Dependable Systems 191.109 – Lab

Wilfried Steiner

2025-03-05

Outline

Lab Overview

- In the practical part of this course we analyse Markov Chains.
- You can do the lab on your own or in teams of two or three.
- We will do so by using a tool called *prism*.
- The tool is available from: `http://www.prismmodelchecker.org/`
- The results shall be documented in a lab report (i.e. a paper with sufficient details).
- Please send the report to: *wilfried.steiner@tuwien.ac.at*
- The lab report shall be presented by all members (!) of the group.
- Lab report will be discussed as part of the exam.

Getting Started

- *prism* is available from: `http://www.prismmodelchecker.org/`
- Download prism and install it on your computer.
- Execute the die example:
  `http://www.prismmodelchecker.org/tutorial/die.php`
- The manual contains valuable examples as well:
  `http://www.prismmodelchecker.org/manual/`
  - Note: it's a bit tricky to navigate; left frame on the website

Simple Example 1 - Problem Description

Description

A simple storage system consists of a storage controller and the storage itself (e.g., a disk).

- failure rate of both (controller and disk) is 1/720

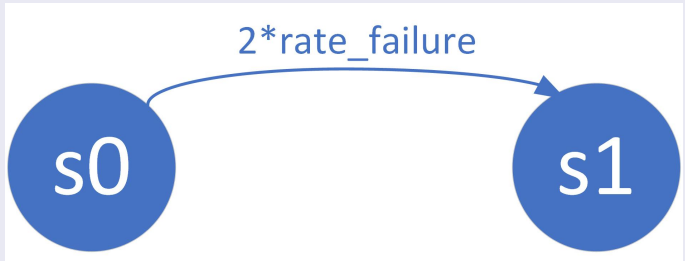
Storage System

Simple Example 1 - *prism* model

prism code

```
ctmc
//definition of the failure rate
const double rate_failure = 1/720;
module DISK
//definition of states
   s: [0..1] init 0;
//guard -> rate: action;
   [] s=0 -> rate_failure*2: (s'=1);
endmodule
//definiton of the reward system
rewards
  s=0: 1;
endrewards
```

Markov Model



Simple Example 1 - Properties

- Reliability: P=? [!(F[t1, t2] s=1)] (e.g. t1=0, t2=1000)
- MTTF: R=? [F (s=1)]
- Availability: S=? [(s=0)]
- Results:
  - Reliability: 0.0622
  - MTTF: 360 hours
  - Availability: ?

Simple Example 2 - Problem Description

Description

Same as Simple Example 1 plus maintenance.

- repair rate = 1/10

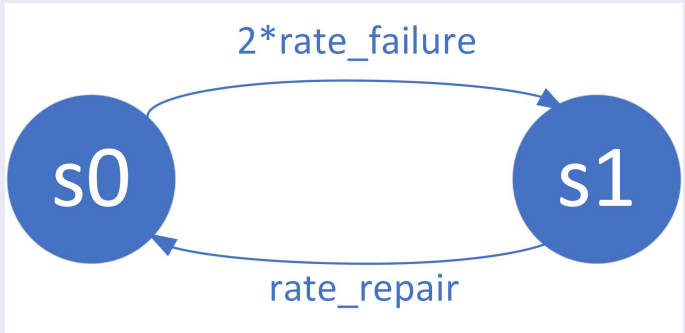
Storage System

Simple Example 2 - *prism* model

prism code

```
ctmc
//definition of the failure rate
const double rate_failure = 1/720;
const double rate_repair = 1/10;
module DISK
//definition of states
   s: [0..1] init 0;
//guard -> rate: action;
   [] s=0 -> rate_failure*2: (s'=1);
   [] s=1 -> rate_repair: (s'=0);
endmodule
//definiton of the reward system
rewards
  s=0: 1;
endrewards
```

Markov Model



Simple Example 2 - Properties

- Reliability: P=? [!(F[t1, t2] s=1)] (e.g. t1=0, t2=1000)
- MTTF: R=? [F (s=1)]
- Availability: S=? [(s=0)]
- Results:
  - Reliability: 0.0622
  - MTTF: 360 hours
  - Availability: 0.97297

prism options

- In the options menu many things can be configured under “options”.
- It may be necessary to change the default options as follows:
  - Linear equations method: set to Gauss-Seidel
  - Termination max. iterations: 1000000 (or even higher)

Excercise 1 - Warmup

- Download *prism* and install it on your computer.
- Realy execute the die example:
  `http://www.prismmodelchecker.org/tutorial/die.php`
- Get familiar with prism.
- Shall not be included in the lab report.

Exercise 2a - Fault-Tolerant Computer System

- A fault-tolerant computer system consist of two main CPUs.
- The fault-tolerant computer system tolerates the failure of any one of the main CPUs. I.e., as long as only one main CPU fails, the system remains operational.
- Failure rate = 1/1000; Repair rate = 1/10
- Tasks
  - Use *prism* to calculate reliability values for the system and generate a plot of the reliability.
  - Use *prism* to calculate the MTTF and the availability of the system.
  - Document the exercise, the model, the properties, and the verification results in the lab report.
- Hint: see part three of the course, slide 40.

Exercise 2b - Fault-Tolerant Computer System

- A fault-tolerant computer system consist of two main CPUs.
- The fault-tolerant computer system tolerates the failure of any one of the main CPUs. I.e., as long as only one main CPU fails, the system remains operational.
- Failure rate = 100 FIT; Repair rate = none;
- Assumption Coverage = 0.7
- Tasks
  - Use *prism* to calculate reliability values for the system and generate a plot of the reliability.
  - Use *prism* to calculate the MTTF and the availability of the system.
  - Document the exercise, the model, the properties, and the verification results in the lab report.
- Hint: see part three of the course, slide 43.

Exercise 3 - Your turn!

- Define a fault-tolerant system of your choice, with the following constraints.
  - The Markov Chain shall consist of at least five states.
  - Maintenance shall be possible, i.e., defined repair rate/s.
  - Assumption coverage *may* be considered.
  - Safety *may* be consider (e.g., see slides part 3, slide 45)
- Tasks
  - Use *prism* to calculate reliability values for the system and generate a plot of the reliability.
  - Use *prism* to calculate the MTTF and the availability of the system.
  - Document the exercise, the model, the properties, and the verification results in the lab report.
- Be creative!
  - Don't just use the system from slide 45 in part 3 of the course.