Exam Model Checking

Marielle Stoelinga and Nils Jansen
Radboud University
18.06.2019, 08:30–11:30

Remarks.

- *As additional material, you are allowed **one** A4 sheet with your notes and nothing else.*
- *Write your name on each separate page that you hand in.*
- *Hand in the exam sheets as well, Question 1 consists of multiple choice questions you need to answer **on the exam sheet**. In the appendix, you may find helpful definitions.*
- *Please provide answers in English.*
- *You can earn 32+15+15+25+15+23=125 points, with a total of 5 questions. Good luck!*

1. **Multiple choice questions.** For each question below, **circle** all statements that are **true**. Note that several (or zero) statements may be true for one question. All statements without a circle are marked as false. You get 2 point per correctly answered question. A question is answered correctly if exactly all true statements are circled.

   (a) (6 points) **Cut sets.**

   1. If C_1 and C_2 are minimal cut sets of a static fault tree, then $C_1 \cup C_2$.
      (a) Is always a cut set
      (b) Can be a minimal cut set
      (c) Is never a minimal cut set
   2. Suppose we add the XOR-gate to fault trees. What will change?
      (a) Cut sets do not exist any more
      (b) Cut set and minimal cut set cannot be computed via BDDs any more
      (c) Probabilities cannot be computed via the bottom up method any more
   3. Does there exist a static fault tree with no cut set at all?
      (a) Yes, such a fault tree exists
      (b) No, such a fault tree does not exist

(b) (6 points) **Failure probabilities.**

4. Suppose we replace in a static fault tree an OR gate by an AND-Gate. What happens to to the failure probabilities. The probability for the top level event
   (a) Always increases or stays the same
   (b) Always decreases or stays the same
   (c) Can increase, decrease or stay the same
   (d) Can never stay the same
5. Consider an AND gate C that has two children A and B. The failure times of A and B are both given by an exponential distribution with parameter λ. The probability that the AND gate fails with time T is given by
   (a) An exponential distribution with parameter 2λ.
   (b) An exponential distribution with parameter $\lambda/2$.
6. Consider an OR gate C that has two children A and B. The failure times of A and B are both given by an exponential distribution with parameter λ. The probability that the OR gate fails with time T is given by
   (a) An exponential distribution with parameter 2λ.
   (b) An exponential distribution with parameter $\lambda/2$.

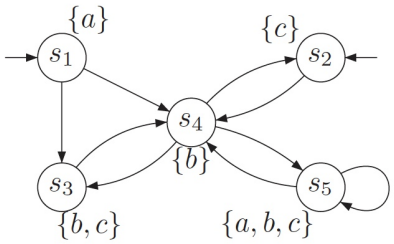
(c) (6 points) **Exponential distributions.**

7. Consider a random variable modeling a component failure time (measured in weeks) and that is exponentially distributed with expected value $\frac{1}{1}0$. What is the probability that the component fails within the first two weeks?
   (a) $e^{-0.2}$
   (b) e^{-5}
   (c) $1 - e^{-0.2}$
   (d) $1 - e^{-5}$
8. Which of the following statements are true for exponentially distributed random variable X? Pick all answers that are correct.
   (a) $P[X > 20|X > 15] = P[X > 5]$
   (b) $P[X > 20|X > 15] = P[X > 20]$
   (c) $P[X > 20|X = 15] = P[X = 15]$
   (d) $P[X < 20|X > 15] = P[X < 5]$
   (e) $P[X < 20|X > 15] = P[15 < X < 20]$

9. Consider a random variable X that is exponentially distributed and $P[X > 10] = 0.5$. What is $P[X > 20]$?
   (a) 0.25
   (b) 0.5
   (c) $e^{0.5}$
   (d) $e^{-0.5}$
   (e) $1 - e^{0.5 \cdot 10}$
   (f) $1 - e^{-0.5 \cdot 10}$

(d) (4 points) **CTL and LTL.**

10. Which formulae hold for state s_4 in the picture below?
    (a) $\Diamond\Box c$
    (b) $\Box\Diamond c$
    (c) $\bigcirc\neg c \rightarrow \bigcirc\bigcirc c$
    (d) $a \; U \; \Box(b \vee c)$
    (e) $(\bigcirc\bigcirc b) \; U \; (b \vee c)$.

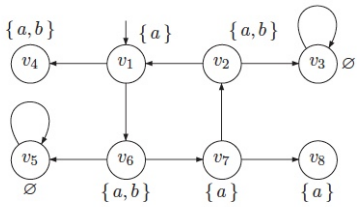


11. Which statement is true:
    (a) CTL is more expressive than LTL
    (b) LTL is more expressive than CTL
    (c) LTL and CTL have the same expressivity

(e) (6 points) **Bisimulation.**

12. Which statement is true?
    (a) Two states are bisimilar if and only if the satisfy exactly the same CTL formulae
    (b) Two states are bisimilar if and only if the satisfy exactly the same LTL formulae
    (c) Two states are trace equivalent if and only if the satisfy exactly the same CTL formulae
    (d) Two states are trace equivalent if and only if the satisfy exactly the same LTL formulae

13. Which states in the figure below are bisimilar?
    (a) v_1 and v_7
    (b) v_2 and v_6
    (c) v_3 and v_5



14. Which statement is true:
    (a) The intersection of two bisimulation relations is a bisimulation relation (i.e., if R and R' are bisimulation relations, then so is $R \cup R'$.)
    (b) The intersection of two bisimulation relations is need not be a bisimulation relation

(f) (4 points) **Probabilistic model checking.**

15. Consider a DTMC M. We create new DTMC M' by dividing all probabilities in M by 2, and by adding a self loop $s \xrightarrow{p} s$ to make sure that the probabilities in M sum up to 1 again. That is, $p = 1 - \sum_{p' \mid s \xrightarrow{p'} s', s \neq s'} p'$.
    Which of the following statements are true:
    (a) $M, s \models P_{=1}[\Diamond a] \implies M', s \models P_{=1}[\Diamond a]$
    (b) $M, s \models P_{>0.7}[\Diamond a] \implies M', s \models P_{>0.7}[\Diamond a]$
16. Given an MDP $\mathcal{M}$ with state space S and a reachability property $\Diamond a$. Recall that $p_{\max}(s, \Diamond a)$ denotes the maximal probability to reach states labelled with a from s under all possible schedulers.
    (a) There exists always a *memoryless scheduler* $\sigma^{\max}$ which yields $p_{\max}(s, \Diamond a)$ for all states $s \in S$.
    (b) The probability $p_{\max}(s, \Diamond a)$ can be computed using a mere linear equation system.

End of the multiple choice questions!

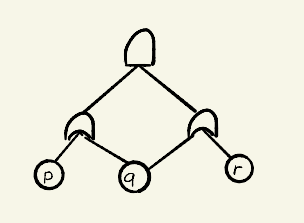
2. **LTL and Büchi automata.**

   (a) (7 points) Assume that $x \in V$ is a program variable. Give an LTL formula φ for the following property: "Initially the value of variable x is 1, and it then it cycles between 1, 2 and 3."

   (b) (8 points) Construct a Büchi automaton over the set of state properties $\{x = 1, x = 2, x = 3\}$ which accepts exactly those state sequences that satisfy φ.

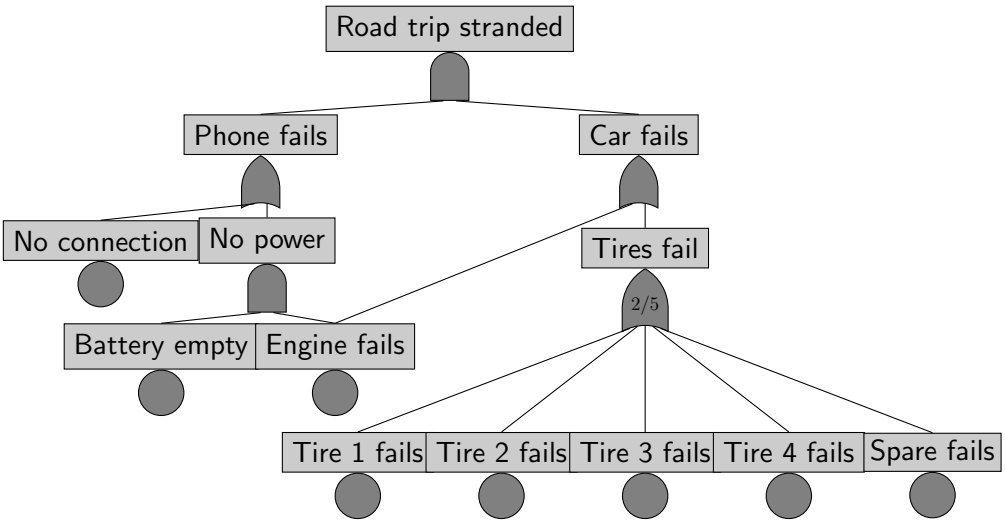
3. **Fault tree analysis**

(a) (10 points) Compute the probability that the top level event fails in the fault tree below. Explain your computation.



(b) (5 points) We consider the road trip fault tree again and assume that all BEs have the same failure rates, see fault tree below. Suppose that you want to increase the reliability of your road trip. Which BEs would you improve (i.e., you make them more reliable). Choose at most two. Explain your answer.

1. The connection
2. The battery
3. The engine
4. Tire 1
5. The spare tire



4. **Probabilistic model checking.**

   (a) (10 points) Prove the correctness of the following statement or give a counterexample. We are given an MDP $M = (S, s_I, Act, P)$ and two PCTL properties $\varphi_1 = \mathbb{P}_{\leq 0.5}(\Diamond T)$ and $\varphi_2 = \mathbb{P}_{\leq 0.5}(\Diamond G)$ with $T, G \subseteq S$ and $T \cap G = \emptyset$. If $M \models \varphi_1$ and $M \models \varphi_2$, that is, both properties hold for **all** schedulers for the MDP, then there exists a memoryless **deterministic** scheduler σ such that $M^\sigma \models \varphi_1$ and $M^\sigma \models \varphi_2$. Recall that M^σ denotes the DTMC induced by the MDP M and the scheduler σ.

   (b) (5 points) Now consider the following PRISM program.

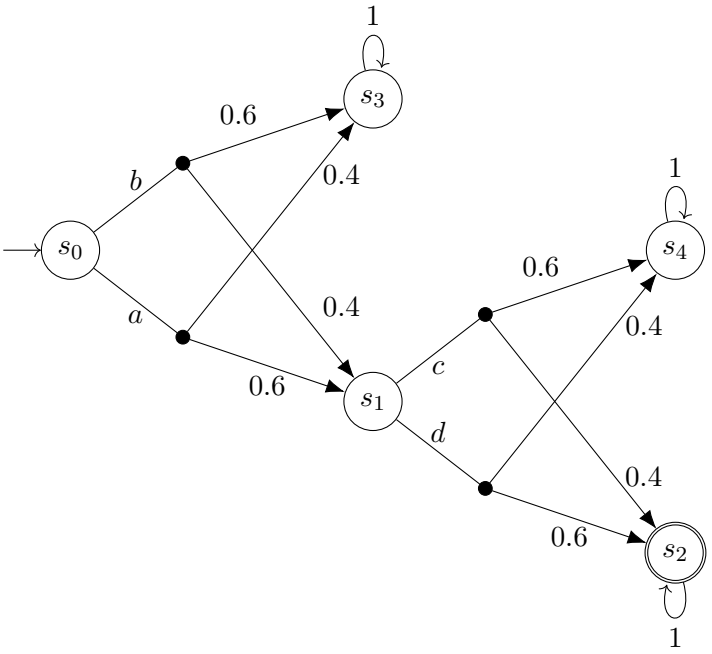
```
mdp

module M1
x : [0..7] init 0;

    [a] x=0 -> 0.8:(x'=2) + 0.2:(x'=1);
    [b] x=0 -> 1.0:(x'=3);
    [a] x=1 | x=4 -> 0.6:(x'=6) + 0.4:(x'=7);
    [b] x=1 | x=2 | x=4 | x=5 -> 1:(x'=7);
    [a] x=2 | x=5 -> 0.25:(x'=6) + 0.75:(x'=7);
    [a] x=3 -> 0.2:(x'=4) + 0.8:(x'=5);
    [b] x=3 -> 1.0:(x'=3);
    []  x=6 -> 1.0:(x'=6);
    []  x=7 -> 1.0:(x'=7);
endmodule
```

   Construct and draw the MDP induced by the PRISM program.

   (c) (10 points) Determine the probabilities $Pr_{\max}(\Diamond \texttt{x=6})$ and $Pr_{\min}(\Diamond \texttt{x=6})$ for the initial state of the MDP (from the previous part) with `x=0`. Note that `x=6` corresponds to the state of the MDP where the variable x has the value 6. Explain how you obtained these probabilities.

5. **Permissive schedulers.** Recall the notion of a permissive scheduler from the lecture. In particular, a *maximally permissive* scheduler allows as many actions at each state as possible to satisfy a specification.

   (a) (10 points) Give a **permissive deterministic memoryless** scheduler for the MDP below such that the specification $\mathbb{P}_{\leq 0.3}(\Diamond s_2)$ is satisfied for the initial state s_0. The scheduler should allow as many actions as possible.

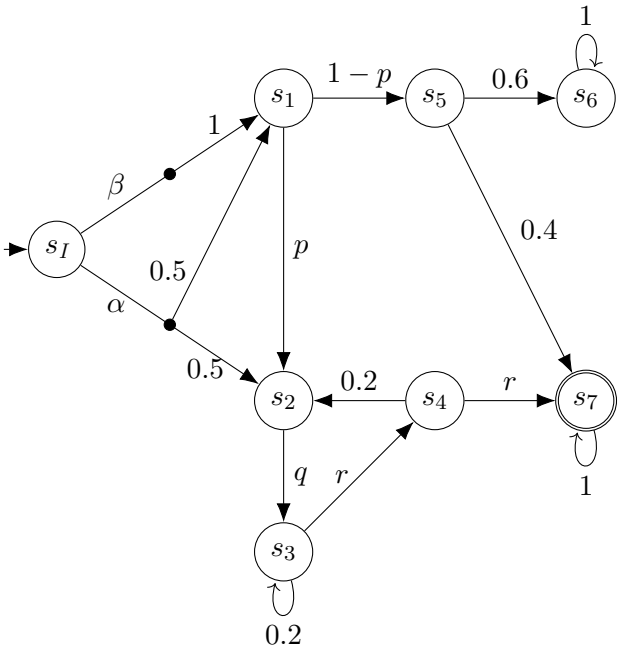


   (b) (5 points) **Discuss** how a **maximally permissive scheduler** could be constructed for this MDP.

6. **Parametric systems.** Consider the parametric discrete-time Markov decision process (pMDP) as depicted below. See the appendix for a definition of pMDPs.

   Note that this pMDP has only one nondeterministic choice at state s_I between actions α and β. This choice induces two different probability distributions of either a uniform distribution between states s_1 and s_2 (α), or reaching state s_1 with probability one (β), respectively.

   At all other states, there is no nondeterministic choice, so in fact the transition probability function is of the form $P\colon S \times S \to \mathbb{Q}_V$ at all states except s_I.



   We are interested in the probability of finally reaching the state s_7 from the initial state s_I, denoted by $Pr^M_{s_I}(\Diamond s_7)$.

   (a) (4 points) List **all** memoryless deterministic schedulers for the pMDP above and depict the induced parametric discrete-time Markov chains (pDTMCs) for these schedulers.

   (b) (13 points) Pick **one** of the schedulers and the induced pDTMC you listed in a). For the pDTMC, compute a rational function representing $Pr^M_{s_I}(\Diamond s_7)$ using the state elimination algorithm and explain each step. Possible intermediate simplifications are allowed if sufficiently explained.

   (c) (6 points) Recall the linear program to compute **maximal** reachability probabilities for (non-parametric) MDPs, see also the appendix.

   Adapt this linear program such that maximal reachability probabilities for pMDPs are computed.

   Hint: The program actually becomes **nonlinear**, as multiple variables have to be multiplied with each other.

Appendix

Linear program for MDP reachability probabilities

Given an MDP $M = (S, s_I, Act, P)$ where $P\colon S \to 2^{Act \times Distr(S)}$. Maximum probabilities $p_{\max}(s, \Diamond a)$ to reach states that are labelled with a can be computed using linear programming as follows:

- $p_{\max}(s, \Diamond a) = 1$ if $s \in Sat(a)$
- $p_{\max}(s, \Diamond a) = 0$ if $s \in S^{\max=0}$
- values for the remaining states in the set $S^? = S \setminus (Sat(a) \cup S^{\max=0})$ can be obtained as the unique solution of the following *linear programming problem*:

  minimize $\sum_{s \in S^?} x_s$
  such that

  $$x_s \geq \sum_{s' \in S^?} \mu(s') \cdot x_{s'} + \sum_{s' \in Sat(a)} \mu(s')$$

  for all $s \in S^?$ and for all $(\alpha, \mu) \in P(s)$.

Parametric MDP

A pMDP is given by a tuple $M = (S, s_I, V, Act, P)$, where S is a finite set of states, $s_I \in S$ is the unique initial state, V is a finite set of parameters, Act is a finite set of actions, and P is a transition probability function of the form $P\colon S \times Act \times S \to \mathbb{Q}_V$ where $\mathbb{Q}_V$ is the set of rational functions (fractions of polynomials) over V.

Exponential distributions

For an exponentially distributed random variable X, we have that $P[X < t] = 1 - e^{-\lambda t}$ (CDF) and $E[X] = 1/\lambda$.