Reachability in Markov Chains

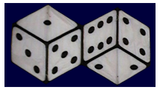
Lecture #19 of Advanced Model Checking

Joost-Pieter Katoen

Lehrstuhl 2: Software Modeling & Verification

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

January 18, 2006

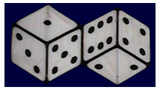


Probabilities help

- When analysing system performance and dependability
  - to quantify arrivals, waiting times, time between failure, QoS, ...
- When modelling uncertainty in the environment
  - to quantify environmental factors in decision support
  - to quantify unpredictable delays, express soft deadlines, ...
- When building protocols for networked embedded systems
  - randomized algorithms
- When analysing large populations
  - number of nodes in the internet, number of end-users, ...

Probabilistic verification so far

- Termination of probabilistic programs (Hart, Sharir & Pnueli, 1983)
  - does a probabilistic program terminate with probability one?
- Markov decision processes (Courcoubetis & Yannakakis, 1988)
  - does a certain (linear) temporal logic formula hold with probability p?
- Discrete-time Markov chains (Hansson & Jonsson, 1990)
  - can we reach a goal state via a given trajectory with probability p?
- Discrete-time Markov decision processes (Bianco & de Alfaro, 1995)
  - what is the maximal (or minimal) probability of doing this?
- Continuous-time Markov chains (Baier, Katoen & Hermanns, 1999)
  - can we do so within a given time interval I?



Characteristics

- What is inside?
  - temporal logics and model checking
  - numerical and optimisation techniques from performance and OR
- What can be checked?
  - time-bounded reachability, long-run averages, safety and liveness
- What is its usage?
  - powerful tools: PRISM (4,000 downloads), MRMC, Petri net tools, Probmela
  - applications: distributed systems, security, biology, quantum computing . . .

A synchronous leader election protocol

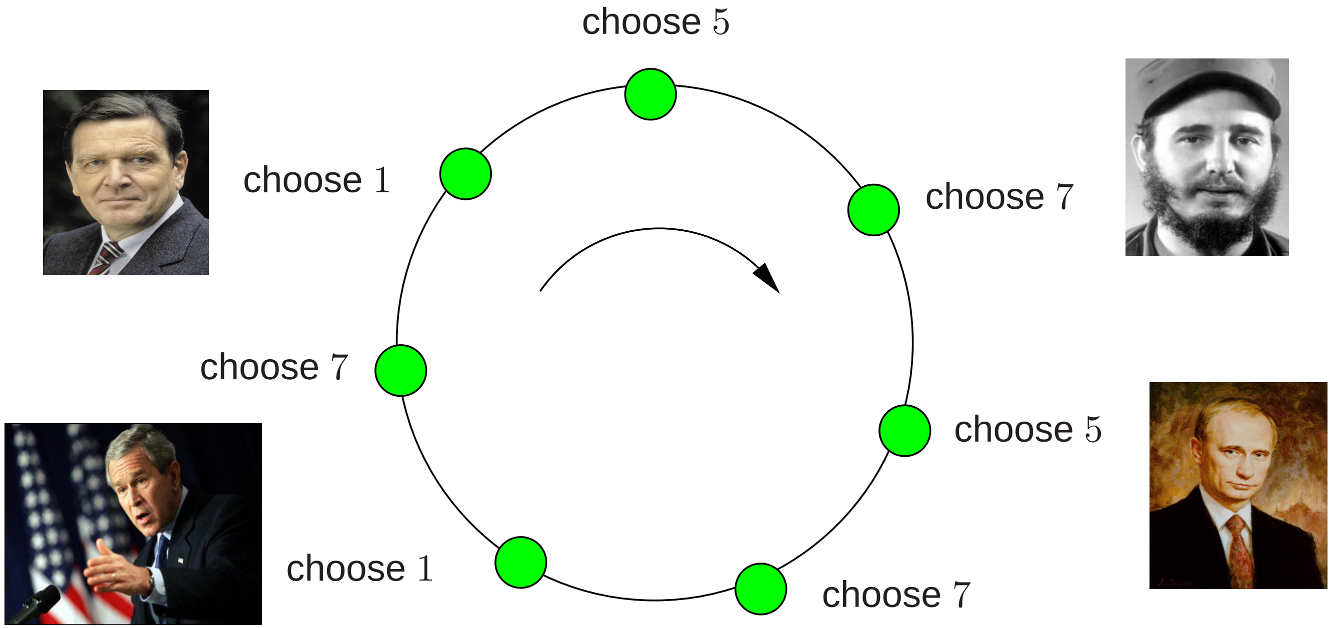
(Itai & Rodeh, 1990)

- A round-based protocol in a synchronous ring of $N > 2$ nodes
  - the nodes proceed in a lock-step fashion
  - each slot = 1 message is read + 1 state change + 1 message is sent

  $\Rightarrow$ this synchronous computation yields a Markov chain

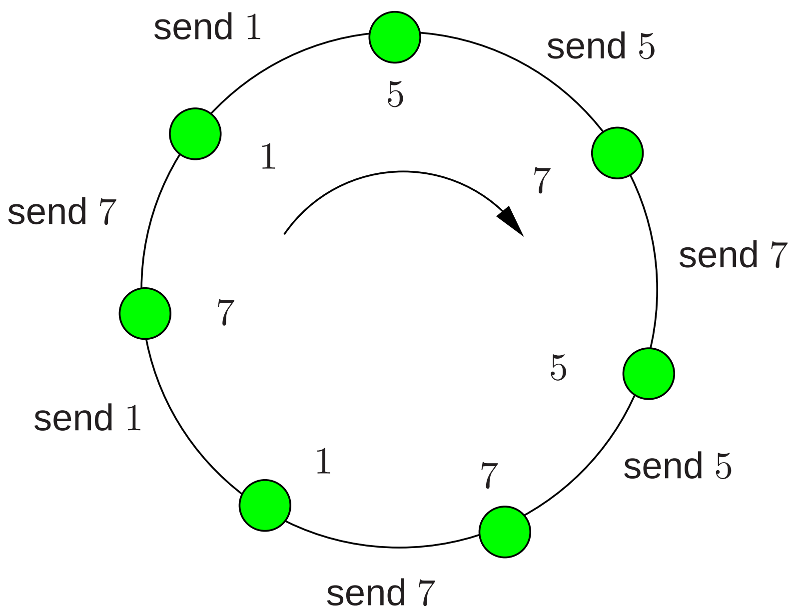
- Each round starts by each node choosing a uniform id $\in \{ 1, \ldots, K \}$
- Nodes pass their selected id around the ring
- If there is a unique id, the node with the maximum unique id is leader
- If not, start another round and try again $\ldots$

Leader election



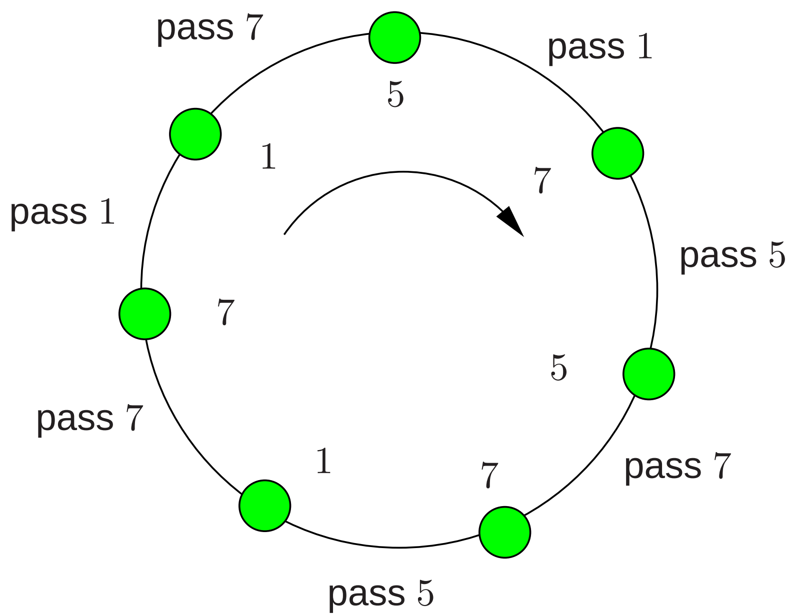
probabilistically choose an id from $[1 \ldots K]$

Leader election



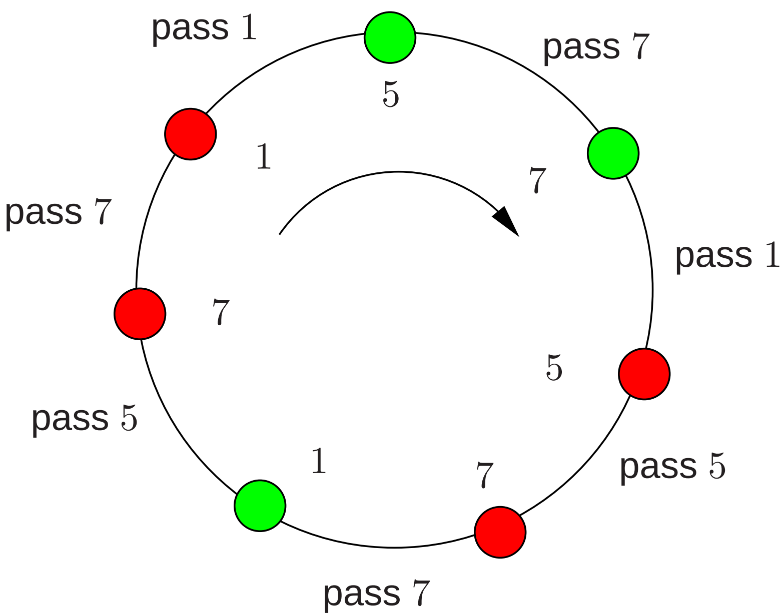
send your selected id to your neighbour

Leader election



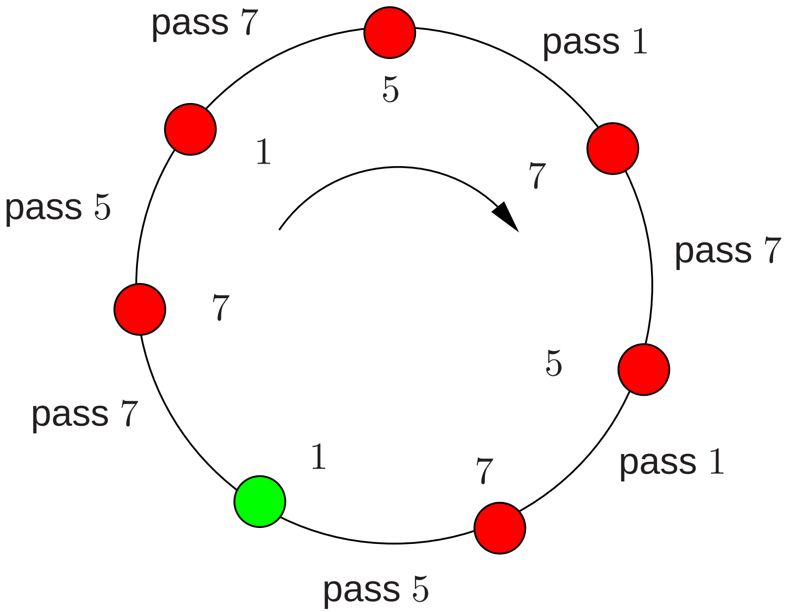
pass the received id, and check uniqueness own id

Leader election



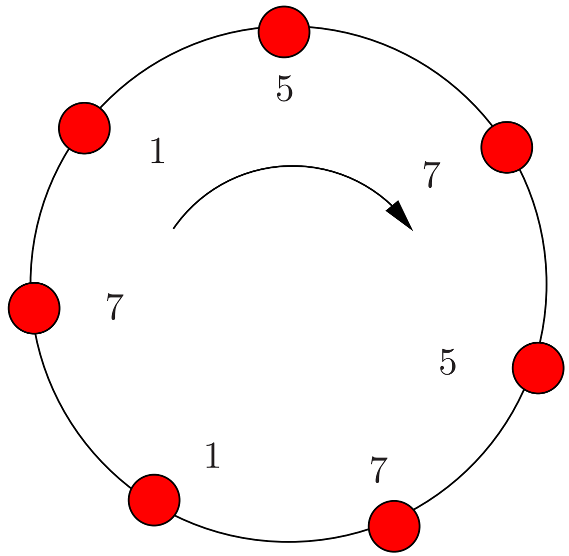
pass the received id, and check uniqueness own id

Leader election



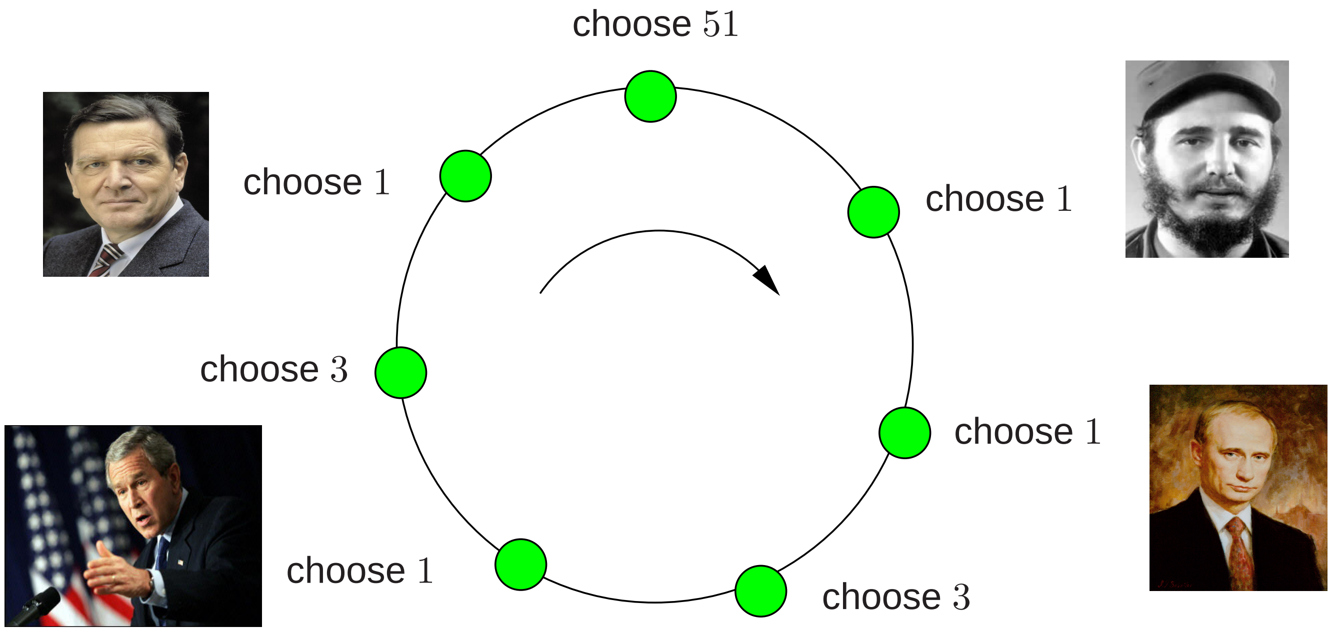
pass the received id, and check uniqueness own id

End of 1st round



no unique leader has been elected

Start a new round



new round and new chances!

Properties of leader election

- Almost surely eventually a leader will be elected:

$$\mathbb{P}_{=1}(\Diamond \textit{leader elected})$$

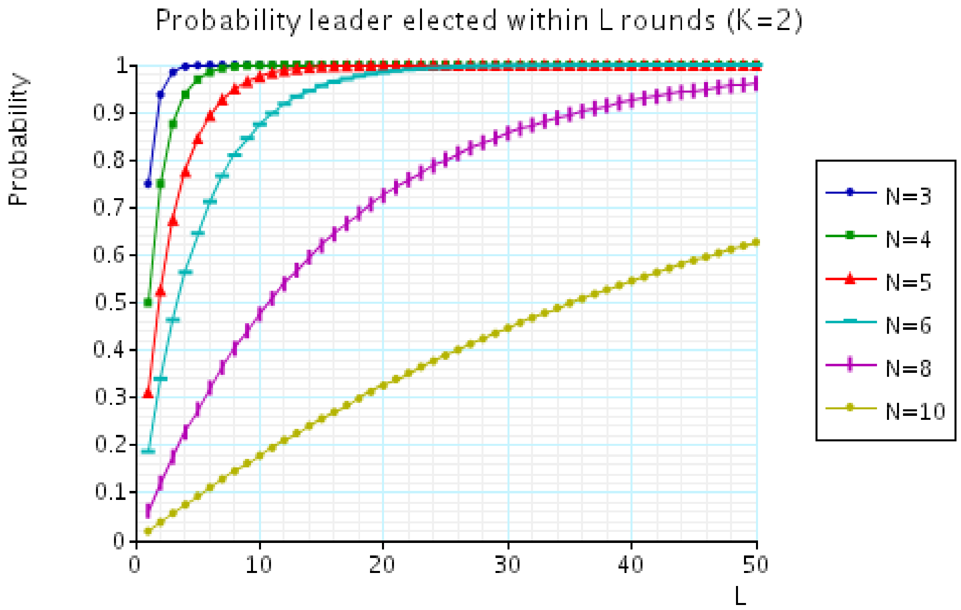
- With probability $\geqslant \frac{4}{5}$, eventually a leader is elected :

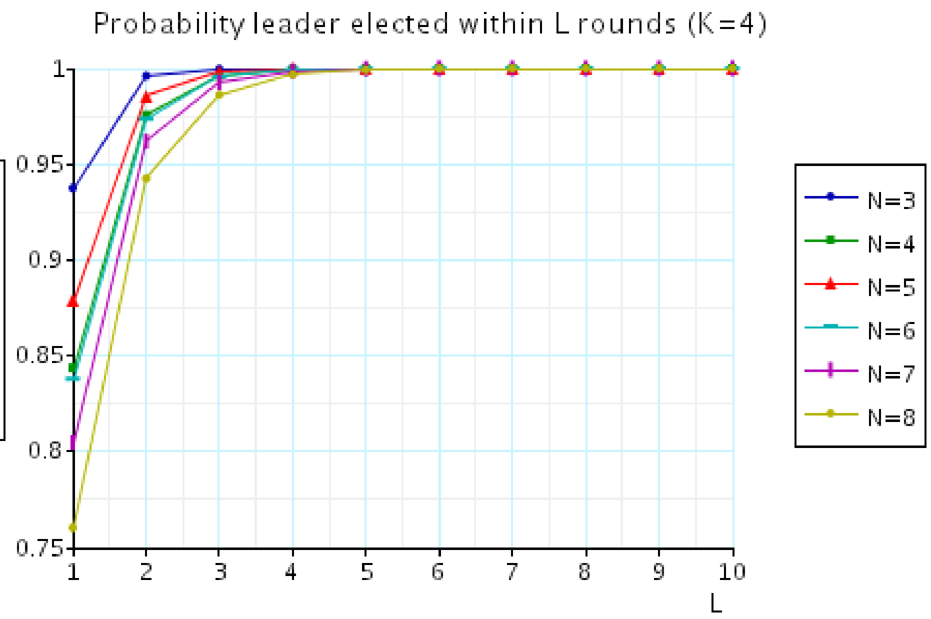
$$\mathbb{P}_{\geqslant 0.8}(\Diamond \textit{leader elected})$$

- . . . . . . within k steps:

$$\mathbb{P}_{\geqslant 0.8}(\Diamond^{\leqslant k} \textit{leader elected})$$

Probability to elect a leader within L rounds





$\mathbb{P}_{\leqslant q}(\Diamond^{\leqslant (N+1)\cdot L}$ *leader elected*$)$ (Itai & Rodeh's algorithm)

Discrete-time Markov chains

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

- S is a countable nonempty set of states
- $\mathbf{P} : S \times S \to [0,1]$, 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
- $\iota_{init} : S \to [0,1]$, the initial distribution with $\sum_{s \in S} \iota_{init}(s) = 1$
  - $\iota_{init}(s)$ is the probability that system starts in state s
  - state s for which $\iota_{init}(s) > 0$ is an initial state
- $L : S \to 2^{AP}$, the labelling function

$\Rightarrow$ a DTMC is a transition system with only probabilistic transitions

Example

Paths

- State graph of DTMC $\mathcal{M}$
  - vertices 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 inits state graph
  - for path π in $\mathcal{M}$, $\mathrm{inf}(\pi)$ is the set of states that are visited infinitely often in π
  - *Paths*$(\mathcal{M})$ and *Paths*$_{\mathit{fin}}(\mathcal{M})$ denote the set of (finite) paths in $\mathcal{M}$
- *Post*$(s) = \{ s' \in S \mid \mathbf{P}(s, s') > 0 \}$ and *Pre*$(s) = \{ s' \in S \mid \mathbf{P}(s', s) > 0 \}$
  - *Post*$^*(s)$ is the set of states reachable from s via a finite path fragment
  - *Pre*$^*(s) = \{ s' \in S \mid s \in$ *Post*$^*(s') \}$

σ-algebra

$(\Omega, \mathcal{F})$ with $\mathcal{F} \subseteq 2^{\Omega}$ is a *σ-algebra* if:

1. $\varnothing \in \mathcal{F}$
2. $E \in \mathcal{F} \;\Rightarrow\; \Omega - E \in \mathcal{F}$, and
3. $(\forall i \geqslant 0.\ E_i \in \mathcal{F})$ implies $\bigcup_{i \geqslant 0} E_i \in \mathcal{F}$

The elements of a σ-algebra are called *measurable sets* (or: *events*)

$\Omega \in \mathcal{F}$ and $\mathcal{F}$ is closed under countable intersections

Probability space

A *probability space* is a structure $(\Omega, \mathcal{F}, \Pr)$ with:

- σ-algebra $(\Omega, \mathcal{F})$
- $\Pr : \mathcal{F} \rightarrow [0, 1]$ is a *probability measure*, i.e.:
  1. $\Pr(\Omega) = 1$, and
  2. $\Pr\left(\bigcup_{i=1}^{\infty} E_i\right) = \sum_{i=1}^{\infty} \Pr(E_i)$ for $E_i \in \mathcal{F}$ and $E_i \cap E_j = \varnothing$ for $i \neq j$

$\Pr(E)$ is the probability of E, i.e., E is measurable

Properties of probability measures

- An event E with $\Pr(E) = 1$ is called *almost sure*
  - $\Pr(D) \;=\; \Pr(E \cap D) + \underbrace{\Pr(D \setminus E)}_{=0} \;=\; \Pr(E \cap D)$

- $E_1, \ldots, E_n$ are almost sure implies $\bigcap_{1 \leqslant i \leqslant n} E_i$ is almost sure

- For any Ω and $\mathcal{F} \subseteq 2^{\Omega}$ there exists a *smallest* σ-algebra containing $\mathcal{F}$
  - it is obtained by taking the intersection over all σ-algebras on Ω that contain $\mathcal{F}$
  - this is called the σ-algebra *generated* by $\mathcal{F}$
  - $\mathcal{F}$ is called the *basis* for this σ-algebra

Probability measure on DTMCs

- 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 $\hat{\pi}$:

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

  - cylinder sets serve as basis events of the smallest σ-algebra on $\mathit{Paths}(\mathcal{M})$
- $\Pr$ is the *probability measure* on the σ-algebra on $\mathit{Paths}(\mathcal{M})$:

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

  - where $\mathbf{P}(s_0\, s_1 \ldots s_n) \;=\; \prod_{0 \leqslant i < n} \mathbf{P}(s_i, s_{i+1})$
  - and $\mathbf{P}(s_0) = 1$ for paths of length zero

Reachability probabilities

- What is the probability to reach a set of states $B \subseteq S$ in DTMC $\mathcal{M}$?
  - B could be certain *bad* states which should be visited only seldomly
- Which event does $\Diamond B$ mean formally?
  - the union of all cylinders *Cyl*$(s_0 \ldots s_n)$ where
  - $s_0 \ldots s_n$ is an initial path fragment in $\mathcal{M}$ with $s_0, \ldots, s_{n-1} \notin B$ and $s_n \in B$

$$\Pr(\Diamond B) = \sum_{s_0 \ldots s_n \in \mathit{Paths}_{\mathit{fin}}(\mathcal{M}) \cap (S \setminus B)^* B} \Pr\big(\mathit{Cyl}(s_0 \ldots s_n)\big)$$

$$= \sum_{s_0 \ldots s_n \in \mathit{Paths}_{\mathit{fin}}(\mathcal{M}) \cap (S \setminus B)^* B} \iota_{\mathit{init}}(s_0) \cdot \mathbf{P}(s_0 \ldots s_n)$$

Reachability probabilities by infinite sums

Reachability probabilities in finite DTMCs

- Let $\Pr(s \models \Diamond B) = \Pr_s(\Diamond B) = \Pr_s\{\pi \in \mathit{Paths}(s) \mid \pi \models \Diamond B\}$
  - where $\Pr_s$ is the probability measure in $\mathcal{M}$ with only initial state s
- Let variable $x_s = \Pr(s \models \Diamond B)$ 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 $s \in \mathit{Pre}^*(B) \setminus B$:

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

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 $\tilde{S} = \mathit{Pre}^*(B) \setminus B$
  - $\mathbf{A} \;=\; \Big(\mathbf{P}(s,t) \Big)_{s,t \in \tilde{S}}$, the transition probabilities in $\tilde{S}$
  - $\mathbf{b} \;=\; \big(b_s \big)_{s \in \tilde{S}}$ 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 $\mathcal{M} = (S, \mathbf{P}, \iota_{init}, AP, L)$ 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

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

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

Furthermore, for $\mathbf{x}^{(0)} = \mathbf{0}$ and $\mathbf{x}^{(n+1)} = \Upsilon(\mathbf{x}^{(n)})$ 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
- $\mathbf{x} = \lim_{n \rightarrow \infty} \mathbf{x}^{(n)}$

partial ordering is: $\mathbf{y} \leqslant \mathbf{y}'$ iff $y_s \leqslant y'_s$ for all $s \in S_?$

Proof

Expansion law

- Recall in CTL: $\exists(C \, \mathsf{U} \, B)$ is the least solution of expansion law:

$$\exists(C \, \mathsf{U} \, B) \;\equiv\; B \;\vee\; (C \wedge \exists \bigcirc \exists(C \, \mathsf{U} \, B))$$

- That is: the set $X = \mathit{Sat}(\exists(C \, \mathsf{U} \, B))$ is the smallest set such that:

$$B \cup \{\, s \in C \setminus B \mid \mathit{Post}(s) \cap X \neq \varnothing \,\} \;\subseteq\; X$$

- Previous theorem “replaces” $s \in X$ by values x_s in $[0,1]$
  - if $s \in B$ then $x_s = 1$ (compare: $s \in B$ implies $s \in X$)
  - if $s \in S \setminus (C \cup B)$ then $x_s = 0$ (compare: $s \notin C \cup B$ implies $s \notin X$)

- If $s \in C \setminus B$ then $x_s = \sum_{t \in C \setminus B} \mathbf{P}(s,t) \cdot x_t + \sum_{t \in B} \mathbf{P}(s,t)$
  - compare: $s \in C \setminus B$ and $\mathit{Post}(s) \cap X \neq \varnothing$ implies $s \in X$

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:

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

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

$$\big(\Pr(s \models C \,\mathsf{U}\, B) \big)_{s \in S_?}$$

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 $s \in C \setminus B$

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

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

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

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

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:

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