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 $I$?
Advanced model checking

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 . . .
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
pass the received id, and check uniqueness own id
End of 1st round

no unique leader has been elected
Start a new round

choose 1

choose 3

choose 1

choose 51

choose 1

choose 1

choose 3

new round and new chances!
Properties of leader election

- Almost surely eventually a leader will be elected:
  \[ P_{=1}(\Diamond \text{leader elected}) \]

- With probability \( \geq \frac{4}{5} \), eventually a leader is elected:
  \[ P_{\geq 0.8}(\Diamond \text{leader elected}) \]

- ...... within \( k \) steps:
  \[ P_{\geq 0.8}(\Diamond \leq^k \text{leader elected}) \]
Probability to elect a leader within $L$ rounds

\[ P \leq q \left( \bigtriangleup \leq (N+1) \cdot L \right) \text{ leader elected} \quad \text{(Itai & Rodeh's algorithm)} \]
Discrete-time Markov chains

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

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

- **Paths** in $\mathcal{M}$ are maximal (i.e., infinite) paths in its state graph
  - for path $\pi$ in $\mathcal{M}$, $\inf(\pi)$ is the set of states that are visited infinitely often in $\pi$
  - $\text{Paths}(\mathcal{M})$ and $\text{Paths}_\text{fin}(\mathcal{M})$ denote the set of (finite) paths in $\mathcal{M}$

- $\text{Post}(s) = \{s' \in S \mid P(s, s') > 0\}$ and $\text{Pre}(s) = \{s' \in S \mid P(s', s) > 0\}$
  - $\text{Post}^*(s)$ is the set of states reachable from $s$ via a finite path fragment
  - $\text{Pre}^*(s) = \{s' \in S \mid s \in \text{Post}^*(s')\}$
\( \sigma \)-algebra

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

1. \( \emptyset \in \mathcal{F} \)

2. \( E \in \mathcal{F} \implies \Omega - E \in \mathcal{F} \), and

3. \( (\forall i \geq 0. E_i \in \mathcal{F}) \) implies \( \bigcup_{i \geq 0} E_i \in \mathcal{F} \)

The elements of a \( \sigma \)-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:

- \(\sigma\)-algebra \((\Omega, \mathcal{F})\)
- \(\Pr : \mathcal{F} \rightarrow [0, 1]\) is a probability measure, i.e.:
  1. \(\Pr(\Omega) = 1\), and
  2. \(\Pr(\bigcup_{i=1}^{\infty} E_i) = \sum_{i=1}^{\infty} \Pr(E_i)\) for \(E_i \in \mathcal{F}\) and \(E_i \cap E_j = \emptyset\) 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 \textit{almost sure}
  \[ \Pr(D) = \Pr(E \cap D) + \Pr(D \setminus E) = \Pr(E \cap D) \]

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

• For any $\Omega$ and $\mathcal{F} \subseteq 2^\Omega$ there exists a \textit{smallest} $\sigma$-algebra containing $\mathcal{F}$
  \begin{itemize}
  \item it is obtained by taking the intersection over all $\sigma$-algebras on $\Omega$ that contain $\mathcal{F}$
  \item this is called the $\sigma$-algebra \textit{generated} by $\mathcal{F}$
  \item $\mathcal{F}$ is called the \textit{basis} for this $\sigma$-algebra
  \end{itemize}
Probability measure on DTMCs

- Events are *infinite paths* in the DTMC $M$, i.e., $\Omega = Paths(M)$

- $\sigma$-algebra on $M$ is generated by *cylinder sets* of finite paths $\hat{\pi}$:
  
  $$Cyl(\hat{\pi}) = \{ \pi \in Paths(M) \mid \hat{\pi} \text{ is a prefix of } \pi \}$$

  - cylinder sets serve as basis events of the smallest $\sigma$-algebra on $Paths(M)$

- $Pr$ is the *probability measure* on the $\sigma$-algebra on $Paths(M)$:
  
  $$Pr(Cyl(s_0 \ldots s_n)) = \nu_{init}(s_0) \cdot P(s_0 \ldots s_n)$$

  - where $P(s_0 s_1 \ldots s_n) = \prod_{0 \leq i < n} P(s_i, s_{i+1})$

  - and $P(s_0) = 1$ 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 $\text{Cyl}(s_0 \ldots s_n)$ where
  - $s_0 \ldots s_n$ is an initial path fragment in $\mathcal{M}$ with $s_0, \ldots, s_{n-1} \notin B$ and $s_n \in B$

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

\[
= \sum_{s_0 \ldots s_n \in \text{Paths}_{\text{fin}}(\mathcal{M}) \cap (S \setminus B)^*B} \nu_{\text{init}}(s_0) \cdot P(s_0 \ldots s_n)
\]
Reachability probabilities by infinite sums
Reachability probabilities in finite DTMCs

- Let $\Pr(s \models \Diamond B) = \Pr(s)(\Diamond B) = \Pr_s\{\pi \in \text{Paths}(s) \mid \pi \models \Diamond B\}$
  - 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 $s \in \text{Pre}^*(B) \setminus B$:
  
  $$x_s = \sum_{t \in S \setminus B} P(s, t) \cdot x_t + \sum_{u \in B} P(s, u)$$

  - reach $B$ via $t$
  - reach $B$ in one step
Linear equation system

- These equations can be rewritten into the following form:

\[ x = Ax + b \]

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

- **Linear equation system:** \( (I - A)x = b \)

  - note: more than one solution may exist if \( I - A \) has no inverse (i.e., is singular)
  \[ \Rightarrow \text{characterize the desired probability as least fixed point} \]
Example

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

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

\[
\begin{align*}
  x_{\text{init}} &= x_{\text{try}} \\
  x_{\text{try}} &= \frac{1}{10} \cdot x_{\text{lost}} + \frac{9}{10} \\
  x_{\text{lost}} &= x_{\text{try}}
\end{align*}
\]

which can be rewritten as:

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

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

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

- $C \cup B$ is the union of the basic cylinders of path fragments:
  - $s_0 s_1 \ldots s_k$ with $k \leq n$ and $s_i \in C$ for all $0 \leq i < k$ and $s_k \in B$

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

- Let $A = (P(s, t))_{s, t \in S_{=}}$ and $(b_s)_{s \in S_{=}}$ where $b_s = P(s, S_{=1})$
Least fixed point characterization

The vector $x = \left( \Pr(s \models C \cup B) \right)_{s \in S^?}$ is the least fixed point of the operator

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

Furthermore, for $x^{(0)} = 0$ and $x^{(n+1)} = \Upsilon(x^{(n)})$ for $n \geq 0$:

- $x^{(n)} = (x_s^{(n)})_{s \in S^?}$ where for any $s$: $x_s^{(n)} = \Pr(s \models C \cup \leq^n s = 1)$

- $x^{(0)} \leq x^{(1)} \leq x^{(2)} \leq \ldots \leq x$, and

- $x = \lim_{n \to \infty} x^{(n)}$

partial ordering is: $y \leq y'$ iff $y_s \leq y'_s$ for all $s \in S^?$
Proof
Expansion law

- Recall in CTL: \( \exists (C \cup B) \) is the least solution of expansion law:
  \[
  \exists (C \cup B) \equiv B \lor (C \land \exists \circ \exists (C \cup B))
  \]

- That is: the set \( X = \text{Sat}(\exists (C \cup B)) \) is the smallest set such that:
  \[
  B \cup \{ s \in C \setminus B \mid \text{Post}(s) \cap X \neq \emptyset \} \subseteq X
  \]

- 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 \( x_s = \sum_{t \in C \setminus B} P(s, t) \cdot x_t + \sum_{t \in B} P(s, t) \)
  - compare: \( s \in C \setminus B \) and \( \text{Post}(s) \cap X \neq \emptyset \) implies \( s \in X \)
Constrained reachability probabilities

• So: \( x \) is the \textit{least} solution of \( Ax + b = x \) in \([0, 1]^S\).

• And: can be approximated by:

\[
x^{(0)} = 0 \quad \text{and} \quad x^{(n+1)} = Ax^{(n)} + b \quad \text{for} \quad n \geq 0
\]

• \textit{Power method}: compute vectors \( x^{(0)}, x^{(1)}, x^{(2)}, \ldots \) and abort if:

\[
\max_{s \in S} |x^{(n+1)}_s - x^{(n)}_s| < \varepsilon \quad \text{for some small tolerance} \, \varepsilon
\]

– 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:

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

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

$$(\Pr(s \models C \cup B))_{s \in S？}$$

is the unique solution of the linear equation system:

$$x = Ax + b \quad \text{where} \quad A = (P(s, t))_{s, t \in S？} \quad \text{and} \quad b = (P(s, S_{=1}))_{s \in S？}$$
Computing constrained reachability probabilities

- The probabilities of the events $C \cup \leq_n B$ can be obtained iteratively:

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

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

- Then: $x^{(n)}(s) = \Pr(s \models C \cup \leq_n B)$ for $s \in C \setminus B$
Transient probabilities

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

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

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

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

\[
\Theta_0^M = \nu_{\text{init}}, \quad \Theta_n^M = P \cdot \Theta_{n-1}^M \quad \text{for } n \geq 1
\]
Reachability = transient probabilities

- Suppose we want to compute probabilities for $\Diamond^{\leq n} B$ in $M$
  - observe: once $B$ is reached, remaining behaviour is not important

- Adapt $M$ by making all states in $B$ absorbing
  - $P_B(s, t) = P(s, t)$ if $s \notin B$ and $P_B(s, s) = 1$ for $s \in B$
  - all outgoing transitions of $s \in B$ are replaced by a single self-loop at $s$

- Then:
  $$\underbrace{\Pr(\Diamond^{\leq n} B)}_{\text{reachability in } M} = \sum_{s' \in B} \Theta^{M_B}_n(s')$$
  $$\underbrace{\Theta^{M_B}_n}_\text{transient probability in } M_B$$
Constrained reachability = transient probabilities

- Suppose we want to compute probabilities for \( C \cup ^{\leq n} B \) in \( M \)
  - 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 \( M \) by making all states in \( B \) and \( S \setminus (C \cup B) \) absorbing
  - \( P_B(s, t) = P(s, t) \) if \( s \notin B \) and \( P_B(s, s) = 1 \) for \( s \in B \) or \( s \in C \cup B \)

- Then:
  \[
  \Pr_{\mathcal{M}}(C \cup ^{\leq n} B) = \sum_{s' \in B} \Theta_{\mathcal{M}_{C,B}}^{\mathcal{M}}(s')
  \]