Tik-79.146 Logic in Computer Science: Special Topics I **Spring 2003**
Homework assignment 3
2.4.2003

Deadline 24.4.2003.

The home assignment can be returned at the lecture or to the box by the room TB336.

CTL Model Checking

This assignment consists of two parts. In the first part some temporal properties (of a mutual exclusion algorithm) are specified using CTL and in the second part a model of the algorithm is checked w.r.t. these properties.

Part One

Specify the following properties in CTL (introducing appropriate atomic formulae):

1. Any two processes (out of three) are never at the same time in the critical section.
2. When process 0 gets into the enter section, it will always eventually get to the critical section.
3. If process 0 gets into the leave_try section, then it stays there until it gets to the critical section.
4. The system can from all system states return to a state in which all processes are in the remainder section.
5. Process 1 cannot enter the critical section without visiting the enter state first.
6. If process 1 is in the enter section, it can move to the critical section in the next state.

Part Two

Check the properties (1-6) above for a model of a mutual exclusion algorithm using the `probe` CTL model checker (available in the `PROD` Pr/T net analyzer system). The model to be checked is the reachability graph of a Pr/T net description of the algorithm (seen as a possible world model). See instructions on the web page of the course (`http://www.tcs.hut.fi/Studies/T-79.146/`) how to create the model (reachability graph) and how to use the `probe` model checker. All the necessary software is available in the Computing Centre SUN workstations ("Gaulls").

Include in your answer paper the properties above specified in CTL and output of a session with `probe` checking all the properties in the initial state of the mutual exclusion algorithm (`Node 0`). (You can obtain the output, for example, by using the "script" -command.)

Did any of the properties have unexpected outcomes? Which ones did and why do you think they did?

The mutual exclusion algorithm

Here is some information on the Pr/T net model of the mutual exclusion algorithm for model checking, e.g., for the syntax of atomic formulae.

The modelled system is a three process mutual exclusion system using a ticket algorithm. The program counters of the processes are modelled by 3 tuples in the place `pc`. There is one tuple for each process and its of the form `<.pid, state.>` where $0 \leq$ `pid` ≤ 2 and `state` $\in$ {`rem, enter, test, leave_try, crit, reset, leave_exit`}. In model checking you can use atomic propositions of the form

$$(\texttt{pc} >=< .\texttt{P}, \texttt{S}. >)$$

where `P` is an integer and `S` is a state. For instance, `(pc >= <.2,crit.>)` is true in all states in which process 2 is in the critical section.