Introduction to Model Checking
Exercises WS 2008/2009

René Thiemann

Institute of Computer Science
November 6, 2008

1. Formalize the following requirements in LTL. (increasing difficulty)
   (a) The traffic light is never red and green at the same time.
   (b) Under the assumption that the traffic light is orange infinitely often, it is green infinitely often and red infinitely often.
   (c) The sequence of lights is exactly $(\mathsf{red}, \mathsf{red\,orange}, \mathsf{green}, \mathsf{orange})^\omega$.
   (d) Whenever the traffic light shows red, at some moment strictly before, both red and orange have been shown.
   (e) The sequence of lights is of the form $(\mathsf{red}^+\,\mathsf{green}^+\,\mathsf{orange}^+)^\omega$.
   (f) The sequence of lights is of the form $(\mathsf{red}^+\,\mathsf{orange}^+\,\mathsf{green}^+\,\mathsf{orange}^+)^\omega$.
2. One of the requirements of the previous exercise is unsatisfiable if one assumes that all three colors are shown at least once. Identify this requirement and shortly explain why it is not satisfiable. How would you repair the requirement?
3. Prove the following equivalences
   - $\mathsf{G}\,(\varphi \wedge \psi) \quad \equiv \quad \mathsf{G}\,\varphi \;\wedge\; \mathsf{G}\,\psi$
   - $\mathsf{F}\,\mathsf{G}\,\mathsf{F}\,\varphi \quad \equiv \quad \mathsf{G}\,\mathsf{F}\,\varphi$
   - $\varphi\,\mathsf{U}\,\psi \quad \equiv \quad \psi \vee (\varphi \wedge \mathsf{X}\,(\varphi\,\mathsf{U}\,\psi))$
4. For each of the requirements in Exercise 1 build a corresponding GNBA that accepts the allowed behaviours.
5. Show that GNBAs are closed under union, i.e., given two GNBAs $\mathcal{A}_1$ and $\mathcal{A}_2$ over the same alphabet Σ, construct a new GNBA $\mathcal{A}$ such that $\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{A}_1) \cup \mathcal{L}(\mathcal{A}_2)$.

6. Consider the LTL-formula

$$\mathsf{G}\,(\mathsf{req} \Rightarrow \mathsf{X}\,\mathsf{F}\,\mathsf{resp}) \equiv \neg(\mathrm{true}\,\mathsf{U}\,(\mathsf{req} \wedge \neg\mathsf{X}\,(\mathrm{true}\,\mathsf{U}\,\mathsf{resp}))) = \psi$$

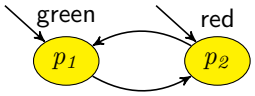
from the lecture. Compute $\mathcal{A}_\psi$ by using the improved translation where $cl'(\varphi) = \mathsf{req}, \mathsf{resp}, \ldots$:

   (a) compute the transition function symbolically in the form of constraints

   (b) compute the sets of final states symbolically

   (c) compute all outgoing transitions of state $(0,0,0,0,1)^T$ explicitly and for each of the states you encounter determine to which final state sets it belongs

7. Use the algorithm depicted on Slide 29 of Chapter 3 to determine $TS \models \varphi$ where $\varphi = \mathsf{G}\,\neg(\mathsf{red} \wedge \mathsf{green})$ and TS is the following transition system. Here, you should perform the computation of $\mathcal{A}_{\neg\varphi}$ and of the intersection automaton lazily, i.e., only construct the reachable part of the intersection automaton and only construct those parts of $\mathcal{A}_{\neg\varphi}$ that are needed!



8. Consider the requirement that whenever there is a *call* then within in two time units the phone is *ringing*. Someone formalized this in CTL as

$$\Phi := \mathsf{A}\,\mathsf{G}\,(\mathsf{call} \Rightarrow (\mathsf{ring} \vee \mathsf{A}\,\mathsf{X}\,\mathsf{ring} \vee \mathsf{A}\,\mathsf{X}\,\mathsf{A}\,\mathsf{X}\,\mathsf{ring})).$$

Figure out the problem of this formalization and provide a CTL*-formula Ψ that correctly describes the desired property.

9. Which of the following equalities are true?

   (a) $\mathsf{A}\,\mathsf{X}\,\mathsf{A}\,\mathsf{F}\,\varphi \equiv \mathsf{A}\,\mathsf{F}\,\mathsf{A}\,\mathsf{X}\,\varphi$

   (b) $\mathsf{E}\,\mathsf{X}\,\mathsf{E}\,\mathsf{F}\,\varphi \equiv \mathsf{E}\,\mathsf{F}\,\mathsf{E}\,\mathsf{X}\,\varphi$

   (c) $\mathsf{A}\,\mathsf{X}\,\mathsf{A}\,\mathsf{G}\,\varphi \equiv \mathsf{A}\,\mathsf{G}\,\mathsf{A}\,\mathsf{X}\,\varphi$

   (d) $\mathsf{A}\,\mathsf{G}\,\mathsf{F}\,\varphi \equiv \mathsf{A}\,\mathsf{G}\,\mathsf{A}\,\mathsf{F}\,\varphi$

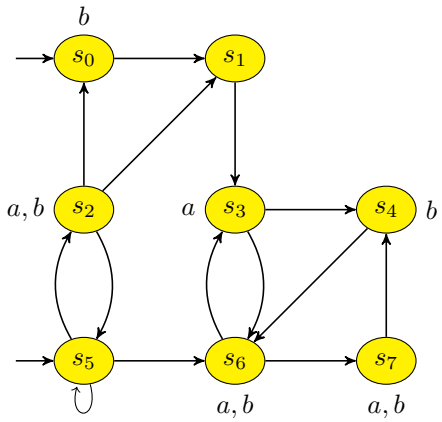
   (e) $\mathsf{A}\,\mathsf{F}\,\mathsf{G}\,\varphi \equiv \mathsf{A}\,\mathsf{F}\,\mathsf{A}\,\mathsf{G}\,\varphi$

   (f) $\neg\mathsf{A}\,\mathsf{G}\,\mathsf{F}\,\varphi \equiv \mathsf{E}\,\mathsf{F}\,\mathsf{G}\,\neg\varphi$

   For those equalities which are not true provide a counterexample.

10. Check whether the following transition system satisfies the formula

$$\mathsf{A}\,\mathsf{F}\,\mathsf{G}\,\mathsf{E}\,\mathsf{X}\,(a\,\mathsf{U}\,\mathsf{E}\,\mathsf{G}\,b).$$



You may perform the LTL-model checking intuitively, but write down all LTL-formulas that are checked.

11. Confirm yourself that it is not a good idea to use asynchronous communication for the traffic lights. To this end, create the transition system for the channel system

$$[\mathit{TrafficLight} \mid \mathit{TrafficLight} \mid \mathit{Starter}]$$

where c has a buffer of size 1.

12. The following nanoPromela code models the alternating bit protocol.

```
-------------  SENDER  -------------
atomic { b := 0; snd := true; }
do
  :: snd     =>  if :: true => c ! <m,b>
                    :: true => skip
                 fi ;
                 tmr_on ! dummy ;
                 snd := false;
  :: not snd => if :: true => timeout ? y ;
                              snd := true
                :: true => d ? x ;
                              if :: x = 1-b => skip
                                 :: x = b   => tmr_off ! dummy ;
                                               snd := true;
                                               b := 1 - b
                              fi
              fi
od
```

```
------------ RECEIVER -------------
b := 0;
do
  :: true => c ? <m,y> ;
              if :: y = 1-b => skip
                 :: y =  b  => d ! b;
                               b := 1-b
              fi
od

--------------  TIMER  -------------
do
  :: true => tmr_on ? x ;
              if :: true => timeout ! dummy
                 :: true => tmr_off ? x
              fi
od
```

Construct the program graphs for these statements according to the formal semantics. For the timer process also derive the transitions formally as demonstrated during the lecture on Slide 44 of Chapter 5.