

# Modeling and Verification of Probabilistic Systems

Joost-Pieter Katoen

Lehrstuhl für Informatik 2  
Software Modeling and Verification Group

<http://moves.rwth-aachen.de/teaching/ss-14/movep14/>

April 24, 2014

## Recapitulating reachability probabilities

### Problem statement

Let  $\mathcal{D}$  be a DTMC with finite state space  $S$ ,  $s \in S$  and  $G \subseteq S$ .

Aim: determine  $Pr(s \models \diamond G) = Pr_s\{\pi \in Paths(s) \mid \pi \models \diamond G\}$

where  $Pr_s$  is the probability measure in  $\mathcal{D}$  with single initial state  $s$ .

### Approach

1. Determine by a graph analysis  $S_{=0} = \{s \in S \mid Pr(s \models \diamond G) = 0\}$  and  $S_{=1} = \{s \in S \mid Pr(s \models \diamond G) = 1\}$
2. Introduce a variable  $x_s$  for any state  $s \in S_T = S \setminus (S_{=0} \cup S_{=1})$
3. Solve a linear equation system  $\mathbf{x} = \mathbf{A} \cdot \mathbf{x} + \mathbf{b}$
4. . . . . using one of your favourite techniques, e.g., iterative methods
5. Intermediate results  $\mathbf{x}^{(i)}$  represent the vector  $(Pr(s \models \diamond^{\leq i} G))_{s \in S_T}$
6. Alternative: reduce reachability probabilities to transient distribution.

## Overview

- 1 Reachability probabilities
- 2 What are qualitative properties?
- 3 Fairness theorem
- 4 Determining almost sure properties
  - Preliminaries
  - Long run theorem
  - Reachability, repeated reachability and persistence
  - Quantitative repeated reachability and persistence
- 5 Summary

## Overview

- 1 Reachability probabilities
- 2 What are qualitative properties?
- 3 Fairness theorem
- 4 Determining almost sure properties
  - Preliminaries
  - Long run theorem
  - Reachability, repeated reachability and persistence
  - Quantitative repeated reachability and persistence
- 5 Summary

## Qualitative properties

### Quantitative properties

Comparing the probability of an event such as  $\Box G$ ,  $\Diamond\Box G$  and  $\Box\Diamond G$  with a threshold  $\sim p$  with  $p \in (0, 1)$  and  $\sim$  a binary comparison operator ( $=, <, \leq, \geq, >$ ) yields a **quantitative property**.

### Example quantitative properties

$$Pr(s \models \Diamond\Box G) > \frac{1}{2} \quad \text{or} \quad Pr(s \models \Diamond^{\leq n} G) \leq \frac{\pi}{5}$$

### Qualitative properties

Comparing the probability of an event such as  $\Box G$ ,  $\Diamond\Box G$  and  $\Box\Diamond G$  with a threshold  $> 0$  or  $= 1$  yields a **qualitative property**. Any event  $E$  with  $Pr(E) = 1$  is called **almost surely**.

### Example qualitative properties

$$Pr(s \models \Diamond\Box G) > 0 \quad \text{or} \quad Pr(s \models \Diamond^{\leq n} G) = 1$$

## Overview

- 1 Reachability probabilities
- 2 What are qualitative properties?
- 3 **Fairness theorem**
- 4 Determining almost sure properties
  - Preliminaries
  - Long run theorem
  - Reachability, repeated reachability and persistence
  - Quantitative repeated reachability and persistence
- 5 Summary

## Aim of today's lecture

### Take-home message

For **finite** DTMCs, qualitative properties do only depend on their state graph and **not** on the transition probabilities! For infinite DTMCs, this does not hold.

### Remark

In the following we will concentrate on **almost sure** events, i.e., events  $E$  with  $Pr(E) = 1$ . This suffices, as  $Pr(E) > 0$  if and only if not  $Pr(\bar{E}) = 1$ .

## Fairness

### Fairness theorem

Let  $\mathcal{D}$  be a (possibly infinite) DTMC and  $s, t$  states in  $\mathcal{D}$ . Then:

$$Pr(s \models \Box\Diamond t) = Pr(s \models \bigwedge_{u \in Post^*(t)} \Box\Diamond u).$$

When infinite branching, this is an infinitary conjunction (countable intersection).

In particular, if  $t$  is visited infinitely often almost surely, then this property carries over to any successor  $u$  of  $t$ .

### Corollary

For any state  $s$  in a (possibly infinite) DTMC we have:

$$Pr(s \models \bigwedge_{t \in S} \bigwedge_{u \in Post^*(t)} (\Box\Diamond t \Rightarrow \Box\Diamond u)) = 1.$$

## Proof (1)

### Fairness theorem

Let  $\mathcal{D}$  be a (possibly infinite) DTMC and  $s, t$  states in  $\mathcal{D}$ . Then:

$$Pr(s \models \Box \Diamond t) = Pr(s \models \bigwedge_{u \in Post^*(t)} \Box \Diamond u).$$

This result follows directly from the following claim that we will prove below.

### Claim

The probability to infinitely often visit state  $t$  equals the probability to take any finite path  $\hat{\pi}$  emanating from state  $t$  infinitely often.

## Proof (3)

## Proof (2)

### Claim

Let  $\mathcal{D}$  be a (possibly infinite) DTMC and  $s, t$  states in  $\mathcal{D}$ . Then:

$$Pr(s \models \Box \Diamond t) = Pr_s \left( \bigwedge_{\hat{\pi} \in Paths^*(t)} \Box \Diamond \hat{\pi} \right)$$

where  $\Box \Diamond \hat{\pi}$  denotes the set of paths  $\pi$  such that  $\hat{\pi}$  occurs infinitely in  $\pi$ .

### Proof:

This claim is proven in three steps:

1. For any  $\hat{\pi} \in Paths^*(t)$ , it holds  $Pr(s \models \Box \Diamond t \wedge \Box \neg \hat{\pi}) = 0$ .
2. For any  $\hat{\pi} \in Paths^*(t)$ , it holds  $Pr(\Box \Diamond t \wedge \Diamond \Box \neg \hat{\pi}) = 0$ .
3.  $Pr(\Box \Diamond t \wedge \bigwedge_{\hat{\pi} \in Paths^*(t)} \Diamond \Box \neg \hat{\pi}) = 0$ .

## Overview

- 1 Reachability probabilities
- 2 What are qualitative properties?
- 3 Fairness theorem
- 4 Determining almost sure properties
  - Preliminaries
  - Long run theorem
  - Reachability, repeated reachability and persistence
  - Quantitative repeated reachability and persistence
- 5 Summary

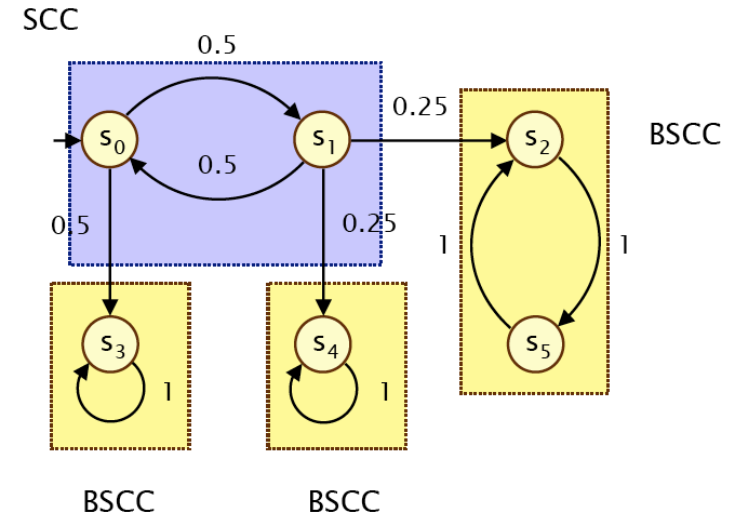
# Graph notions

Let  $\mathcal{D} = (S, \mathbf{P}, l_{init}, AP, L)$  be a (possibly infinite) DTMC.

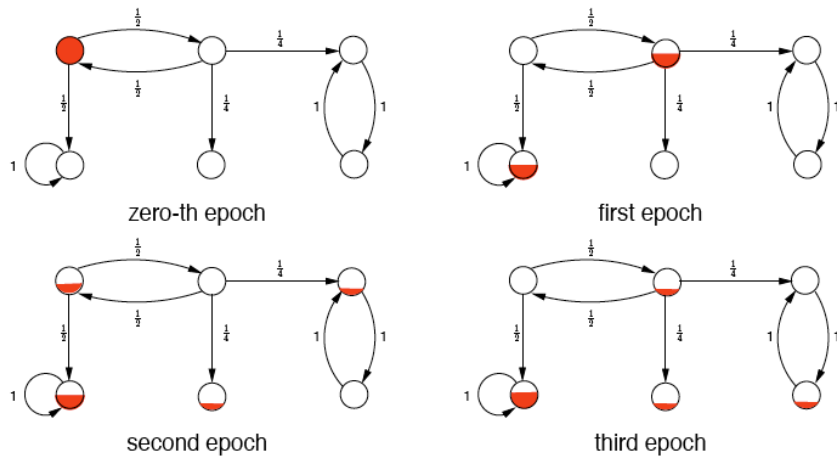
## Strongly connected component

- ▶  $T \subseteq S$  is *strongly connected* if for any  $s, t \in T$ , states  $s$  and  $t \in T$  are mutually reachable via edges in  $T$ .
- ▶  $T$  is a *strongly connected component* (SCC) of  $\mathcal{D}$  if it is strongly connected and no proper superset of  $T$  is strongly connected.
- ▶ SCC  $T$  is a *bottom SCC* (BSCC) if no state outside  $T$  is reachable from  $T$ , i.e., for any state  $s \in T$ ,  $\mathbf{P}(s, T) = \sum_{t \in T} \mathbf{P}(s, t) = 1$ .
- ▶ Let  $BSCC(\mathcal{D})$  denote the set of BSCCs of DTMC  $\mathcal{D}$ .

# Example

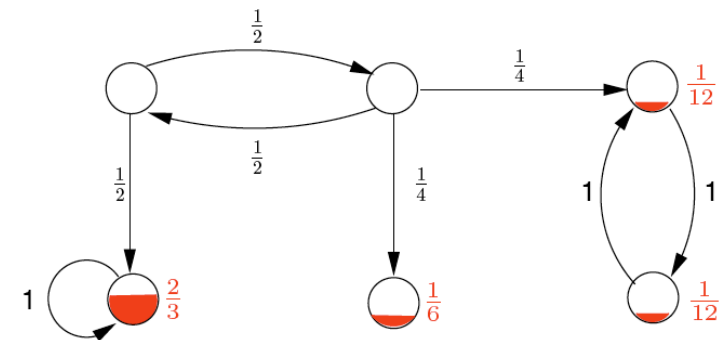


# Evolution of an example DTMC



Which states have a probability  $> 0$  when repeating this on the long run?

# On the long run



The probability mass on the long run is only left in BSCCs.

## Measurability

### Lemma

For any state  $s$  in (possibly infinite) DTMC  $\mathcal{D}$ :

$$\{\pi \in Paths(s) \mid \text{inf}(\pi) \in BSCC(\mathcal{D})\} \text{ is measurable}$$

where  $\text{inf}(\pi)$  is the set of states that are visited infinitely often along  $\pi$ .

### Proof:

1. For BSCC  $T$ ,  $\{\pi \in Paths(s) \mid \text{inf}(\pi) = T\}$  is measurable as:

$$\{\pi \in Paths(s) \mid \text{inf}(\pi) = T\} = \bigcap_{t \in T} \square \diamond t \cap \diamond \square T.$$

2. As  $BSCC(\mathcal{D})$  is countable, we have:

$$\{\pi \in Paths(s) \mid \text{inf}(\pi) \in BSCC(\mathcal{D})\} = \bigcup_{T \in BSCC(\mathcal{D})} \bigcap_{t \in T} \square \diamond t \wedge \diamond \square T.$$

## Fundamental result

### Long-run theorem

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

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

### Intuition

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

## Fundamental result

### Long-run theorem

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

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

### Proof:

- ▶ As  $\mathcal{D}$  is finite,  $\text{inf}(\pi)$  is strongly connected, i.e., part of SCC  $T$ , say.
- ▶ Hence,  $\sum_{SCC T} Pr_s\{\pi \in Paths(s) \mid \text{inf}(\pi) = T\} = 1$  (\*)
- ▶ Assume  $Pr_s\{\pi \in Paths(s) \mid \text{inf}(\pi) = T\} > 0$ .
- ▶ By the fairness theorem, almost all paths  $\pi$  with  $\text{inf}(\pi) = T$  fulfill

$$Post^*(T) = Post^*(\text{inf}(\pi)) \subseteq \text{inf}(\pi) = T.$$

- ▶ Hence,  $T = Post^*(T)$ , i.e.,  $T$  is a BSCC. The claim follows from (\*).

## Zeroconf example

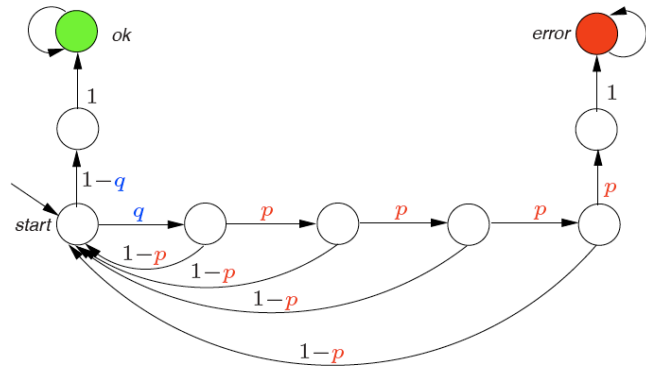
### Aim of the Zeroconf protocol

- ▶ IPv4 is aimed at plug-and-play networks for domestic appliances.
- ▶ New devices must get a unique IP address in an automated way.
- ▶ This is done by the IPv4 zeroconf protocol (proposed by IETF).

### Basic functioning of the Zeroconf protocol

1. Randomly select one of the 65,024 possible addresses.
2. Loop: as long as number of sent probes  $< n$ .
3. Broadcast probe "who is using my current address?"
4. Receive reply? Goto step 1.
5. Receive no reply within  $r > 0$  time units, then
  - 5.1 number of sent probes =  $n$ ? Exit, and use selected address.
  - 5.2 number of sent probes  $< n$ ? Goto step 2.

Let  $p$  be probability that no reply is received on a probe.

Zeroconf example ( $n=4$ )

$p$  = probability of message loss;  $q$  = probability of selecting occupied address

By the long-run theorem, the probability of acquiring an address infinitely often is zero.

## Computing almost sure reachability properties

## Aim:

For finite DTMC  $\mathcal{D}$  and  $G \subseteq S$ , determine  $\{s \in S \mid \Pr(s \models \diamond G) = 1\}$ .

## Algorithm

1. Make all states in  $G$  absorbing yielding  $\mathcal{D}[G]$ .
2. Determine  $S \setminus \text{Pre}^*(S \setminus \text{Pre}^*(G))$  by a graph analysis:
  - 2.1 do a backward search from  $G$  in  $\mathcal{D}[G]$  to determine  $\text{Pre}^*(G)$ .
  - 2.2 followed by a backward search from  $S \setminus \text{Pre}^*(G)$  in  $\mathcal{D}[G]$ .

This yields a time complexity which is linear in the size of the DTMC  $\mathcal{D}$ .

## Almost sure reachability

Recall: an absorbing state in a DTMC is a state with a self-loop with probability one.

## Almost sure reachability theorem

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

$$\Pr(s \models \diamond G) = 1 \quad \text{iff} \quad s \in S \setminus \text{Pre}^*(S \setminus \text{Pre}^*(G)).$$

Note:  $S \setminus \text{Pre}^*(S \setminus \text{Pre}^*(G))$  are states that cannot reach states from which  $G$  cannot be reached.

## Proof:

Show that both sides of the equivalence are equivalent to  $\text{Post}^*(t) \cap G \neq \emptyset$  for each state  $t \in \text{Post}^*(s)$ . Rather straightforward.

## Repeated reachability

## Almost sure repeated reachability theorem

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

$$\Pr(s \models \square \diamond G) = 1 \quad \text{iff} \quad \text{for each BSCC } T \subseteq \text{Post}^*(s). T \cap G \neq \emptyset.$$

## Proof:

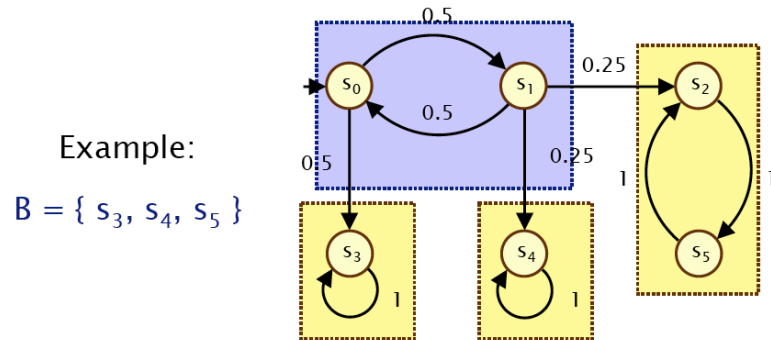
Immediate consequence of the long-run theorem.

## Almost sure repeated reachability

### Almost sure repeated reachability theorem

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

$$Pr(s \models \Box \Diamond G) = 1 \text{ iff for each BSCC } T \subseteq Post^*(s). T \cap G \neq \emptyset.$$

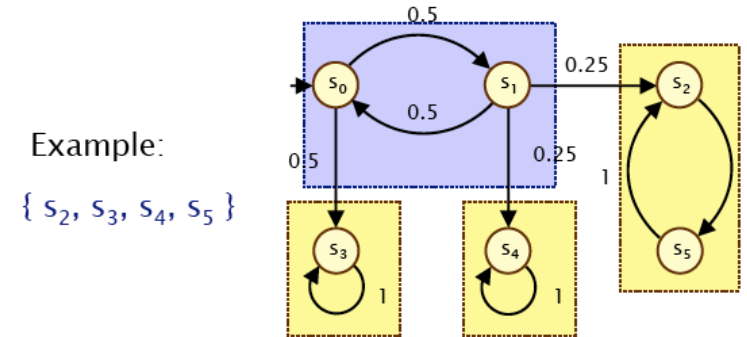


## Almost sure persistence

### Almost sure persistence theorem

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

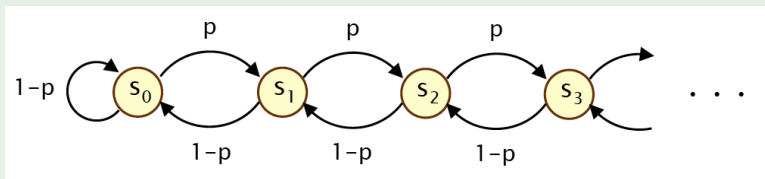
$$Pr(s \models \Diamond \Box G) = 1 \text{ if and only if } T \subseteq G \text{ for any BSCC } T \subseteq Post^*(s)$$



## A remark on infinite Markov chains

### Graph analysis for infinite DTMCs does not suffice!

Consider the following infinitely countable DTMC, known as *random walk*:



The value of rational probability  $p$  **does** affect qualitative properties:

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

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

## Quantitative properties

### Quantitative repeated reachability theorem

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

$$Pr(s \models \Box \Diamond G) = Pr(s \models \Diamond U)$$

where  $U$  is the union of all BSCCs  $T$  with  $T \cap G \neq \emptyset$ .

### Quantitative persistence theorem

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

$$Pr(s \models \Diamond \Box G) = Pr(s \models \Diamond U)$$

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

### Remark

Thus probabilities for  $\Box \Diamond G$  and  $\Diamond \Box G$  are reduced to *reachability probabilities*. These can be computed by solving a linear equation system.

## Example

## Summary

- ▶ Executions of a DTMC are strongly fair with respect to all probabilistic choices.
- ▶ A finite DTMC almost surely ends up in a BSCC on the long run.
- ▶ Almost sure reachability = double backward search.
- ▶ Almost sure  $\Box\Diamond G$  and  $\Diamond\Box G$  properties can be checked by BSCC analysis and reachability.
- ▶ Probabilities for  $\Box\Diamond G$  and  $\Diamond\Box G$  reduce to reachability probabilities.

### Take-home message

For **finite** DTMCs, qualitative properties do only depend on their state graph and **not** on the transition probabilities! For infinite DTMCs, this does not hold.

## Overview

- 1 Reachability probabilities
- 2 What are qualitative properties?
- 3 Fairness theorem
- 4 Determining almost sure properties
  - Preliminaries
  - Long run theorem
  - Reachability, repeated reachability and persistence
  - Quantitative repeated reachability and persistence
- 5 Summary

## Outlook

- ▶  $\Diamond\Box G$  and  $\Box\Diamond G$  are  $\omega$ -regular.
- ▶ Their likelihood can be reduced to reachability probabilities.
- ▶ How about arbitrary  $\omega$ -regular properties?
- ▶ Such as  $(\Diamond\Box F \wedge \Box\Diamond G)$  or  $\bar{F}U(\Diamond\Box G) \dots$
- ▶ Can they also be reduced to reachability probabilities? **Yes**, they can!