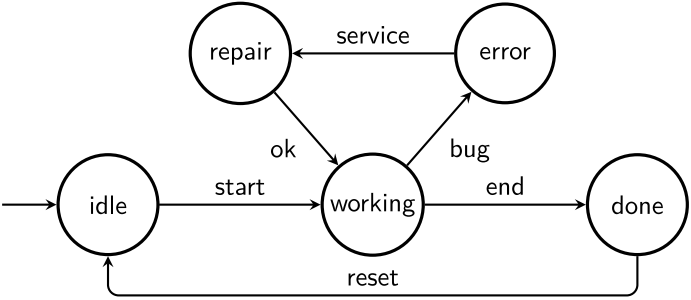
IA169 System Verification and Assurance

Verification of Systems with Probabilities

Vojtěch Řehák

Motivation example

Fail-repair system

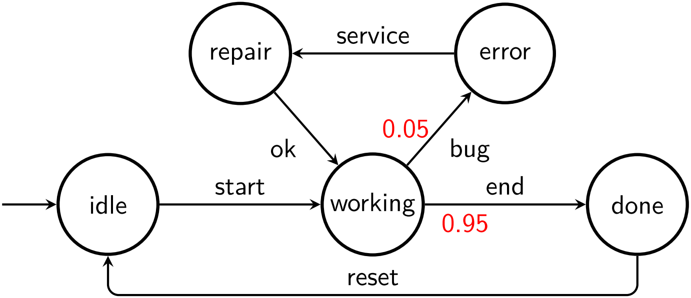


What are the properties of the model?

- $G(\text{working} \implies F \text{ done})$ **NO**
- $G(\text{working} \implies F \text{ error})$ **NO**
- $FG(\text{working} \vee \text{error} \vee \text{repair})$ **NO**

Motivation example

Fail-repair system



- What is the probability of reaching “done” from “working” with no visit of “error”?
- What is the probability of reaching “done” from “working” with at most one visit of “error”?
- What is the probability of reaching “done” from “working”?

Discrete-time Markov Chains (DTMC)

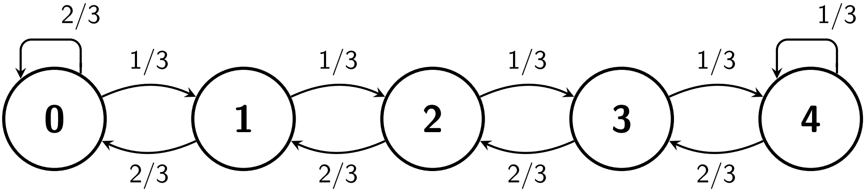
Probabilistic models

Discrete-time Markov Chains (DTMC)

- Standard model for probabilistic systems.
- State-based model with probabilities on branching.
- Based on the current state, the succeeding state is given by a discrete probability distribution.
- Markov property ("memorylessness") — only the current state determines the successors (the past states are irrelevant).
- Probabilities on outgoing edges sums to 1 for each state.
- Hence, each state has at least one outgoing edge ("no deadlock").

DTMC examples

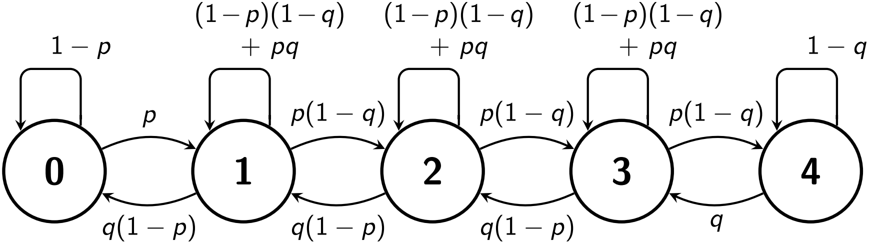
Model of a queue



Queue for at most 4 items. In every time tick, a new item comes with probability $1/3$ and an item is consumed with probability $2/3$.

What if a new items comes with probability $p = 1/2$ and an item is consumed with probability $q = 2/3$?

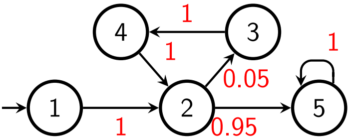
Model of the new queue



DTMC - formal definition

Discrete-time Markov Chain is given by

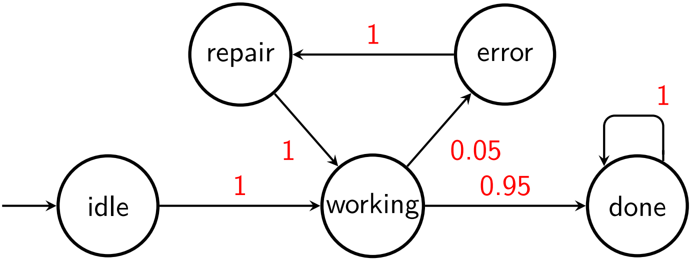
- a set of states S,
- an initial state s_0 of S,
- a probability matrix $P : S \times S \to [0,1]$, and
- an interpretation of atomic propositions $I : S \to AP$.



$$P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0.05 & 0 & 0.95 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Back to our questions

Fail-Repair System



- What is the probability of reaching “done” from “working” with no visit of “error”?
- What is the probability of reaching “done” from “working” with at most one visit of “error”?
- What is the probability of reaching “done” from “working”?

Markov chain analysis

Transient analysis

- distribution after k-steps
- reaching/hitting probability
- hitting time

Long run analysis

- probability of infinite hitting
- stationary (invariant) distribution
- mean inter visit time
- long run limit distribution

Property Specification

Property specification languages

Recall some non-probabilistic specification languages:

LTL formulae

$$\varphi ::= p \mid \neg\varphi \mid \varphi \vee \varphi \mid X\,\varphi \mid \varphi\, U\, \varphi$$

CTL formulae

$$\varphi ::= p \mid \neg\varphi \mid \varphi \vee \varphi \mid EX\,\varphi \mid E[\varphi\, U\, \varphi] \mid EG\,\varphi$$

Syntax of CTL*

state formula	$\varphi ::= p \mid \neg\varphi \mid \varphi \vee \varphi \mid E\,\psi$
path formula	$\psi ::= \varphi \mid \neg\psi \mid \psi \vee \psi \mid X\,\psi \mid \psi\, U\, \psi$

Property specification languages

We need to quantify probability that a certain behaviour will occur.

Probabilistic Computation Tree Logic (PCTL)

Syntax of PCTL

state formula	$\varphi ::= p \mid \neg\varphi \mid \varphi \vee \varphi \mid P_{\bowtie b}\psi$
path formula	$\psi ::= X\,\varphi \mid \varphi\,U\,\varphi \mid \varphi\,U^{\leq k}\,\varphi$

where

- $b \in [0, 1]$ is a probability bound,
- $\bowtie \in \{\leq, <, \geq, >\}$, and
- $k \in \mathbf{N}$ is a bound on the number of steps.

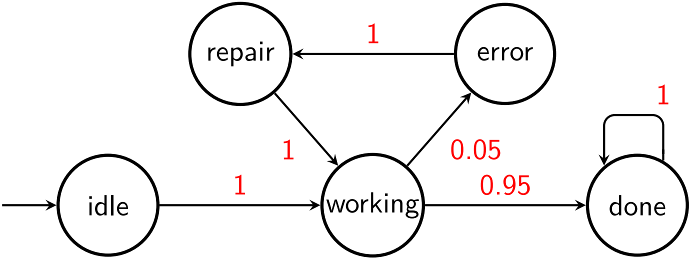
A PCTL formula is always a state formula.

$\alpha\,U^{\leq k}\,\beta$ is a bounded until saying that α holds until β within k steps.
For $k = 3$ it is equivalent to $\beta \vee (\alpha \wedge X\,\beta) \vee (\alpha \wedge X\,(\beta \vee \alpha \wedge X\,\beta))$.

Some tools also supports $P_{=?}\psi$ asking for the probability that the specified behaviour will occur.

PCTL examples

We can also use derived operators like G, F, $\wedge$, $\Rightarrow$, etc.



Probabilistic reachability $P_{\geq 1}(\, F\, done\,)$

- probability of reaching the state *done* is equal to 1

Probabilistic bounded reachability $P_{>0.99}(\, F^{\leq 6}\, done\,)$

- probability of reaching the state *done* in at most 6 steps is > 0.99

Probabilistic until $P_{<0.96}(\,(\neg error)\, U\, (done)\,)$

- probability of reaching *done* with no visit of *error* is less than 0.96

Qualitative vs. quantitative properties

Qualitative PCTL properties

- $P_{\bowtie b}\,\psi$ where b is either 0 or 1

Quantitative PCTL properties

- $P_{\bowtie b}\,\psi$ where b is in $(0, 1)$

Qualitative properties

In DTMC where zero probability edges are erased, it holds that

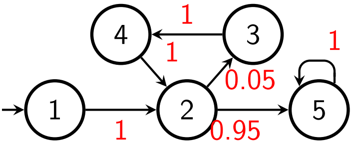
- $P_{>0}(X\,\varphi)$ is equivalent to $EX\,\varphi$
  - there is a next state satisfying φ
- $P_{\geq 1}(X\,\varphi)$ is equivalent to $AX\,\varphi$
  - the next states satisfy φ
- $P_{>0}(F\,\varphi)$ is equivalent to $EF\,\varphi$
  - there exists a finite path to a state satisfying φ

but

- $P_{\geq 1}(F\,\varphi)$ is **not** equivalent to $AF\,\varphi$
  (see, e.g., *AF done* on our running example)

There is no CTL formula equivalent to $P_{\geq 1}(F\,\varphi)$,
and no PCTL formula equivalent to $AF\,\varphi$.

Quantitative - forward reachability



$$P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0.05 & 0 & 0.95 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Probability distribution after k steps when starting in 1

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix} \times P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

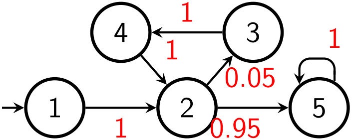
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix} \times P^2 = \begin{bmatrix} 0 & 0 & 0.05 & 0 & 0.95 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix} \times P^3 = \begin{bmatrix} 0 & 0 & 0 & 0.05 & 0.95 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix} \times P^4 = \begin{bmatrix} 0 & 0.05 & 0 & 0 & 0.95 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix} \times P^5 = \begin{bmatrix} 0 & 0 & 0.0025 & 0 & 0.9975 \end{bmatrix}$$

Quantitative - backward reachability



$$P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0.05 & 0 & 0.95 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Prob. of being in states 2 or 5 after k steps, i.e. $P_{=?}F^{=k}(2 \vee 5)$

$$P \times \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \end{bmatrix}^T = \begin{bmatrix} 1 & 0.95 & 0 & 1 & 1 \end{bmatrix}^T$$

$$P^2 \times \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \end{bmatrix}^T = \begin{bmatrix} 0.95 & 0.95 & 1 & 0.95 & 1 \end{bmatrix}^T$$

$$P^3 \times \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \end{bmatrix}^T = \begin{bmatrix} 0.95 & 1 & 0.95 & 0.95 & 1 \end{bmatrix}^T$$

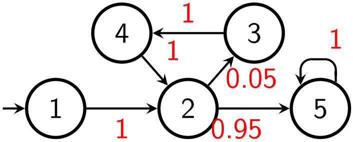
$$P^4 \times \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \end{bmatrix}^T = \begin{bmatrix} 1 & 0.9975 & 0.95 & 1 & 1 \end{bmatrix}^T$$

$$P^5 \times \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \end{bmatrix}^T = \begin{bmatrix} 0.9975 & 0.9975 & 1 & 0.9975 & 1 \end{bmatrix}^T$$

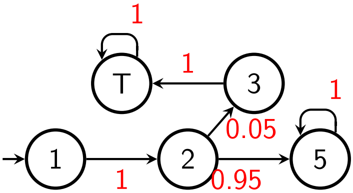
"Up to" reachability

Computing $P_{=?}\ F^{\leq 6}\ 3$.

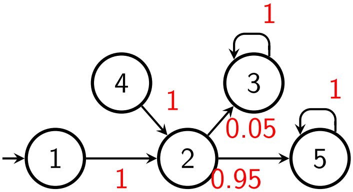
Is it $\sum_{i=0}^{6} P_{=?}\ F^{=i}\ 3$?



No, we are summing probabilities of repeated visits.
It is true when the model is changed such that repeated visits are not possible. Alternativelly we can make the target state is absorbing.



and it is $\sum_{i=0}^{6} P_{=?}\ F^{=i}\ 3$



and it is $P_{=?}\ F^{=6}\ 3$

Unbounded reachability - optional slide

Unbounded reachability

Let $p(s, A)$ be the probability of reaching a state in A from s.

It holds that:

- $p(s, A) = 1$ for $s \in A$
- $p(s, A) = \sum_{s' \in succ(s)} P(s, s') * p(s', A)$ for $s \notin A$

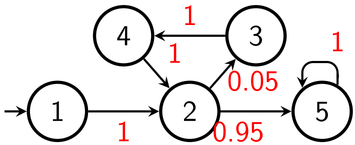
where $succ(s)$ is a set of successors of s and $P(s, s')$ is the probability on the edge from s to s'.

Theorem

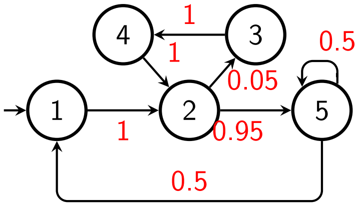
- The minimal non-negative solution of the above equations equals to the probability of unbounded reachability.

Long Run Analysis

Long run analysis



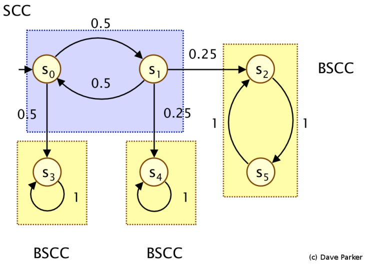
Recall that we reach the state 5(*done*) with probability 1.



What are the states visited infinitely often with probability 1?

States visited infinitely often

Decompose the graph representation onto strongly connected components.



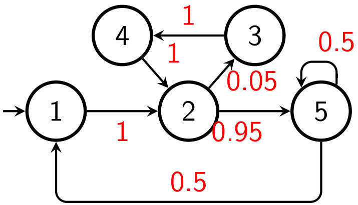
Theorem [1]

- A state is **visited infinitely often** with probability 1 if and only if it is in a **bottom strongly connected component**.
- All other states are **visited finitely many times** with probability 1.

[1] This holds only in DTMC models with finitely many states.

Frequency of visits

How often is a state visited among the states visited infinitely many times?



Theorem

$$lim_{n\to\infty} E\left(\frac{\#\text{ visits of state } i \text{ during the first } n \text{ steps}}{n}\right) = \pi_i$$

where π is a so called **stationary** (or **steady-state** or **invariant** or **equilibrium**) **distribution** satisfying $\pi \times P = \pi$.

DTMC extensions - communication and nondeterminism

Last remark on some DTMC extensions.

Modules and synchronisation

- modules
- actions
- rewards

Decision extension

- Markov Decision Processes (MDP)
- **Pmin** and **Pmax** properties