Qualitative Properties in Markov Chains

Lecture #20 of Advanced Model Checking

Joost-Pieter Katoen

Lehrstuhl 2: Software Modeling & Verification

E-mail: `katoen@cs.rwth-aachen.de`

July 15, 2009

Discrete-time Markov chains

A DTMC $\mathcal{M}$ is a tuple $(S, \mathbf{P}, \iota_{\text{init}}, AP, L)$ with:

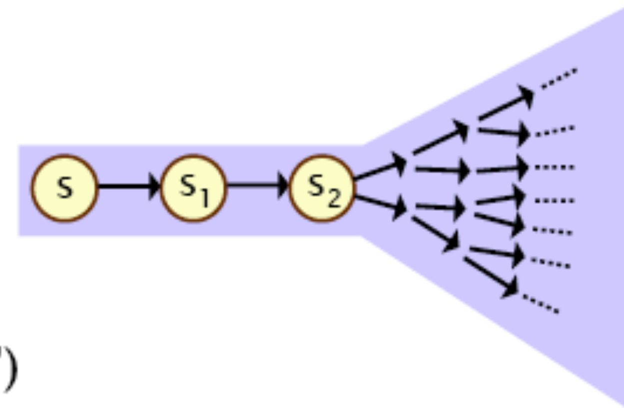
- S is a countable nonempty set of states
- $\mathbf{P} : S \times S \rightarrow [0, 1]$, transition probability function s.t. $\sum_{s'} \mathbf{P}(s, s') = 1$
  - $\mathbf{P}(s, s')$ is the probability to jump from s to s' in one step
- $\iota_{\text{init}} : S \rightarrow [0, 1]$, the initial distribution with $\sum\limits_{s \in S} \iota_{\text{init}}(s) = 1$
  - $\iota_{\text{init}}(s)$ is the probability that system starts in state s
  - state s for which $\iota_{\text{init}}(s) > 0$ is an initial state
- $L : S \rightarrow 2^{AP}$, the labelling function

Paths in a DTMC

- State graph of DTMC $\mathcal{M}$ is a digraph $G = (V, E)$ with
  - vertices in V are states of $\mathcal{M}$, and $(s, s') \in E$ if and only if $\mathbf{P}(s, s') > 0$
- Paths in $\mathcal{M}$ are maximal (i.e., infinite) paths in its state graph
  - infinite sequence of states $s_0 s_1 s_2 \ldots\ldots$
  - *Paths*$(\mathcal{M})$ and *Paths*$_{fin}(\mathcal{M})$ denote the set of (finite) paths in $\mathcal{M}$
- Direct successors and predecessors
  - *Post*$(s) = \{ s' \in S \mid \mathbf{P}(s, s') > 0 \}$ and *Pre*$(s) = \{ s' \in S \mid \mathbf{P}(s', s) > 0 \}$
  - *Post*$^*(s)$ and *Pre*$^*(s)$ are reflexive and transitive closure of *Post* and *Pre*

Paths and probabilities

- To reason (quantitatively) about this system
  - need to define a probability space over paths
- Intuitively:
  - sample space: Path(s) = set of all infinite paths from a state s
  - events: sets of infinite paths from s
  - basic events: cylinder sets (or "cones")
  - cylinder set Cyl(ω), for a finite path ω = set of infinite paths with the common finite prefix ω
  - for example: $Cyl(ss_1s_2)$



Probability space on DTMC paths

- Events are *infinite paths* in the DTMC $\mathcal{M}$, i.e., $\Omega = \mathit{Paths}(\mathcal{M})$
- σ-algebra on $\mathcal{M}$ is generated by *cylinder sets* of finite paths $\hat{\pi}$:

$$\mathit{Cyl}(\hat{\pi}) \; = \; \{ \, \pi \in \mathit{Paths}(\mathcal{M}) \mid \hat{\pi} \text{ is a prefix of } \pi \, \}$$

  - cylinder sets serve as events of the smallest σ-algebra on $\mathit{Paths}(\mathcal{M})$

- *Pr* is the *probability measure* on the σ-algebra on $\mathit{Paths}(\mathcal{M})$:

$$\mathit{Pr}\big(\mathit{Cyl}(s_0 \ldots s_n)\big) \; = \; \iota_{\text{init}}(s_0) \cdot \mathbf{P}(s_0 \ldots s_n)$$

  - where $\mathbf{P}(s_0 \, s_1 \ldots s_n) \; = \prod_{0 \leqslant i < n} \mathbf{P}(s_i, s_{i+1})$ if $n > 0$
  - and $\mathbf{P}(s_0) = 1$ for paths containing a single state

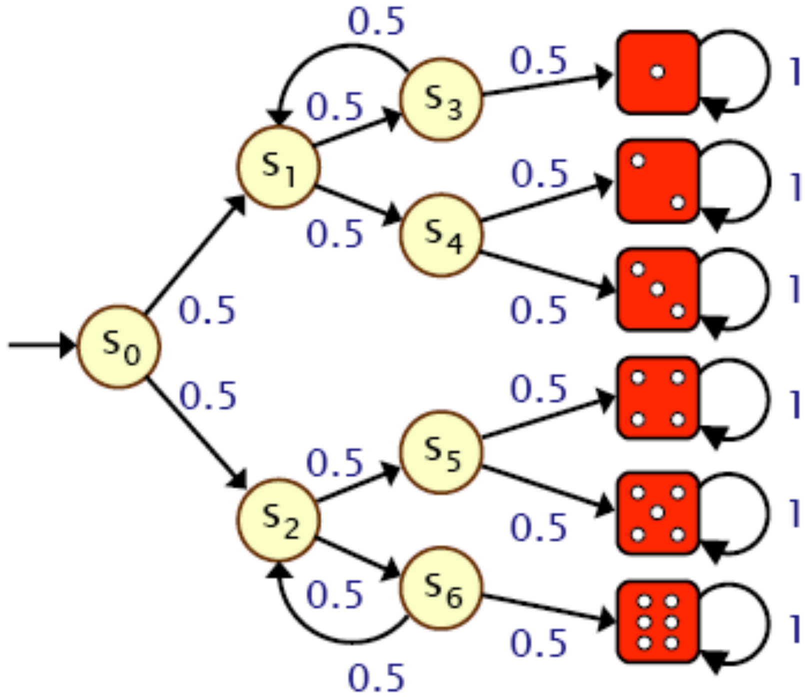
Reachability probabilities in finite DTMCs

- Let $\textit{Pr}(s \models \Diamond B) = \textit{Pr}_s(\Diamond B) = \textit{Pr}_s\{\pi \in \textit{Paths}(s) \mid \pi \models \Diamond B\}$
  - where $\textit{Pr}_s$ is the probability measure in $\mathcal{M}$ with only initial state s
- Let variable $x_s = \textit{Pr}(s \models \Diamond B)$ for any state s
  - if B is not reachable from s then $x_s = 0$
  - if $s \in B$ then $x_s = 1$
- For any state $s \in \textit{Pre}^*(B) \setminus B$:

$$x_s = \underbrace{\sum_{t \in S \setminus B} \mathbf{P}(s,t) \cdot x_t}_{\text{reach } B \text{ via } t} + \underbrace{\sum_{u \in B} \mathbf{P}(s,u)}_{\text{reach } B \text{ in one step}}$$

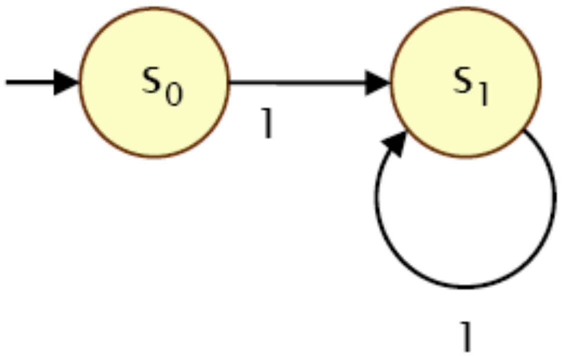
Example

- Compute ProbReach(s_0, {4})



Unique solution

- Why the need to identify states that can reach T?
- Consider this simple DTMC:
  - compute probability of reaching $\{s_0\}$ from s_1



  - linear equation system: $x_{s0} = 1$, $x_{s1} = x_{s1}$
  - multiple solutions: $(x_{s0}, x_{s1}) = (1,p)$ for any p

Linear equation system

- These equations can be rewritten into the following form:

$$\mathbf{x} = \mathbf{A}\mathbf{x} + \mathbf{b}$$

  - where vector $\mathbf{x} = (x_s)_{s \in \tilde{S}}$ with $\tilde{S} = Pre^*(B) \setminus B$
  - $\mathbf{A} = \left(\mathbf{P}(s,t)\right)_{s,t \in \tilde{S}}$, the transition probabilities in $\tilde{S}$
  - $\mathbf{b} = \left(b_s\right)_{s \in \tilde{S}}$ contains the probabilities to reach B within one step

- *Linear equation system*: $(\mathbf{I} - \mathbf{A})\mathbf{x} = \mathbf{b}$

  - note: more than one solution may exist if $\mathbf{I} - \mathbf{A}$ has no inverse (i.e., is singular)

$\Rightarrow$ characterize the desired probability as least fixed point

Example

Let $B = \{ \textit{delivered} \}$

$\tilde{S} = \{\textit{init}, \textit{try}, \textit{lost}\}$ and the equations:

$$\begin{aligned} x_{\textit{init}} &= x_{\textit{try}} \\ x_{\textit{try}} &= \frac{1}{10} \cdot x_{\textit{lost}} + \frac{9}{10} \\ x_{\textit{lost}} &= x_{\textit{try}} \end{aligned}$$

which can be rewritten as:

$$\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -\frac{1}{10} \\ 0 & -1 & 1 \end{pmatrix} \cdot \mathbf{x} = \begin{pmatrix} 0 \\ \frac{9}{10} \\ 0 \end{pmatrix}$$

and yields the (unique) solution: $x_{\textit{try}} = x_{\textit{init}} = x_{\textit{lost}} = 1$.

Constrained reachability

- Let $\mathcal{M} = (S, \mathbf{P}, \iota_{\text{init}}, AP, L)$ be a (possibly infinite) DTMC and $B, C \subseteq S$

- $C \,\mathsf{U}^{\leqslant n} B$ is the union of the basic cylinders of path fragments:
  - $s_0\, s_1 \ldots s_k$ with $k \leqslant n$ and $s_i \in C$ for all $0 \leqslant i < k$ and $s_k \in B$

- Let $S_{=0}$, $S_{=1}$, $S_?$ be a partition of S such that:
  - $B \subseteq S_{=1} \subseteq \{ s \in S \mid Pr(s \models C \,\mathsf{U}\, B) = 1 \}$
  - $S \setminus (C \cup B) \subseteq S_{=0} \subseteq \{ s \in S \mid Pr(s \models C \,\mathsf{U}\, B) = 0 \}$
  - so: all states in $S_?$ belong to $C \setminus B$

- Let $\mathbf{A} = \big(\mathbf{P}(s,t) \big)_{s,t \in S_?}$ and $\big(b_s \big)_{s \in S_?}$ where $b_s = \mathbf{P}(s, S_{=1})$

Least fixed point characterization

- An alternative: least fixed point characterization
- Consider functions of the form $F : [0,1]^S \rightarrow [0,1]^S$
  - F thus maps vectors of probabilities (of length $|S|$) to such vectors
- Define $\mathbf{y} \leqslant \mathbf{y}'$ if and only if $y_s \leqslant y'_s$ for all $s \in S$
- $\mathbf{y}$ is a fixed point of F if $F(\mathbf{y}) = \mathbf{y}$
- A fixed point $\mathbf{x}$ is the least fixed point of F if
  - $\mathbf{x} \leqslant \mathbf{y}$ for any other fixed point $\mathbf{y}$ of F

Least fixed point characterization

The vector $\mathbf{x} = \big(Pr(s \models C \, \mathsf{U} \, B)\big)_{s \in S_?}$ is the *least fixed point* of:

$$F : [0,1]^{S_?} \to [0,1]^{S_?} \quad \text{given by} \quad F(\mathbf{y}) = \mathbf{A} \cdot \mathbf{y} + \mathbf{b}$$

Furthermore, for $\mathbf{x}^{(0)} = \mathbf{0}$ and $\mathbf{x}^{(n+1)} = F(\mathbf{x}^{(n)})$ for $n \geqslant 0$:

- $\mathbf{x}^{(n)} = (x_s^{(n)})_{s \in S_?}$ where for any s: $x_s^{(n)} = Pr(s \models C \, \mathsf{U}^{\leqslant n} \, S_{=1})$
- $\mathbf{x}^{(0)} \leqslant \mathbf{x}^{(1)} \leqslant \mathbf{x}^{(2)} \leqslant \ldots \leqslant \mathbf{x}$, and
- $\mathbf{x} = \lim_{n \to \infty} \mathbf{x}^{(n)}$

Proof

Constrained reachability probabilities

- So: $\mathbf{x}$ is the *least* solution of $\mathbf{A}\mathbf{x} + \mathbf{b} = \mathbf{x}$ in $[0,1]^{S_?}$
- And: can be approximated by:

$$\mathbf{x}^{(0)} = \mathbf{0} \quad \text{and} \quad \mathbf{x}^{(n+1)} = \mathbf{A}\mathbf{x}^{(n)} + \mathbf{b} \ \text{ for } \ n \geqslant 0$$

- *Power method*: compute vectors $\mathbf{x}^{(0)}, \mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots$ and abort if:

$$\max_{s \in S_?} \left| x_s^{(n+1)} - x_s^{(n)} \right| < \varepsilon \qquad \text{for some small tolerance } \varepsilon$$

  - convergence guaranteed
  - alternative techniques: e.g., Jacobi or Gauss-Seidel, successive overrelaxation

Unique solution

Let $\mathcal{M}$ be a finite DTMC with state space S partitioned into:

- $S_{=0} = \mathit{Sat}(\neg\exists(C \cup B))$
- $S_{=1}$ a subset of $\{s \in S \mid \mathit{Pr}(s \models C \cup B) = 1\}$ that contains B
- $S_{?} = S \setminus (S_{=0} \cup S_{=1})$

For B, $C \subseteq S$, the vector

$$\big(\mathit{Pr}(s \models C \cup B)\big)_{s \in S_?}$$

is the *unique* solution of the linear equation system:

$$\mathbf{x} = \mathbf{A}\mathbf{x} + \mathbf{b} \quad \text{where} \quad \mathbf{A} = \big(\mathbf{P}(s,t)\big)_{s,t \in S_?} \text{ and } \mathbf{b} = \big(\mathbf{P}(s, S_{=1})\big)_{s \in S_?}$$

Computing constrained reachability probabilities

- The probabilities of the events $C \,\mathsf{U}^{\leqslant n} B$ can be obtained iteratively:

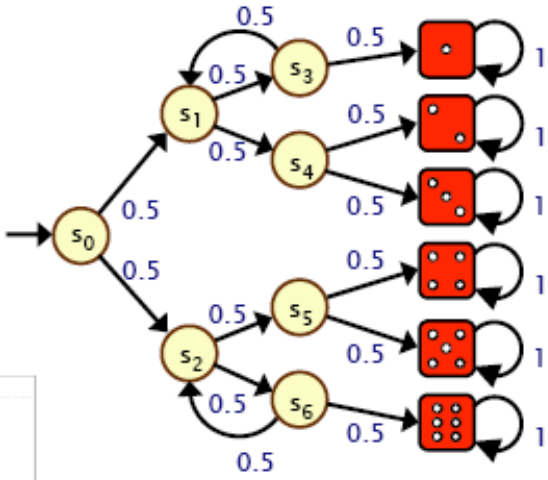
$$\mathbf{x}^{(0)} = \mathbf{0} \quad \text{and} \quad \mathbf{x}^{(i+1)} = \mathbf{A}\mathbf{x}^{(i)} + \mathbf{b} \text{ for } 0 \leqslant i < n$$

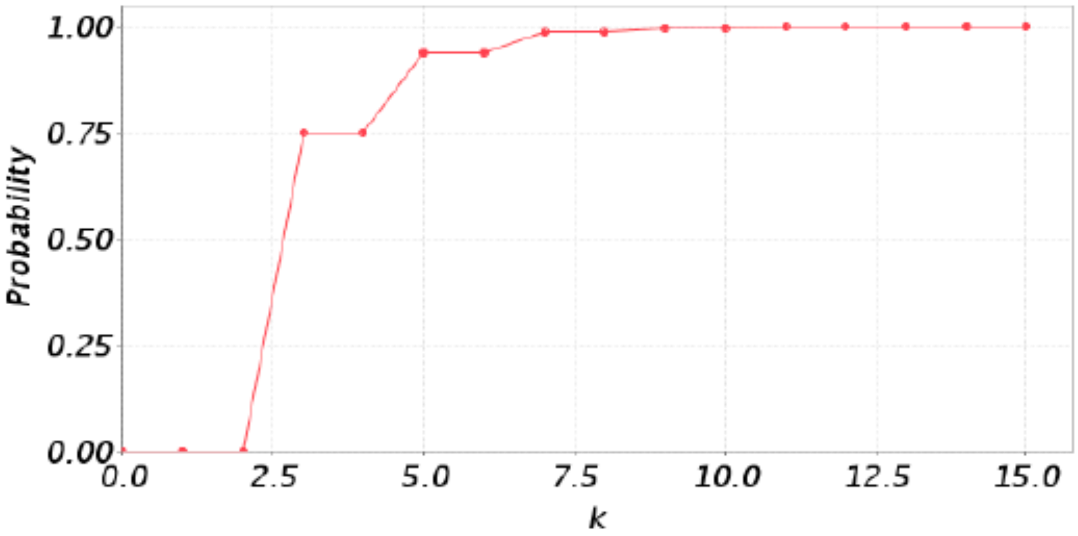
- where $\mathbf{A} = \big(\mathbf{P}(s,t)\big)_{s,t \in C \setminus B}$ and $\mathbf{b} = \big(\mathbf{P}(s,B)\big)_{s \in C \setminus B}$

- Then: $\mathbf{x}^{(n)}(s) = Pr(s \models C \,\mathsf{U}^{\leqslant n} B)$ for $s \in C \setminus B$

Bounded reachability probabilities

- $\text{ProbReach}(s_0, \{1,2,3,4,5,6\}) = 1$
- $\text{ProbReach}^{\leq k}(s_0, \{1,2,3,4,5,6\}) = \ldots$





Example on constrained reachability

Transient probabilities

- Given that $\mathbf{A}^n(s,t) = Pr(s \models S_? \, \mathsf{U}^{=n} \, t)$
  - if $B = \varnothing$, $C = S$, we have $S_{=1} = S_{=0} = \varnothing$ and $S_? = S$ and $\mathbf{A} = \mathbf{P}$
  - $\mathbf{P}^n(s,t)$ is the probability to be in state t after n steps once started in s

- Transient probability: $\Theta_n^{\mathcal{M}}(t) = \sum_{s \in S} \iota_{\text{init}}(s) \cdot \mathbf{P}^n(s,t)$

- $\Theta_n^{\mathcal{M}} = \underbrace{\mathbf{P} \cdot \mathbf{P} \cdot \ldots \cdot \mathbf{P}}_{n \text{ times}} \cdot \iota_{\text{init}} = \mathbf{P}^n \cdot \iota_{\text{init}}$
  - where the initial distribution ι_{init} is viewed as column-vector

- Compute $\Theta_n^{\mathcal{M}}$ by successive vector-matrix multiplication:

$$\Theta_0^{\mathcal{M}} = \iota_{\text{init}}, \qquad \Theta_n^{\mathcal{M}} = \mathbf{P} \cdot \Theta_{n-1}^{\mathcal{M}} \text{ for } n \geqslant 1$$

Reachability = transient probabilities

- Suppose we want to compute probabilities for $\Diamond^{\leqslant n} B$ in $\mathcal{M}$
  - observe: once B is reached, remaining behaviour is not important
- Adapt $\mathcal{M}$ by making all states in B absorbing
  - $\mathbf{P}_B(s,t) = \mathbf{P}(s,t)$ if $s \notin B$ and $\mathbf{P}_B(s,s) = 1$ for $s \in B$
  - all outgoing transitions of $s \in B$ are replaced by a single self-loop at s
- Then:

$$\underbrace{Pr^{\mathcal{M}}(\Diamond^{\leqslant n} B)}_{\text{reachability in } \mathcal{M}} = \underbrace{\sum_{s' \in B} \Theta_n^{\mathcal{M}_B}(s')}_{\text{transient probability in } \mathcal{M}_B}$$

Constrained reachability = transient probabilities

- Suppose we want to compute probabilities for $C \, \mathsf{U}^{\leqslant n} B$ in $\mathcal{M}$
  - observe: once B is reached, remaining behaviour is not important
  - observe: once $s \in S \setminus (C \cup B)$ is reached, remaining behaviour not important
- Adapt $\mathcal{M}$ by making all states in B and $S \setminus (C \cup B)$ absorbing
  - $\mathbf{P}_B(s,t) = \mathbf{P}(s,t)$ if $s \notin B$ and $\mathbf{P}_B(s,s) = 1$ for $s \in B$ or $s \in C \cup B$
- Then:

$$\underbrace{Pr^{\mathcal{M}}(C \, \mathsf{U}^{\leqslant n} B)}_{\text{reachability in } \mathcal{M}} = \underbrace{\sum_{s' \in B} \Theta_n^{\mathcal{M}_{C,B}}(s')}_{\text{transient probability in } \mathcal{M}_{C,B}}$$

Example

Qualitative properties

- Quantitative properties
  - what is the probability of an event?
- Qualitative properties
  - does an event happen with probability one?, or
  - does an event happen with probability larger than zero?
- For finite MCs, qualitative properties do only depend on state graph
  - and not on the transition probabilities!
  - e.g., limit behaviour depends on the bottom strongly connected components
  - and almost sure reachability or repeated reachability are graph properties

Measurability of some events

Let $T \subseteq S$ a subset of states in a (possibly infinite) DTMC.

- The event $\Box\Diamond T$ is measurable
  - $\Box\Diamond T$ can be written as countable intersection of countable unions of cylinder sets:

$$\Box\Diamond T \;=\; \bigcap_{n \geqslant 0} \; \bigcup_{m \geqslant n} \textit{Cyl}(\text{“}(m{+}1)\text{-st state is in } T\text{”})$$

  - where *Cyl*$(\ldots)$ is the union of all cylinder sets *Cyl*$(t_0 \ldots t_m)$ for $t_0 \ldots t_m \in$ *Paths*$_{fin}(\mathcal{M})$ and $t_m \in T$

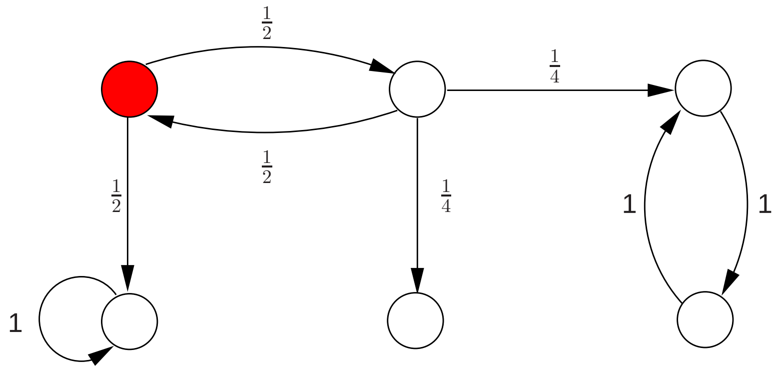
- The event $\Diamond\Box T$ is measurable
  - as it is the complement of the measurable event $\Box\Diamond(S \setminus T)$

Graph notions

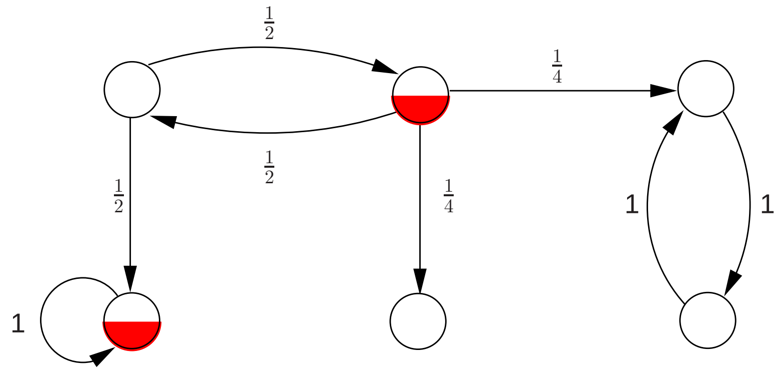
Let $\mathcal{M} = (S, \mathbf{P}, \iota_{\text{init}}, \mathit{AP}, L)$ be a *finite* Markov chain

- $T \subseteq S$ is *strongly connected* if:
  - $s \in T$ and $t \in T$ are mutually reachable via edges in T
- T is a *strongly connected component* (SCC) of $\mathcal{M}$ if:
  - it is strongly connected and no proper superset of T is strongly connected
- T is a *bottom SCC* (BSCC) if:
  - it is an SCC and no state outside T is reachable from T
  - for any state $t \in T$ it holds $\mathbf{P}(s, T) = \sum_{t \in T} \mathbf{P}(s, t) = 1$
  - let *BSCC*$(\mathcal{M})$ denote the set of BSCCs of $\mathcal{M}$

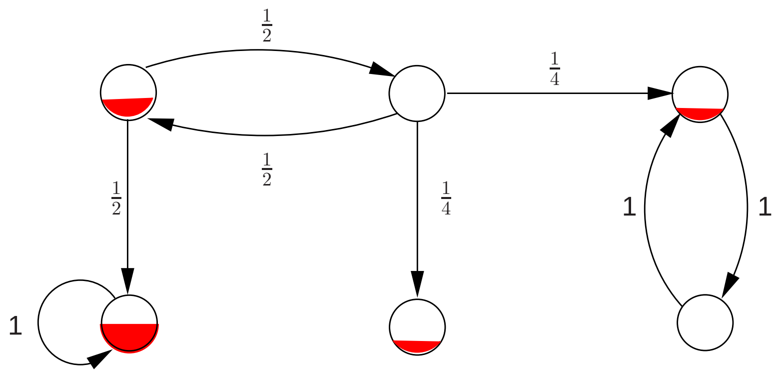
Evolution of an example DTMC



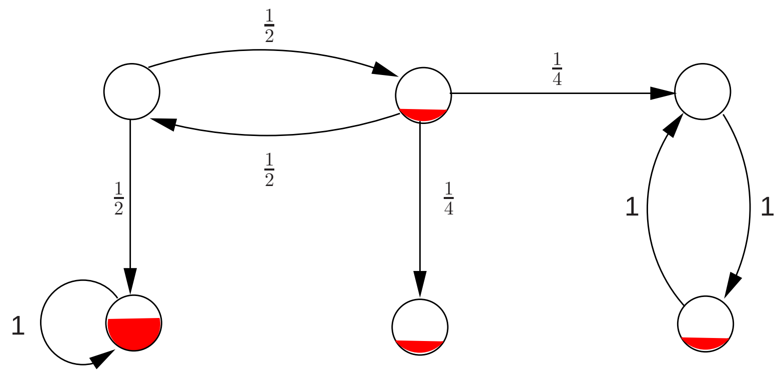
zero-th epoch



first epoch

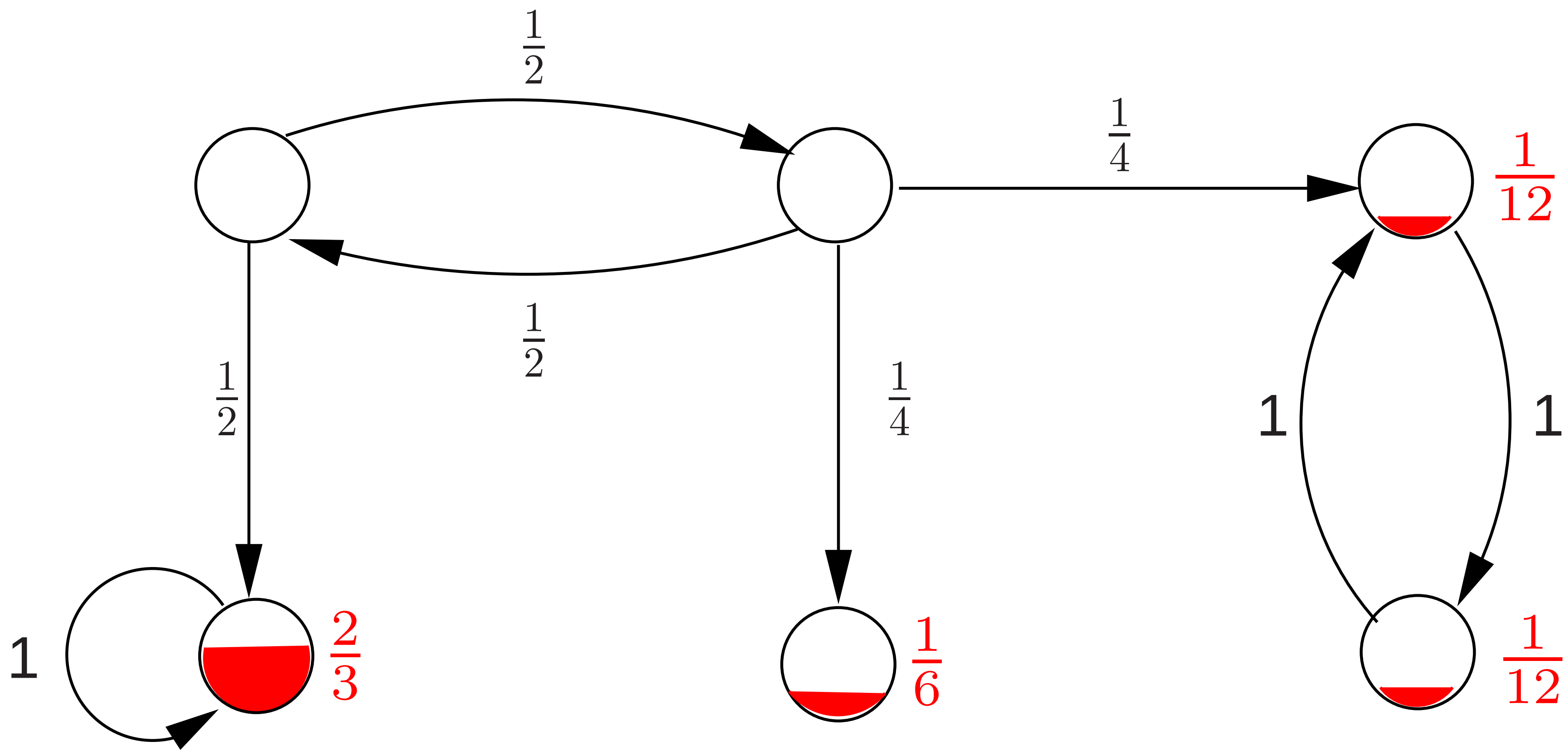


second epoch



third epoch

On the long run



probability mass is only left in bottom SCCs

Fundamental result

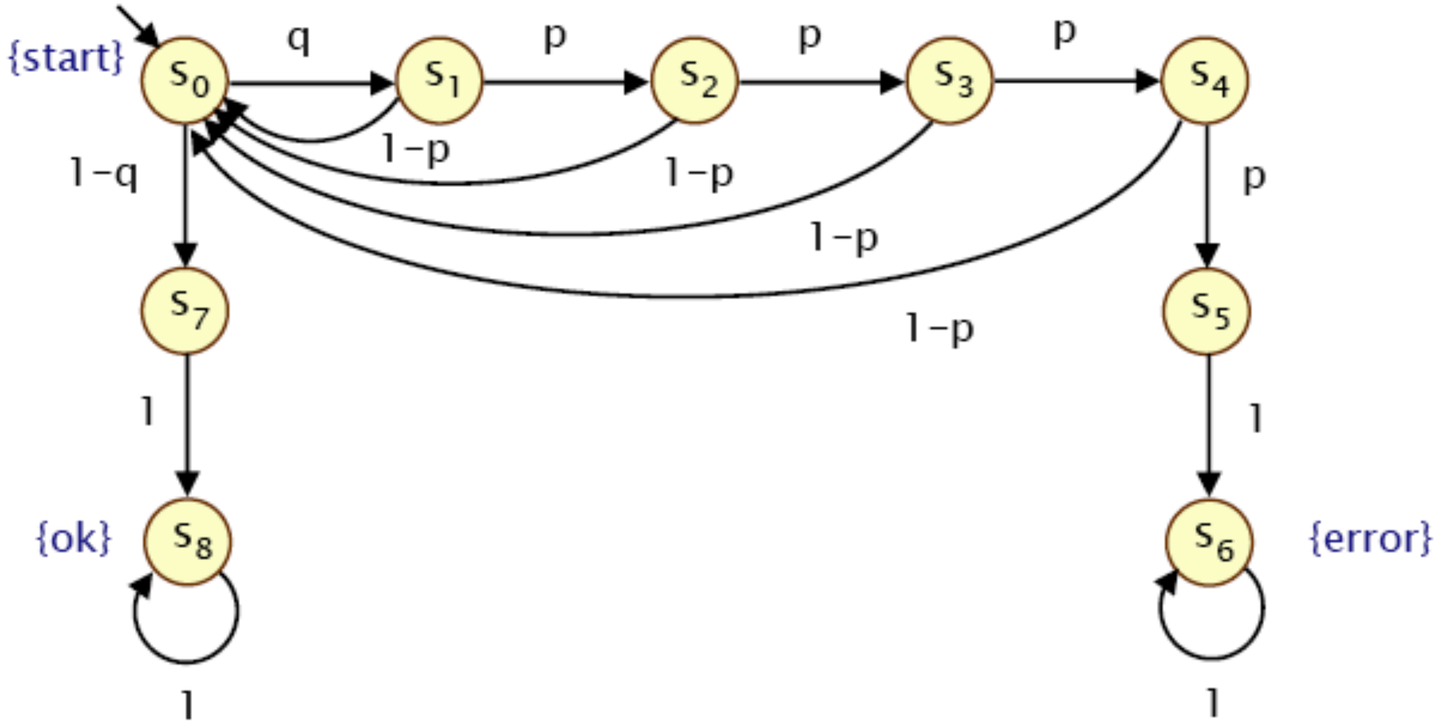
For each state s of a finite Markov chain $\mathcal{M}$:

$$Pr_s\{\ \pi \in Paths(s) \mid \inf(\pi) \in BSCC(\mathcal{M})\ \} = 1$$

almost surely any finite DTMC eventually reaches a BSCC
and visits all its states infinitely often

Zeroconf example

- 2 BSCCs: $\{s_6\}$, $\{s_8\}$
- Probability of trying to acquire a new address infinitely often is 0



Almost sure reachability

For finite DTMC with state space S, $s \in S$ and $B \subseteq S$ a set of absorbing states:

$$Pr(s \models \Diamond B) = 1 \quad \text{iff} \quad s \in S \setminus Pre^*\Big(S \setminus Pre^*(B) \Big)$$

Proof

Computing almost sure reachability properties

- Given finite DTMC $\mathcal{M}$ and $B \subseteq S$, determine:

$$s \in S \quad \text{such that} \quad \mathit{Pr}(s \models \Diamond B) = 1$$

1. Make all states in B absorbing (yielding $\mathcal{M}_B$)
2. Determine $S \setminus \mathit{Pre}^*\big(\, S \setminus \mathit{Pre}^*(B)\,\big)$ by a graph analysis
   - do a backward search from B in $\mathcal{M}_B$ to determine $\mathit{Pre}^*(B)$
   - then a backward search from $S \setminus \mathit{Pre}^*(B)$ in $\mathcal{M}_B$

- Time complexity: linear in the size of $\mathcal{M}$

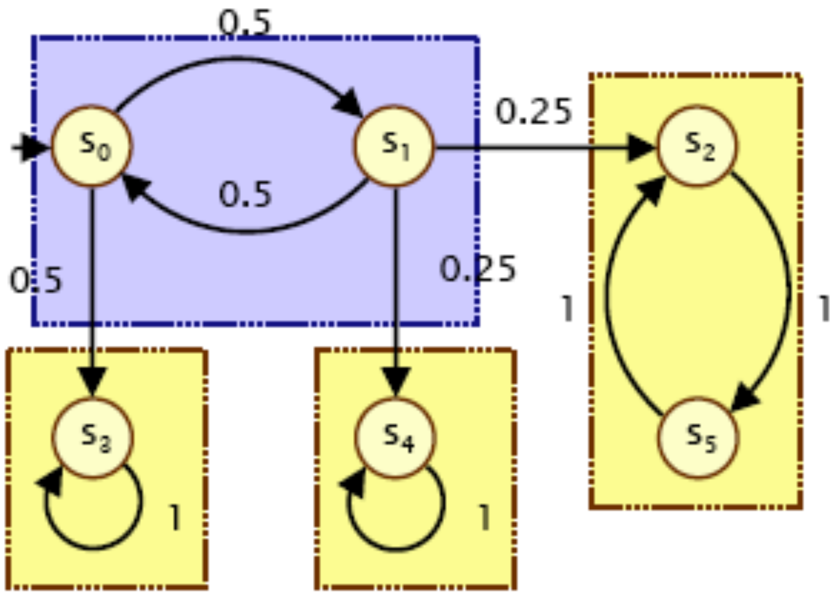
Qualitative repeated reachability

For finite DTMC with state space S, $B \subseteq S$, and $s \in S$:

$$\textit{Pr}(s \models \Box\Diamond B) = 1 \quad \text{iff} \quad \text{for each BSCC } T \subseteq \textit{Post}^*(s).\, T \cap B \neq \varnothing$$

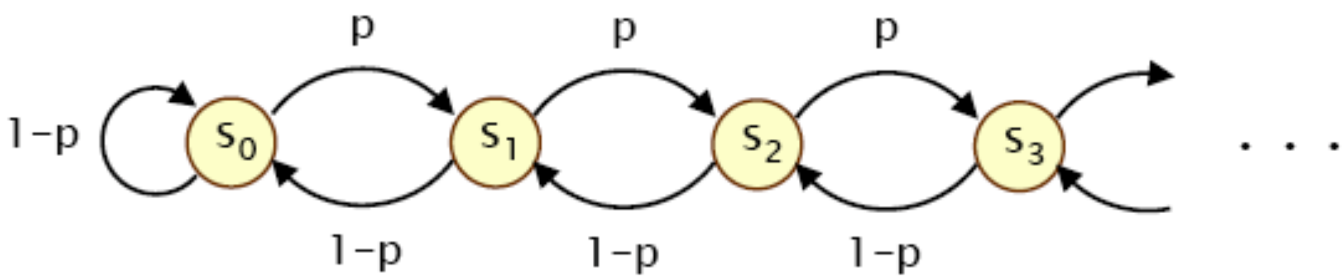
Example:

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



A remark on infinite Markov chains

- For infinite MCs, qualitative properties may rely on transition probs



- Value of probability p does affect qualitative properties:

$$Pr(s \models \Diamond\, s_0) = \begin{cases} 1 & \text{if } p \leqslant \frac{1}{2} \\ < 1 & \text{if } p > \frac{1}{2} \end{cases} \quad \text{and} \quad Pr(s \models \Box\Diamond\, s_0) = \begin{cases} 1 & \text{if } p \leqslant \frac{1}{2} \\ 0 & \text{if } p > \frac{1}{2} \end{cases}$$

Quantitative repeated reachability

For finite DTMC with state space S, $B \subseteq S$, and $s \in S$:

$$\mathit{Pr}(s \models \Box\Diamond B) \;=\; \mathit{Pr}(s \models \Diamond U)$$

where U is the union of all BSCCs T with $T \cap B \neq \varnothing$

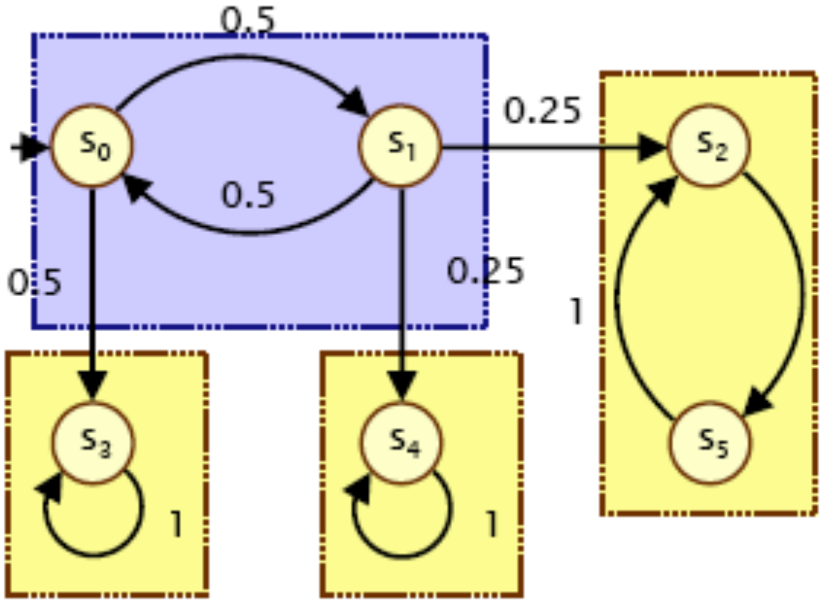
Qualitative persistence

For finite DTMC with state space S, $B \subseteq S$, and $s \in S$:

$$Pr(s \models \Diamond\Box B) = 1 \quad \text{iff} \quad T \subseteq B \text{ for any BSCC } T \subseteq Post^*(s)$$

Example:

$B = \{ s_2, s_3, s_4, s_5 \}$



Quantitative persistence

For finite DTMC with state space S, $B \subseteq S$, and $s \in S$:

$$Pr(s \models \Diamond\Box B) \; = \; Pr(s \models \Diamond U)$$

where U is the union of all BSCCs T with $T \subseteq B$