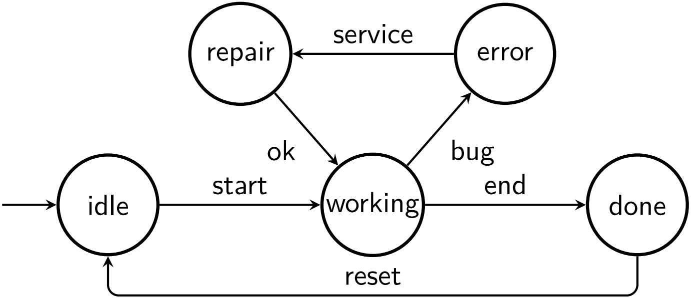
IA169 System Verification and Assurance

Verification of Systems with Probabilities

Vojtěch Řehák
Jiří Barnat

Motivation Example

Fail-repair system

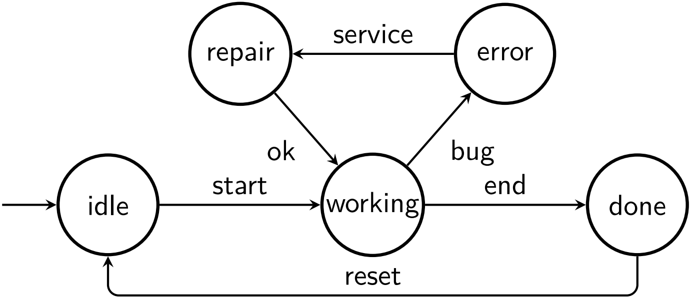


What are the properties of the model?

- $G(\text{working} \implies F \text{ done})$
- $G(\text{working} \implies F \text{ error})$
- $FG(\text{working} \vee \text{error} \vee \text{repair})$

Motivation Example

Fail-repair system

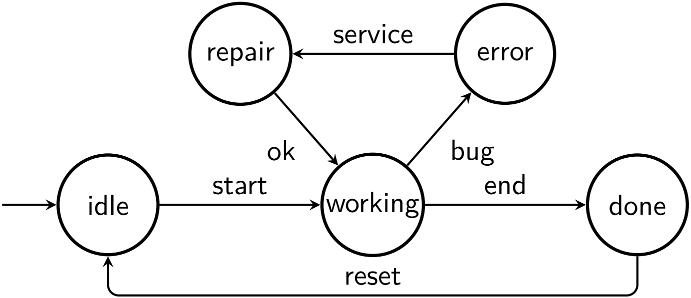


What are the properties of the model?

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

Motivation Example

Fail-repair system

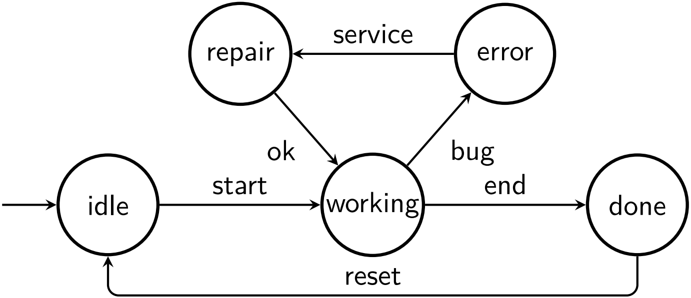


What are the properties of the model?

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

Motivation Example

Fail-repair system

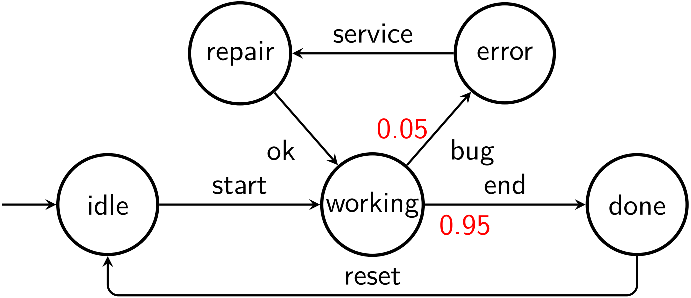


What are the properties of the model?

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

Motivation Example

Fail-repair system

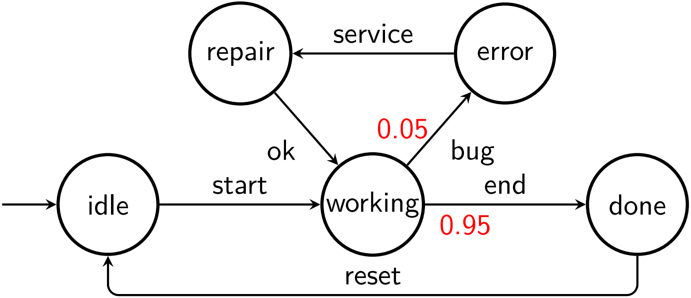


What is the probability of reaching “done” from “working”

- with no visit of “error”?
- with at most one visit of “error”?
- with arbitrary many visits of “error”?

Motivation Example

Fail-repair system

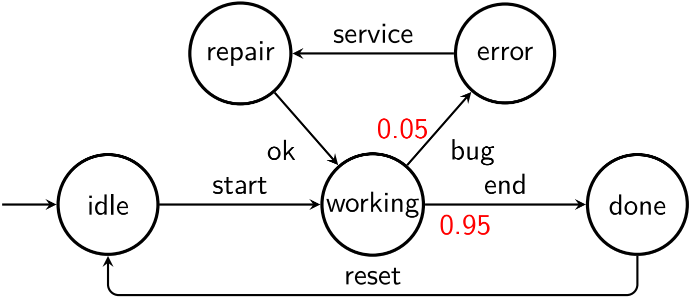


What is the probability of reaching “done” from “working”

- with no visit of “error”? **0.95**
- with at most one visit of “error”?
- with arbitrary many visits of “error”?

Motivation Example

Fail-repair system

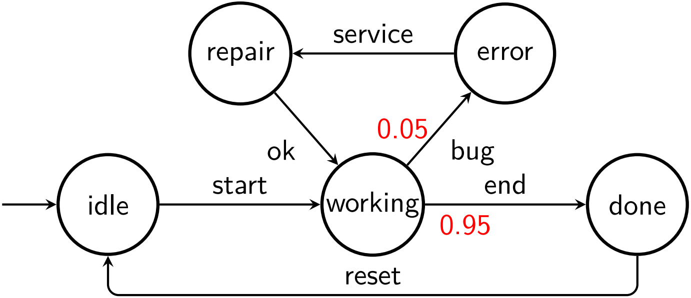


What is the probability of reaching "done" from "working"

- with no visit of "error"? **0.95**
- with at most one visit of "error"? **0.95 + (0.05*0.95)**
- with arbitrary many visits of "error"?

Motivation Example

Fail-repair system



What is the probability of reaching "done" from "working"

- with no visit of "error"? **0.95**
- with at most one visit of "error"? **0.95 + (0.05*0.95)**
- with arbitrary many visits of "error"? **1**

Discrete-time Markov Chains (DTMC)

Probabilistic Models

Discrete-time Markov Chains (DTMC)

- Standard modeling formalism for probabilistic systems.
- A finite diagram of states and state-changing transitions.
- Each transition is annotated with a probability p ($p \in [0, 1]$).
- The probabilities over transitions from a single state sum to 1. (They form discrete probability distribution.)

Observation

- Markov property ("memoryless structure") — only the current state determines the successors (the past states are irrelevant).
- Each state has at least one outgoing edge ("no deadlock").

DTMC Examples

Task: create DTMC modeling the following scenario

- A queue for at most 4 items.
- States of the graph encode how many items are enqueued.
- Every transitions encodes that either an item has arrived in the queue or one item has been consumed from the queue (exclusive or).
- Arrival of an item happens with the probability of $1/3$, while the dequeue operation happens with the probability of $2/3$.

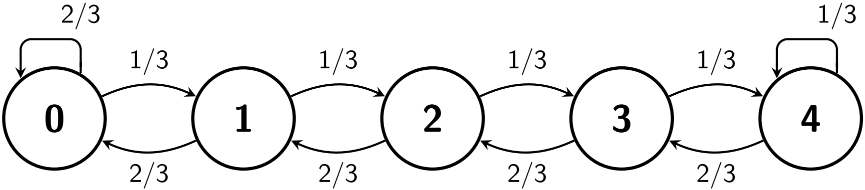
Solution

DTMC Examples

Task: create DTMC modeling the following scenario

- A queue for at most 4 items.
- States of the graph encode how many items are enqueued.
- Every transitions encodes that either an item has arrived in the queue or one item has been consumed from the queue (exclusive or).
- Arrival of an item happens with the probability of 1/3, while the dequeue operation happens with the probability of 2/3.

Solution



DTMC examples

Task: create DTMC modeling the following scenario - continued

- If the actions of item arrival and item removal are independent, they both have their own probability of appearance with every time tick.
- A new item comes with probability $p = 1/2$, an item is removed with probability $q = 2/3$?
- With every time tick, one of the actions may occur, both actions may occur simultaneously, or none of them may occur at all.

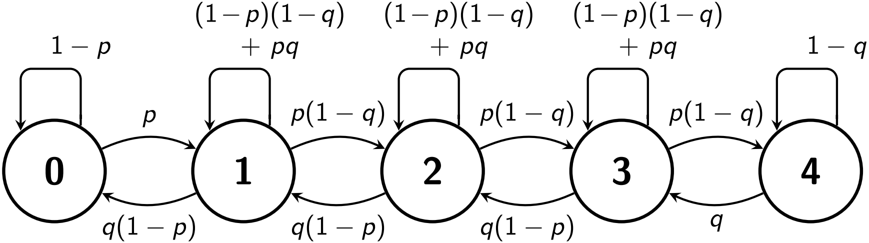
Solution

DTMC examples

Task: create DTMC modeling the following scenario - continued

- If the actions of item arrival and item removal are independent, they both have their own probability of appearance with every time tick.
- A new item comes with probability $p = 1/2$, an item is removed with probability $q = 2/3$?
- With every time tick, one of the actions may occur, both actions may occur simultaneously, or none of them may occur at all.

Solution



DTMC – Formal Definition

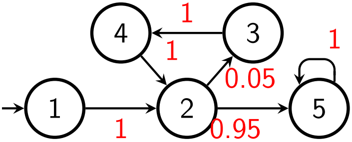
Discrete-time Markov Chain is given by

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

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 $P : S \times S \rightarrow [0, 1]$, and
- an interpretation of atomic propositions $I : S \rightarrow AP$.



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

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.

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.

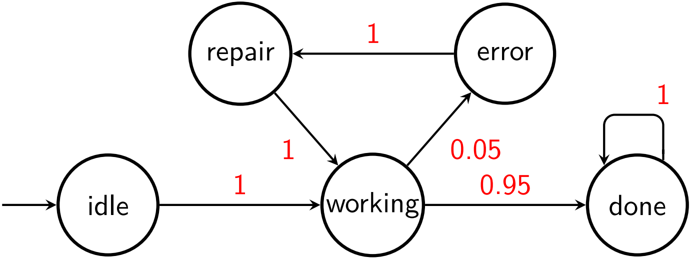
A PCTL formula is always a state formula.

$\alpha\,U^{\leq k}\,\beta$ 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 $b \in (0, 1)$

Selected Qualitative PCTL 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)

Selected Qualitative PCTL 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 $AF\,\varphi$.

Analysis of Discrete-time Markov Chains

DT Markov Chain Analysis - General Approaches

Transient analysis

- probability distribution after k-steps
- probability of reaching a state within k-steps

Long run analysis

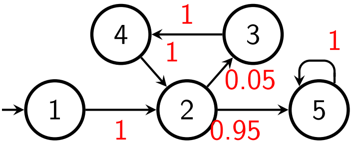
- states visited infinitely often with probability one
- stationary (invariant) distribution

Model Checking

- model checking DTMCs
- model checking MDPs

Transient Analysis

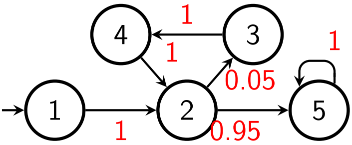
Quantitative - forward reachability



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

Probability distribution after k steps when starting in 1

Quantitative - forward reachability

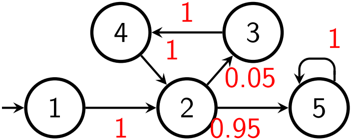


$$P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0.05 & 0 & 0.95 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Probability distribution after k steps when starting in 1

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

Quantitative - forward reachability



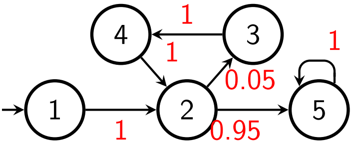
$$P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0.05 & 0 & 0.95 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Probability distribution after k steps when starting in 1

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

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

Quantitative - forward reachability



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

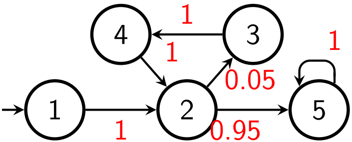
Probability distribution after k steps when starting in 1

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

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

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

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

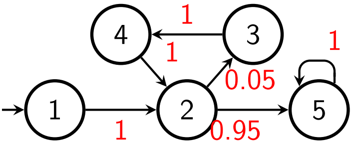
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix} \times P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

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

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

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

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

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

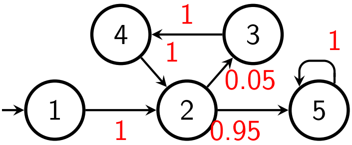
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix} \times P^2 = \begin{bmatrix} 0 & 0 & 0.05 & 0 & 0.95 \end{bmatrix}$$

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

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

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

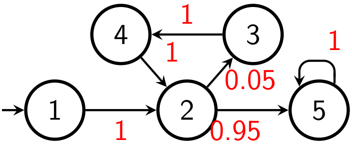
Quantitative - backward reachability



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

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

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. $P_{=?}F^{=k}(2 \vee 5)$

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

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

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

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

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

Unbounded reachability

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

Observation: 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'.

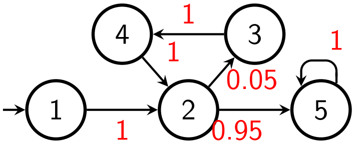
Theorem

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

"Up to" reachability

Task

- For the given DTMC compute the probability of reaching state 3 within 6 steps.
- Compute $P_{=?}\ F^{\leq 6}\ 3$.



Wrong Solution

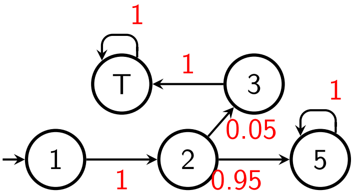
- BEWARE!
- We cannot sum the probabilities of repeated visits!

$$P_{=?}\ F^{\leq 6}\ 3 \neq \sum_{i=0}^{6} P_{=?}\ F^{=i}\ 3$$

"Up to" reachability – continued

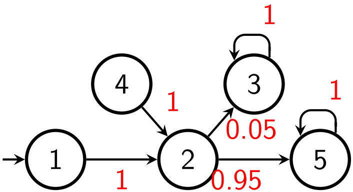
Possible Solution 1

- We may only sum the probabilities if we make sure, that no revisit of a state is possible.
- We have to modify the DTMC.
- $P_{=?}\ F^{\leq 6}\ 3 = \sum_{i=0}^{6} P_{=?}\ F^{=i}\ 3$



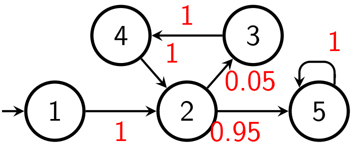
Possible Solution 2

- Alternativelly, we can make the target state absorbing.
- $P_{=?}\ F^{\leq 6}\ 3 = P_{=?}\ F^{=6}\ 3$



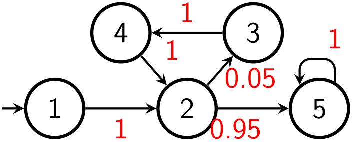
Long Run Analysis

Long run analysis

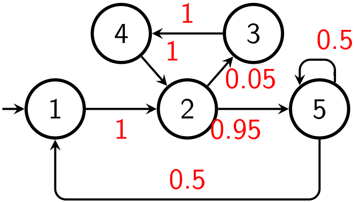


Recall that we reach the state 5(*done*) with probability 1.

Long run analysis



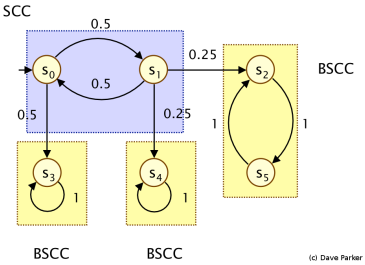
Recall that we reach the state 5(*done*) with probability 1.



What are the states visited infinitely often with probability 1?

States visited infinitely often

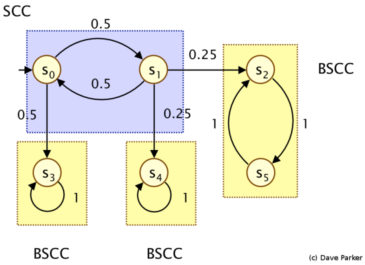
Decompose the graph representation onto strongly connected components.



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

States visited infinitely often

Decompose the graph representation onto strongly connected components.



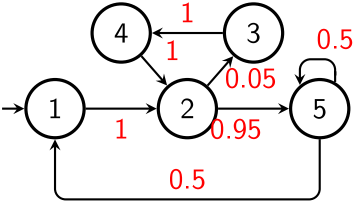
Theorem [1]

- A state is **not visited** or **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

Markov Decision Processes

Markov Decision Processes (MDP)

- Extends DTMC with non-determinism.
- For a given state, there is a choice of probability distribution we may use to proceed to the next state (non-deterministic choice of action, every action represents one probability distribution over the successors).

Model Checking MDPs

- Satisfaction of a property ranges between **Pmin** and **Pmax** depending on the resolution of the non-determinism.
- By resolving the non-determinism in MDP we get DTMC.
- `PRISM` – Probabilistic model checker

Other DTMC, MDP Extensions

- Rewards
- Partial observability