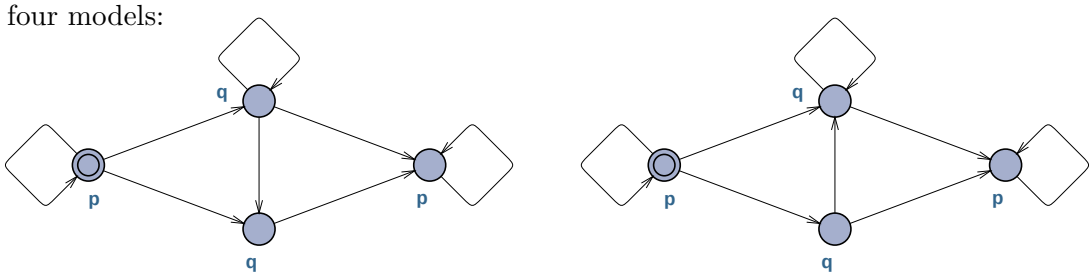
University of Innsbruck — Institute of Computer Science
Verification using Model Checking — Final Exam — 1st opportunity — 5.7.2007

Name: **Matr.nr.:**

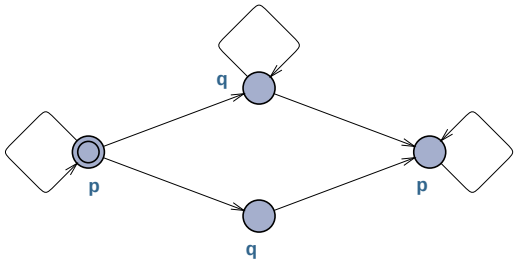
This exam consists of five exercises. Please motivate your answers unless mentioned otherwise. The number of points per question is indicated in the left margin. The exam is passed if you get 30 out of 60 points or more.

Exercise 1 (Models)
Given four models:

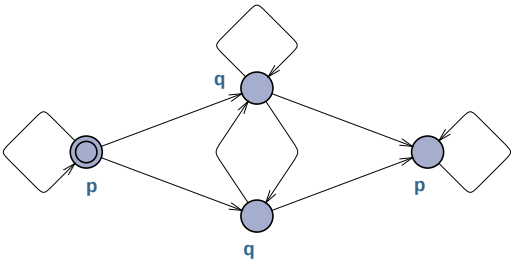


M_1

M_2



M_3



M_4

a. Prove that for all LTL formulas ϕ: $M_1 \models \phi$ if an only if $M_2 \models \phi$ or give a counter example. [4]

b. Prove that for all CTL formulas ϕ: $M_1 \models \phi$ if an only if $M_3 \models \phi$ or give a counter example. [4]

c. Prove that for all CTL formulas ϕ: $M_2 \models \phi$ if an only if $M_4 \models \phi$ or give a counter example. [4]

Exercise 2 (process algebra)
Let

$$X = c? \cdot \tau \cdot c! \cdot \tau \cdot X \qquad Y = c? \cdot a? \cdot a? \cdot Y \qquad Z = a! \cdot c! \cdot a! \cdot Z$$

Prove that [8]

$$\partial_{\{a!,a?\}}(Y \parallel Z) = X$$

Exercise 3 (Büchi Automata)
If a description is ambiguous then explain the ambiguity briefly and solve the problem by selecting one of the possibilities.

a. Give a Büchi automaton over the alphabet $\{a, b, c\}$, which accepts the language of all infinite words in which there are never two consecutive a's. [4]

b. Give a Büchi automaton over the alphabet $\{a, b, c\}$, which accepts the language of all infinite words in which b's occur in pairs only. [4]

c. Give a Büchi automaton that corresponds to the LTL formula $(\neg(p \wedge r))\ \mathsf{U}\ (\mathsf{G}\, q)$. [4]
(Direct manual construction is recommended over the formal construction.)

Exercise 4
Consider a board game with two players: A and B. Each player can have a maximum of 7 runners on the board. The variables in the model are:

T_A	True if it is player A's turn.
$A_2A_1A_0$	3-bit binary number describing the number of runners of A.
$B_2B_1B_0$	3-bit binary number describing the number of runners of B.
$\vdots$	Many other variables are needed for the game, but not for this exercise.

Consider the properties:

a. It is not possible for either player to make infinitely many moves in one turn. [4]

b. At any time, players A and B can work together to to let player A score a point, where a player scores a point if (s)he has 6 or more runners on the board or the other player has no runners left. [8]

Give both LTL and/or CTL formulas for these properties or explain why LTL and/or CTL is not appropriate.

Exercise 5 (Uppaal)
Consider the following (timing based) mutual exclusion protocol. There are N processes that each have a critical section. To avoid that more than one process is in its critical section at the same time we have the following rules:

- We have a global array of booleans `request`.
- When process i wants to access its critical section it will:

  1. Set `request[i]` to true.
  2. If more than one element of `request` is true then
  3. set `request[i]` to false
  4. wait between 2 and 3 or between 5 and 6 seconds (non-deterministic)
  5. goto step 1.
  6. else
  7. enter critical section
  8. no later than 10 seconds later leave critical section
  9. set `request[i]` to false
  10. fi

- Processes may enter the critical section as many times as they wish.

a. Give an Uppaal style timed automaton for a single process and declare a system with $N = 2$ processes. [8]
Use common sense to fill in missing details and/or resolve ambiguities, if any.

b. Give an Uppaal query for: [3]
At most one process is in its critical section.

c. Does the query hold in your model? (answer suffices) [1]

d. Give an Uppaal query for: [3]
Whenever process 1 wants to enter its critical section, it will eventually do so.

e. Does the query hold in your model? (answer suffices) [1]