“Model checking”

Prof. Dr. Marcel Kyas

Assignment 7, December 1, 2009

Freie Universität Berlin

Exercise 22 (5 Points) The following program is a mutual exclusion protocol for two processes due to Amir Pnueli. There is a single shared variable s that is either 0 or 1 and initially 1. Besides, each process has a local Boolean variable y that initially equals 0. The program text for process P_i ($i \in \{0,1\}$ is as follows:

```
for(;;) {
  // Non-critical section
  ($y_i$,s) = (1,i);
  await (($y_{i-1}$==0) || (s != i));
  // critical section
  $y_i$ = 0;
}
```

Here, the statement `(`y_i`,s)=(1,i)` is a multiple assignment in which y_i`=1` and `s=i` are executed as one single atomic step.

1. Model this algorithm in NuSMV and answer the following questions.
2. Give a CTL specifications that expresses mutual exclusion. Check, whether your algorithm satisfies your specification.
3. Give a CTL specifications that expresses absence of deadlock. Check, whether your algorithm satisfies your specification. Which fairness assumptions, if any, did you have to introduce to verify your claim?
4. Give a CTL specifications that expresses absence of starvation. Check, whether your algorithm satisfies your specification. Which fairness assumptions, if any, did you have to introduce to verify your claim?
5. We say that a mutual-exclusion algorithm has r-bounded waiting, if any process that tries to enter its critical section can do so before each other thread is able to enter its critical section $r+1$ times. Does there exist such a bound for Pnueli’s algorithm? If yes, provide one and check its validity using NuSMV. If not, explain why.

Exercise 23 (8 Points) The following problem was originally formulated by John A. Trono [1].

> Santa Claus sleeps in his shop up at the north pole, and can only be wakened up by either all nine reindeer being back from their year long vacation on the beaches of some tropical island in the South Pacific, or by some elves who are having some difficulties in making toys. One elf’s problem is never serious enough to wake up Santa (otherwise, he may *never* get any sleep), so, the elves visit Santa in a group of three. When three elves are having their problem solved, any other elves wishing to visit Santa must wait for those elves to return. If Santa wakes up to find three elves waiting at his shop’s door, along with the last reindeer having to come back from the tropics, Santa has decided that the elves can wait until after Christmas, because it is more important to get his sleigh ready as soon as possible. (It is assumed that the reindeer don’t want to leave the tropics, and therefore they stay there until the last possible moment. They might not even come back, but since Santa is footing

the bill for their year in paradise…This could also explain the quickness in their delivering of presents, since the reindeer can't wait to get back to where it is warm.) The penalty for the last reindeer to arrive is that it must get Santa while the others wait in a warming hut before being harnessed to the sleigh.

1. Model a solution to this problem in NuSMV. (You may consult the Solution of Trono's original article, but keep in mind that this one is erroneous. Maybe you can find his error.)
2. Specify one invariant for each of Santa, the elves, and the reindeers that describes all correct states of these processes. Use NuSMV to prove that this invariant is true.
3. Give a CTL specifications that expresses absence of deadlock. Check, whether your algorithm satisfies your specification. Which fairness assumptions, if any, did you have to introduce to verify your claim?
4. Give a CTL specifications that expresses absence of starvation. Check, whether your algorithm satisfies your specification. Which fairness assumptions, if any, did you have to introduce to verify your claim? (*Hint:* Your model should still give priority to reindeers. This should be reflected by your specification and be respected by Your fairness assumptions.)

Exercise 24 (8 Points) Consider the four transition systems in Figure 1. Check, whether $T_i \cong T_j$ and $T_i \leq_L T_j$ for all indexes i, j. Justify your answers by either providing a simulation for T_i, T_j or, when $T_i \not\leq_L T_j$, by providing a $\forall -$ CTL formula φ with $T_j \models \varphi$ and $T_i \not\models \varphi$.

Handing in this Assignment Please submit your hand-written solutions on paper no later than December 18, 2009, 12:15 (before the lecture).

The models shall be placed in a directory that carries the last name of one of the group members. Add a `README` file, or better, a `Makefile`, that explains or automates the modelling and checking procedures. Explain, how to interprete the results of model checking in an accompanying PDF or ASCII file.

Put all this into a tape archive that shares the name with the directory and send it by e-mail to marcel.kyas@fu-berlin.de. Use "Model checking 09 Series 7 *your last names*" as the subject line.

References

[1] John A Trono. A new exercise in concurrency. *SIGCSE Bulletin*, 26(3):8–10, 1994. Corrigendum: 26(4): 63.

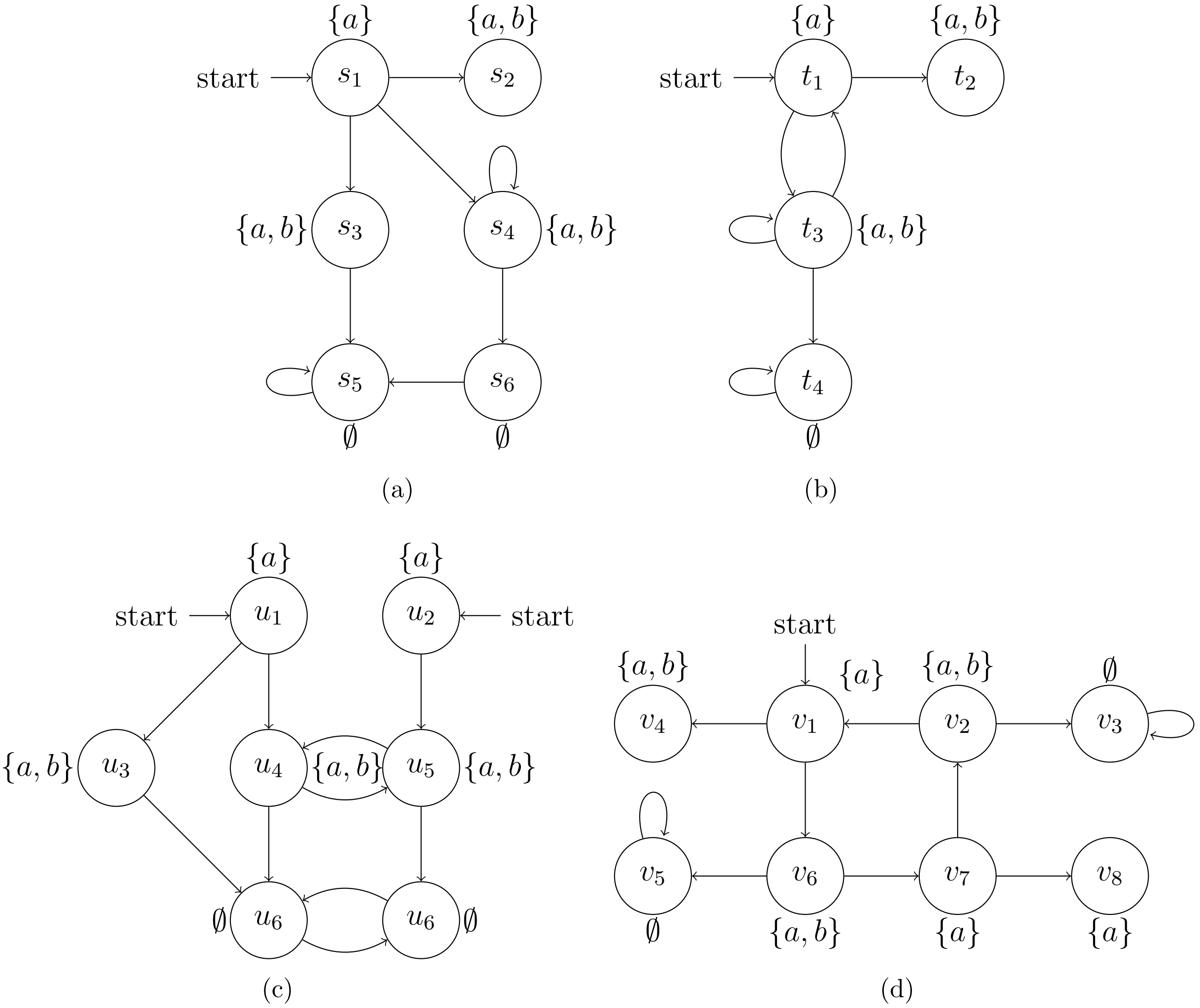

Figure 1: Four transition systems