T-79.146 Logic in Computer Science: Special Topics I **Spring 2005**
Homework assignment 3
13.4.2005

Deadline 29.4.2005.

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 1 gets into the trying state, it can eventually get to the critical section.
3. If process 1 gets into the trying state, 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 noncritical section.
5. From the noncritical state process 1 cannot enter the critical section without visiting the trying state first.
6. From the initial state process 1 can enter the critical section before process 2 enters it.

Part Two

Check the properties (1-6) above for a model of a mutual exclusion algorithm (see below) using the `SMV` model checker. See instructions on the web page of the course (`http://www.tcs.hut.fi/Studies/T-79.146/`) how to use the `SMV` model checker which is available, e.g., in the Computing Centre Unix/Linux workstations.

Include in your answer paper the properties above specified in CTL and output of a session with `SMV` where all the properties are checked on the SMV model of the mutual exclusion algorithm.

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

The mutual exclusion algorithm

The model to be checked is the (possible world) model of a three process mutual exclusion system using a ticket algorithm, given as a `SMV` description which is available on the course web page. The program states of the processes are modelled by variables `statei`, for $1 \leq i \leq 3$. Consequently, there is one variable `statei` for each process `i`, which can have one of the following values: `ni` (noncritical), `ti` (trying), `ci` (critical). In model checking you can use atomic propositions of the form

$$\texttt{statei} = \texttt{ni}, \quad \texttt{statei} = \texttt{ti}, \quad \texttt{statei} = \texttt{ci}$$

where `i` is an integer in $\{1, 2, 3\}$. For instance, `(state2 = c2)` is true in all states in which process 2 is in the critical section.