Technische Universität München (I7)
Javier Esparza

Summer 2015

Model Checking – Endterm

Last name: ______________________________

First name: ______________________________

Student ID no.: ______________________________

Signature: ______________________________

- If you feel ill, let us know immediately.
- You have **100 minutes** to fill in all the required information and write down your solutions.
- Don't forget to **sign**.
- Write with a non-erasable **pen**, do not use red or green color.
- You are not allowed to use **auxiliary means**.
- You may answer in **English or German**.
- Please turn off your **cell phone**.
- Should you require additional **scrap paper**, please tell us.
- You can obtain **40 points** in the exam. You need **17 points** in total to pass (grade 4.0).
- Don't fill in the table below.
- Good luck!

Ex1	Ex2	Ex3	Ex4	Ex5	Ex6	$\sum$

Exercise 1 LTL 2+2+2+2=8P

Consider the following LTL formulas over the set of atomic propositions $AP = \{p, q\}$:

$$\varphi_1 = \mathbf{G}(\mathbf{F}p \rightarrow q) \qquad \varphi_2 = \mathbf{G}(q\,\mathcal{U}\,p) \qquad \varphi_3 = \mathbf{G}(\mathbf{F}p \vee (\neg q\,\mathcal{U}\,\neg p))$$

(a) Is there a word satisfying φ_1 but not φ_2 ?
If so, exhibit such a word and briefly explain why it does; else, justify briefly why it does not exist.

(b) Is there a word satisfying φ_2 but not φ_1 ?
If so, exhibit such a word and briefly explain why it does; else, justify briefly why it does not exist.

(c) Is there a word satisfying all three formulas ?
If so, exhibit such a word and briefly explain why it does; else, justify briefly why it does not exist.

(d) Give a Büchi automaton accepting exactly the words satisfying φ_2.

Exercise 2 Spin 2+2+2= 6P

Consider the following Promela model:

```
1  byte g = 0;
2  chan c = [0] of { byte };
3
4  active proctype x() {
5    c!1;
6    do
7    :: c?0 -> g--; label1: c!1;
8    od
9  }
10
11 active proctype y() {
12   do
13   :: c?1 -> g++; c!0;
14   :: c?2 -> label2: g++;
15   od
16 }
17
18 ltl p1 { [] (x@label1 -> <> (g == 1)) }
19 ltl p2 { []<> (g == 0) }
```

Recall that `x@label1` (line 18) is `true` only in the states where the process `x` is at `label1`.

(a) Does the LTL formula `p1` at line 18 hold? Justify your answer.

(b) Write a process named `z` such that every execution of the code consisting of the processes `x,y,z` executes the statement at `label2` in line 14 *exactly* once. Use the following template:

```
active proctype z() { * Here comes your code * }
```

(c) Does the LTL formula `p2` at line 19 hold after the process `z` is added? Justify your answer.

Exercise 3 LTL to Büchi translation 2+3+3= 8P

Consider the LTL formula ϕ over the set of atomic propositions $AP = \{p, q, r\}$ (each state is marked with the atomic propositions it satisfies):

$$\phi = [(p\,\mathcal{U}\,q) \rightarrow (r\,\mathcal{R}\,q)]\;\mathcal{U}\;(\mathbf{X}(p \wedge q \wedge r))$$

(a) Put $\neg\phi$ in negation normal form (NNF), i.e., give a formula ψ in NNF equivalent to $\neg\phi$.
OBSERVE: you have to put $\neg\phi$ in NNF, not ϕ!

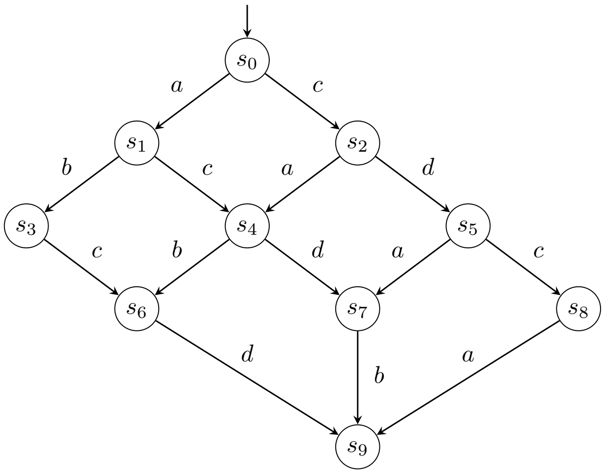
(b) Give a smallest consistent state of the automaton containing the following subformulas:

$$\psi,\ \mathbf{X}(\neg p \vee \neg q \vee \neg r),\ p,\ q,\ \neg r$$

(c) Give the target state and the label of a transition of the automaton having the state of (b) as source.

Exercise 4 Partial Order Reduction **2+3=5P**

Consider a labelled Kripke structure $\mathcal{K} = (S, A, \rightarrow, r, AP, \nu)$ where S, A, $\rightarrow$, and r are graphically represented as follows:

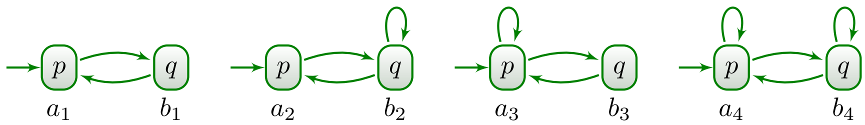


(a) Give all pairs of actions that violate the diamond condition of independence relations. Justify your answer.

(b) Assume that only the actions a and b are visible. Recall that $red(s)$ denotes the set of actions a for which there is a transition $s \xrightarrow{a} s'$ after the reduction. Can we have $red(s_7) = \emptyset$ and satisfy conditions C_0-C_3 ? And $red(s_1) = \{c\}$? And $red(s_0) = \{c\}$? Justify your answers.

Exercise 5 CTL **2+4= 6P**

Consider the following Kripke structure over the set of atomic propositions $AP = \{p, q\}$:



(a) Give the set of states satisfying the CTL formulas:

$$\psi_1 = A\mathbf{G}E\mathbf{F}p \qquad \psi_2 = A\mathbf{F}E\mathbf{G}p$$

(b) Apply the fixpoint algorithm of the lecture to compute the set of states satisfying $A\mathbf{F}E\mathbf{X}E\mathbf{G}p$. Describe briefly the intermediate steps.

Exercise 6 BDDs **3+4= 7P**

(a) Exhibit a BDD with 4 variables and 11 states (including the 0 state).

(b) Prove that no BDD for a boolean function of arity 4 can have more than 11 states.