leq j \leq n$ s.t. $\rho(j) \models \Psi$ and for all $0 \leq k < j, \rho(k) \models \Phi$

PCTL in MDP

A PCTL formula Φ holds in state $s \in S$ of a MDP $\mathcal{M}$, denoted by $s \models \Phi$, whenever:

state formulas

$s \models p$ iff $p \in L(s)$

$s \models \neg\Phi$ iff $s \not\models \Phi$

$s \models \Phi_1 \wedge \Phi_2$ iff $s \models \Phi_1$ and $s \models \Phi_2$

$s \models \mathsf{P}_{\bowtie a}(\phi)$ iff for every scheduler $\mathfrak{S}$, $\Pr^{\mathfrak{S}}(s \models \phi) \bowtie a$

where $\Pr^{\mathfrak{S}}(s \models \phi) = \Pr^{\mathfrak{S}}_{s}(\{\rho \in \mathit{Path}(s) \mid \rho \models \phi\})$ and

path formulas

$\rho \models \bigcirc\Phi$ iff $\rho(1) \models \Phi$

$\rho \models \Phi \,\mathsf{U}\, \Psi$ iff exists $j \geq 0$ s.t. $\rho(j) \models \Psi$ and for all $0 \leq k < j, \rho(k) \models \Phi$

$\rho \models \Phi \,\mathsf{U}^{\leq n}\, \Psi$ iff exists $0 \leq j \leq n$ s.t. $\rho(j) \models \Psi$ and for all $0 \leq k < j, \rho(k) \models \Phi$

PCTL in MDP

A PCTL formula Φ holds in state $s \in S$ of a MDP $\mathcal{M}$, denoted by $s \models \Phi$, whenever:

state formulas

$s \models p$ iff $p \in L(s)$

$s \models \neg\Phi$ iff $s \not\models \Phi$

$s \models \Phi_1 \wedge \Phi_2$ iff $s \models \Phi_1$ and $s \models \Phi_2$

$s \models \mathsf{P}_{\bowtie a}(\phi)$ iff for every scheduler $\mathfrak{S}$, $\Pr^{\mathfrak{S}}(s \models \phi) \bowtie a$

How is this computed?

where $\Pr^{\mathfrak{S}}(s \models \phi) = \Pr^{\mathfrak{S}}_s(\{\rho \in \mathit{Path}(s) \mid \rho \models \phi\})$ and

path formulas

$\rho \models \bigcirc\Phi$ iff $\rho(1) \models \Phi$

$\rho \models \Phi \,\mathsf{U}\, \Psi$ iff exists $j \geq 0$ s.t. $\rho(j) \models \Psi$ and for all $0 \leq k < j, \rho(k) \models \Phi$

$\rho \models \Phi \,\mathsf{U}^{\leq n}\, \Psi$ iff exists $0 \leq j \leq n$ s.t. $\rho(j) \models \Psi$ and for all $0 \leq k < j, \rho(k) \models \Phi$

Algorithm for PCTL model checking

```
fun Sat($\Phi$) {
    // input: a PCTL formula $\Phi$
    // output: $\{s \in S \mid s \models \Phi\}$
    case {  $\Phi \in AP$                return $\{s \in S \mid \Phi \in L(s)\}$
            $\Phi \equiv \neg\Psi$               return $S \setminus \mathit{Sat}(\Psi)$
            $\Phi \equiv \Psi_1 \wedge \Psi_2$           return $\mathit{Sat}(\Psi_1) \cap \mathit{Sat}(\Psi_2)$
            $\Phi \equiv \mathtt{P}_{\lhd a}(\phi)$          return $\{s \in S \mid \mathit{maxProb}(s, \phi) \lhd a\}$
            $\Phi \equiv \mathtt{P}_{\rhd a}(\phi)$          return $\{s \in S \mid \mathit{minProb}(s, \phi) \rhd a\}$
    }
}

fun maxProb($s, \phi$) {
    // input: a state $s$ and a path formula $\phi$
    // output: $\Pr_s^{\max}(s \models \phi)$
    case {  $\phi \equiv \bigcirc\Phi$               return $\max\left\{\sum_{t \in S} \mathbf{P}(s, \alpha, t) \cdot \mathbf{1}_{\mathit{Sat}(\Phi)}(t) \mid \alpha \in \mathit{Act}(s)\right\}$
            $\phi \equiv \Phi \, \mathtt{U} \, \Psi$            let $B = \mathit{Sat}(\Psi)$;  let $C = \mathit{Sat}(\Phi)$
                                    return $\Pr_s^{\max}(C \, \mathtt{U} \, B)$        // constrained reachability
            $\phi \equiv \Phi \, \mathtt{U}^{\leq n} \, \Psi$         let $B = \mathit{Sat}(\Psi)$;  let $C = \mathit{Sat}(\Phi)$
                                    return $\Pr_s^{\max}(C \, \mathtt{U}^{\leq n} \, B)$     // bounded constrained reachability
    }
}
```

$\lhd \in \{<, \leq\}$

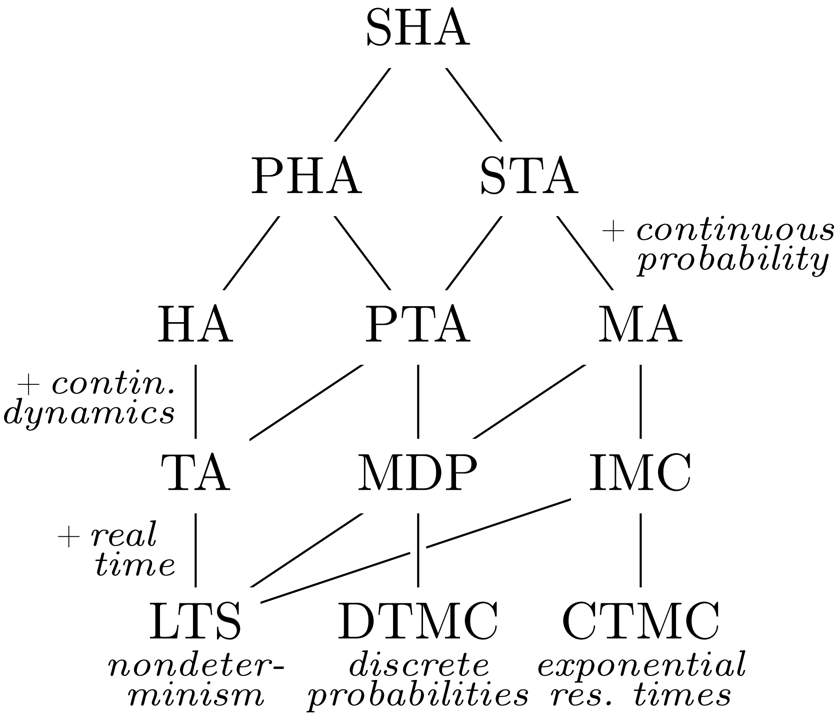
$\rhd \in \{\geq, >\}$

minProb is the same but changing max for min

Polynomial on the size of M
Linear on the size of Φ
Linear on the largest n

Probabilistic model checkers

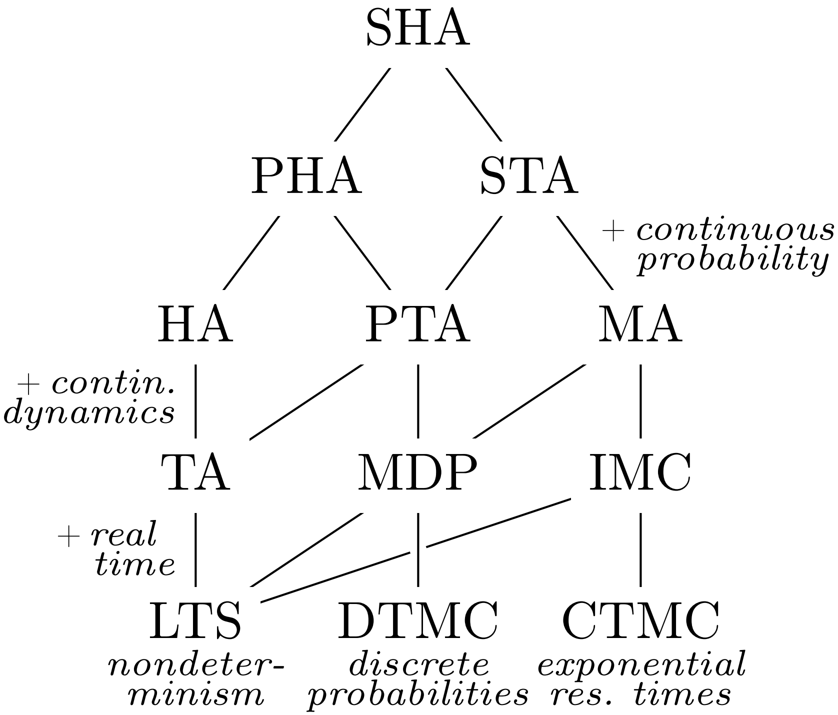
The quantitative automata zoo

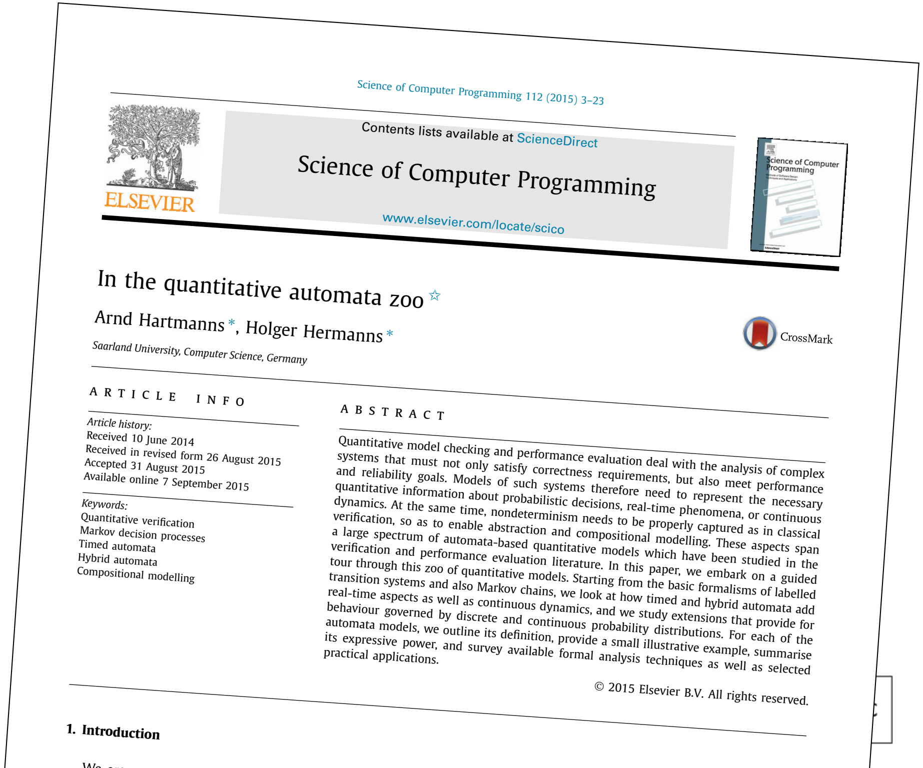


CONICET

UNC

The quantitative automata zoo





Science of Computer Programming 112 (2015) 3–23

Contents lists available at ScienceDirect

Science of Computer Programming

www.elsevier.com/locate/scico

In the quantitative automata zoo ☆

Arnd Hartmanns *, Holger Hermanns *

Saarland University, Computer Science, Germany

ARTICLE INFO

Article history:
Received 10 June 2014
Received in revised form 26 August 2015
Accepted 31 August 2015
Available online 7 September 2015

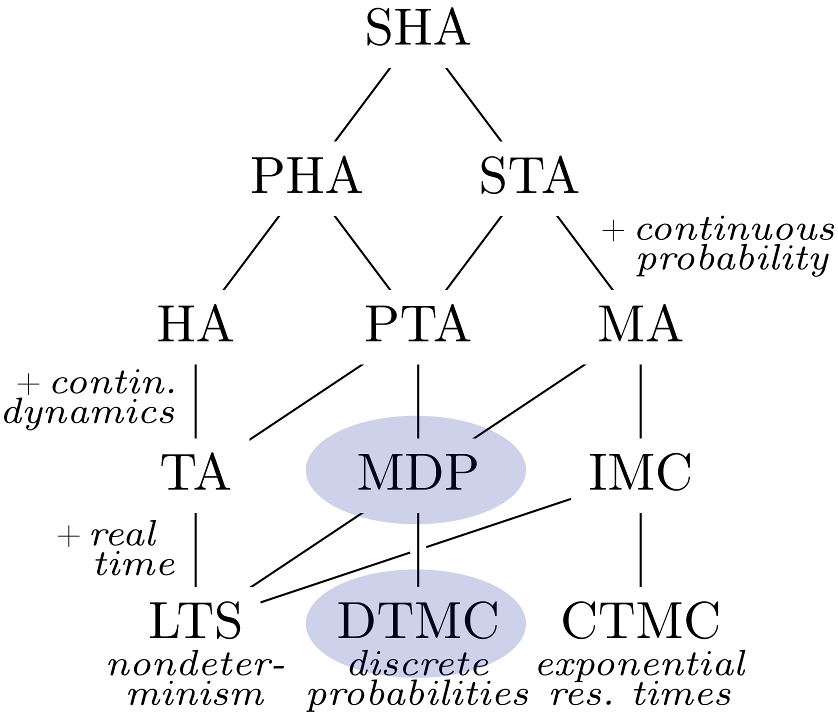
Keywords:
Quantitative verification
Markov decision processes
Timed automata
Hybrid automata
Compositional modelling

ABSTRACT

Quantitative model checking and performance evaluation deal with the analysis of complex systems that must not only satisfy correctness requirements, but also meet performance and reliability goals. Models of such systems therefore need to represent the necessary quantitative information about probabilistic decisions, real-time phenomena, or continuous dynamics. At the same time, nondeterminism needs to be properly captured as in classical verification, so as to enable abstraction and compositional modelling. These aspects span a large spectrum of automata-based quantitative models which have been studied in the verification and performance evaluation literature. In this paper, we embark on a guided tour through this zoo of quantitative models. Starting from the basic formalisms of labelled transition systems and also Markov chains, we look at how timed and hybrid automata add real-time aspects as well as continuous dynamics, and we study extensions that provide for behaviour governed by discrete and continuous probability distributions. For each of the automata models, we outline its definition, provide a small illustrative example, summarise its expressive power, and survey available formal analysis techniques as well as selected practical applications.

1. Introduction

The quantitative automata zoo



SHA

PHA

STA

+ *continuous probability*

HA

PTA

MA

+ *contin. dynamics*

TA

MDP

IMC

+ *real time*

LTS

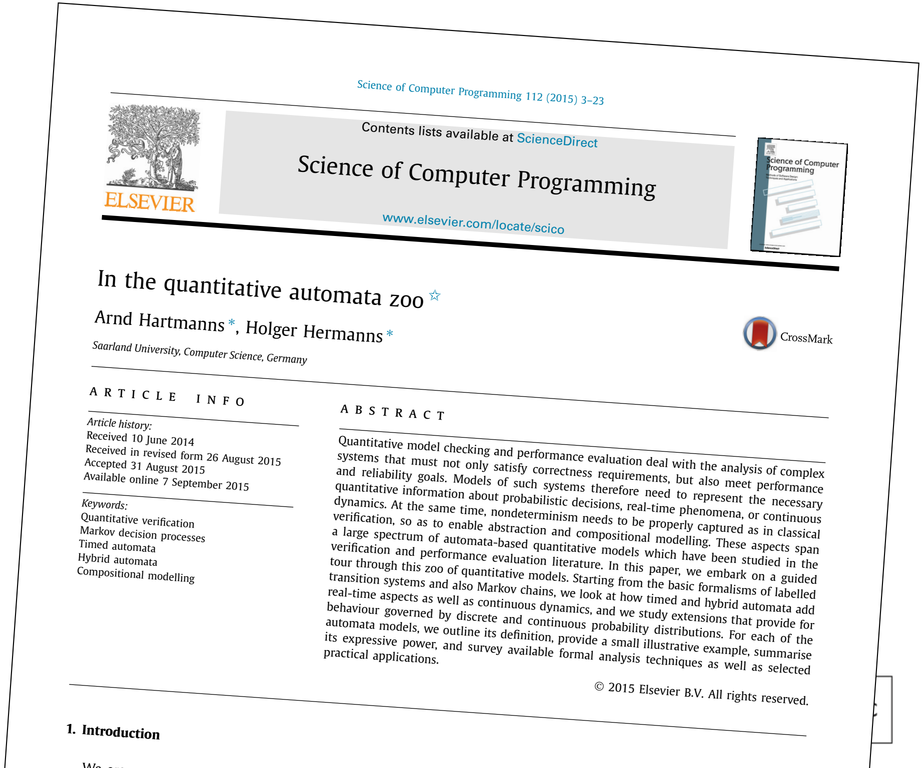
DTMC

CTMC

nondeterminism

discrete probabilities

exponential res. times



Science of Computer Programming 112 (2015) 3–23

Contents lists available at ScienceDirect

Science of Computer Programming

www.elsevier.com/locate/scico

In the quantitative automata zoo ☆

Arnd Hartmanns *, Holger Hermanns *

Saarland University, Computer Science, Germany

ARTICLE INFO

Article history:
Received 10 June 2014
Received in revised form 26 August 2015
Accepted 31 August 2015
Available online 7 September 2015

Keywords:
Quantitative verification
Markov decision processes
Timed automata
Hybrid automata
Compositional modelling

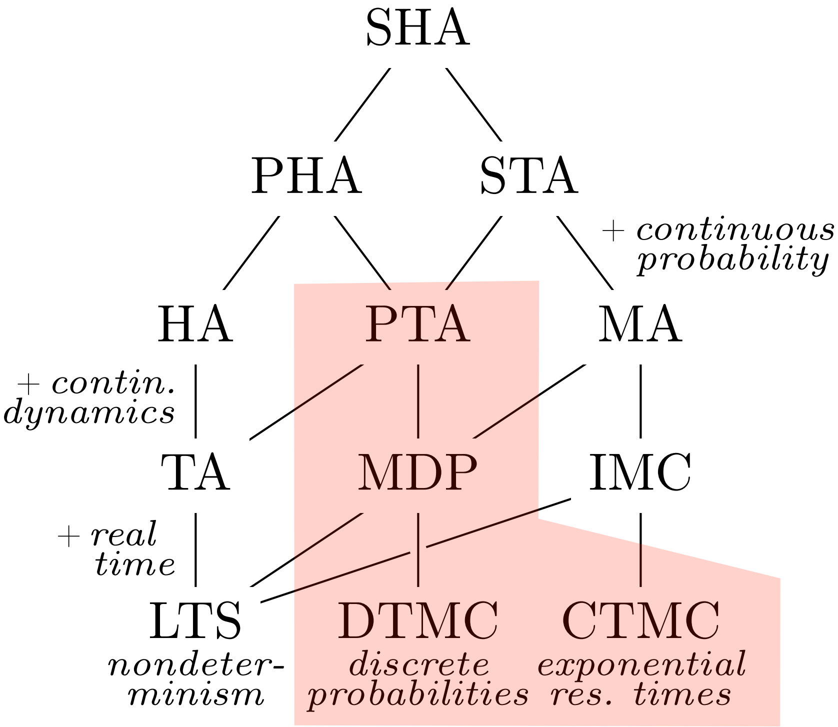
ABSTRACT

Quantitative model checking and performance evaluation deal with the analysis of complex systems that must not only satisfy correctness requirements, but also meet performance and reliability goals. Models of such systems therefore need to represent the necessary quantitative information about probabilistic decisions, real-time phenomena, or continuous dynamics. At the same time, nondeterminism needs to be properly captured as in classical verification, so as to enable abstraction and compositional modelling. These aspects span a large spectrum of automata-based quantitative models which have been studied in the verification and performance evaluation literature. In this paper, we embark on a guided tour through this zoo of quantitative models. Starting from the basic formalisms of labelled transition systems and also Markov chains, we look at how timed and hybrid automata add real-time aspects as well as continuous dynamics, and we study extensions that provide for behaviour governed by discrete and continuous probability distributions. For each of the automata models, we outline its definition, provide a small illustrative example, summarise its expressive power, and survey available formal analysis techniques as well as selected practical applications.

1. Introduction

We ar

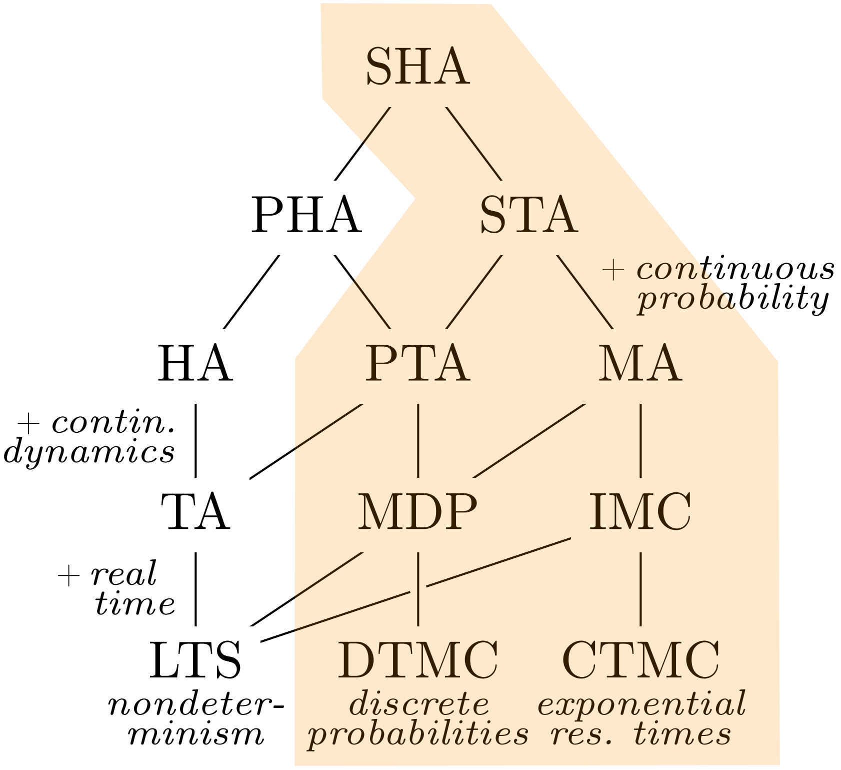
State of the Art PMC



PRISM

- First appeared in 2000 [KNP00, dAKNPS00]
- https://www.prismmodelchecker.org/
- In addition POMDP, POPTA, IMDP
- PRISM language → network of modules
- Properties: PCTL, CSL, LTL, PCTL*, steady state, rewards and costs, multi-objective
- Symbolic, hybrid, and explicit engines
- Also SMC on deterministic models
- Alternate version for stochastic games

State of the Art PMC



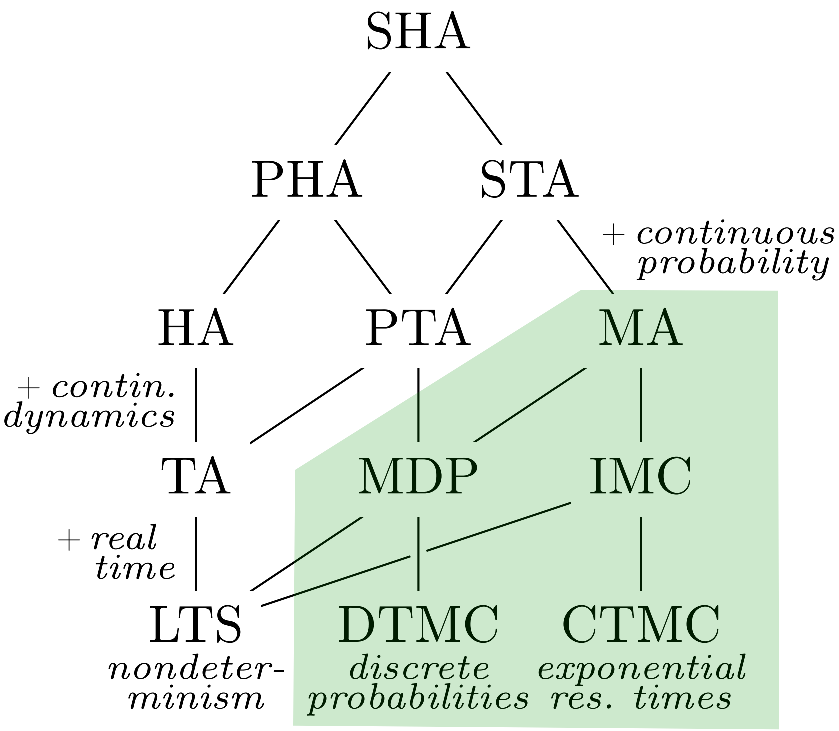
The Modest toolset

- First appeared in 2009 [Hartmanns09]
- https://www.modestchecker.net/
- Modest language includes conventional programming constructs with ideas from process algebra [DHKK01]
- Properties: reachability, bounded reachability, steady state, expected rewards
- **mcsta**: disk-based explicit engine
- **modes**: SMC for non-det. models and RES
- More tools: **prohver**, **modysh**, **mosta**, **moconv**

CONICET

UNC

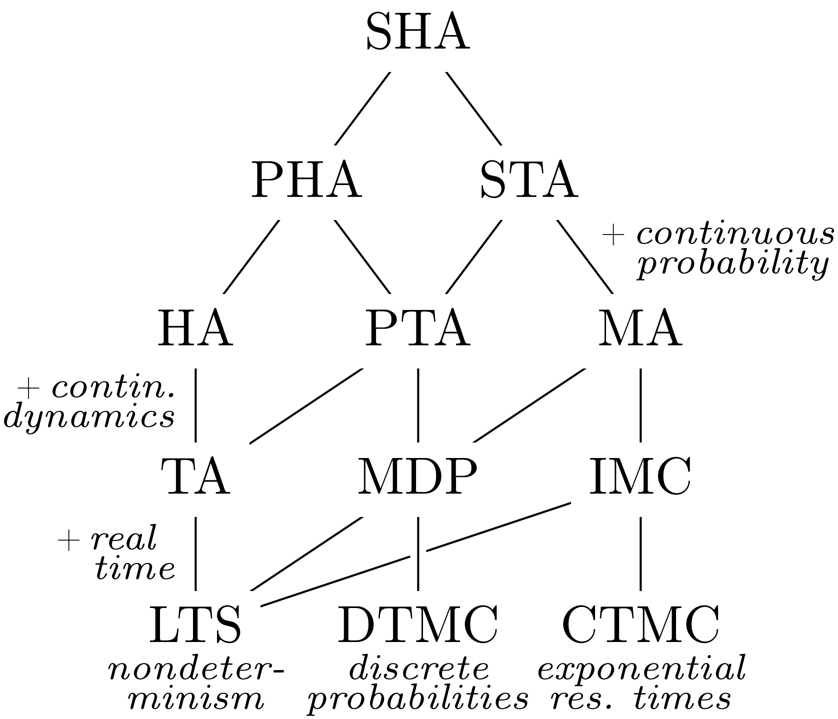
State of the Art PMC

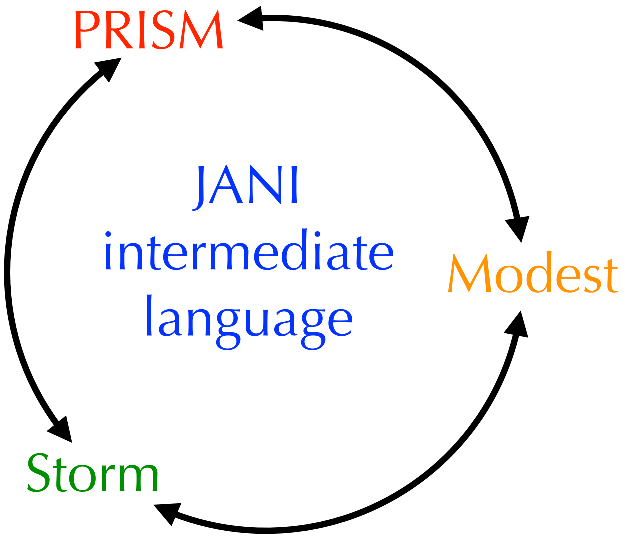


Storm

- First appeared in 2017 [DJKV17]
- https://www.stormchecker.org/
- In addition POMDP, Parametric models
- Languages: PRISM, cpGCL, GSPN, DFT
- Properties: PCTL, CSL, LTL, steady state, expected rewards, multi-objective, conditional probabilies
- Counterexample generation
- Explicit and symbolic engine

State of the Art PMC





Probabilistic Model Checking

Pedro R. D'Argenio

Universidad Nacional de Córdoba – CONICET
https://cs.famaf.unc.edu.ar/~dargenio/

ICTAC 2023 Training School on Applied Formal Methods