Homework 4 - Exercises

Mikael Tulldahl, 901007
Björn Nilsson, 880302

Friday 8th May, 2015

1 Exercise 3.2

In the states, the first two letters denote if the signal is either green (g) or red (r), the two last letters describe if the train is either in mode bridge (b), waiting (w) or away (a) just like: {West signal, East signal, $Mode_W$, $Mode_E$}. For the transitions the first two letters denote the red and green signals for either east or west and the two last letters denote the controller signals arrive (a), leave (l) and absent (-) for the two stations respectively.

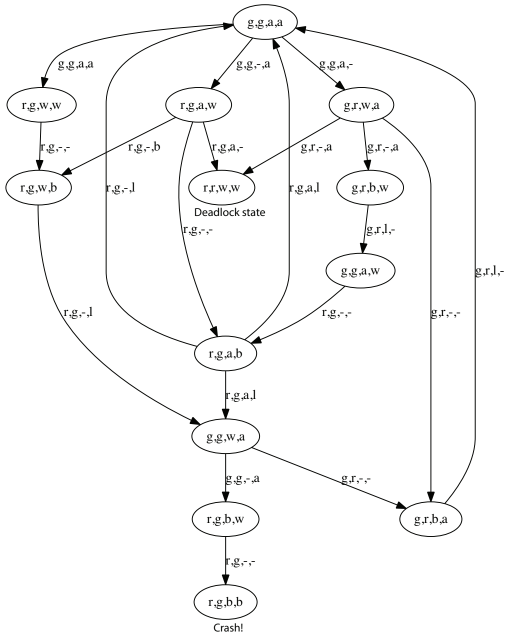

Figure 1: Exercise 3.2

This gives us that we have 13 reachable states.

2 Exercise 3.5

Is the property WestFairMonitor.mode $\neq$ 3 an invariant of the composite system RailRoadSystem2 || WestFairMonitor?

Yes it is, there is only three different branches in the RailRoadSystem2 automata:

- east and west train arrives
- west train arrives → east train arrives → west train leaves → west train arrives
- east train arrives → west train arrives → east train leaves → east train arrives → west train leaves → west train arrives

and it's easily seen that none of these contain the sequence: west train arrive → east train leave → east train leave

3 Exercise 3.8

The property $\varphi : x \geq 0$ is not an inductive invariant of the system in Figure 3.11 because the second requirement for an inductive invariant is not fulfilled.

The first requirement, that every initial state s satisfies φ is fulfilled because s(x)=0 and thus φ is satisfied.

the second requirement is not fulfilled because the state s(mode) = on, s(x) = 0 satisfies φ but the transition (s,on → off) does not.

ψ : x $\geq 0 \wedge ((mode =$ off) $\vee$ (x $\geq 1 \wedge mode =$ on))

ψ is stronger than φ because each state s that fulfills ψ also fulfills φ. ψ is an inductive invariant because:

- The initial state fulfills ψ.
- For a transition (s,t) where s satisfy ψ, t will also satisfy ψ.

Proof: s(mode) is either on or off. In the case when s(mode) = off, then s(x) $\geq$ 0. so t(x)= s(x) + 1 which satisfy ψ no matter what t(mode) is. In the case when s(mode) = on, then t(x)= s(x) - 1 so s(x) $\geq 1 \Rightarrow$ t(x)$\geq$ 0 which satisfy ψ.

4 Exercise 3.9

For each property below, state if it is an invariant and if it is an inductive variant

1. $\varphi : (near_E = 0) \leftrightarrow (node_E = away)$. φ is an inductive invariant because the initial state satisfies it, and every transition (s,t) satisfies it. proof: assume either of:
   - $s(mode_E) = away$ and $s(near_E) = 0$ then these two scenarios are possible:
     - $t(mode_E) = s(mode_E)$ which will mean that any update of Controller2 will have out_E as absent, and it can be seen in the code that it will result in $t(near_E)) = s(near_E)$ which satisfies the property.
     - $t(mode_E) \neq away$ which will mean that an event $out_E = arrive$ will update Controller2 and it can be seen in the code that it will result in $t(near_E) = 1$ which satisfies the property.
   - $s(mode_E) \neq away$ and $s(near_E) = 1$ then these two scenarios are possible:
     - $t(mode_E) = s(mode_E) = away$ which will mean that any update of Controller2 will have out_E as absent, and it can be seen in the code that it will result in $t(near_E)) = s(near_E)$ which satisfies the property.
     - $t(mode_E) \neq s(mode_E) \Leftrightarrow t(mode_E) = away$ which will mean that an event $out_E = leave$ will update Controller2 and it can be seen in the code that it will result in $t(near_E) = 0$ which satisfies the property.
2. $\varphi : mode_E = bridge \rightarrow east = green$. φ is an invariant because:

   before the train enter the bridge, it will be near, and it will continue be near until it leaves the bridge. so $mode_E = bridge \Rightarrow near_E = 1$. it will only enter the bridge if $east = green$, so transition from $mode_E = wait$ to $mode_E = bridge \Rightarrow east = green \wedge near_E = 1$ It is not possible to switch from $east = green$ to $east = red$ if $near_E = 1 \Rightarrow east = green$ while $mode_E = bridge$.

But it's not inductive. counterexample: transition (s,t) where $s(mode) = bridge$. $s(east) = green$ $s(near_E) = 0$ which satisfy the property, but then it's possible for $t(mode) = bridge$, $t(east) = red$ which is not satisfying the property.

3. *they can not be green at the same time* it's an inductive invariant, proof: The initial state satisfies φ and for every transition (s,t) where s satisfy φ, t satisfy φ.

    - if s(east)=green and s(west)red, then it can be easily seen in the Controller2 that if t(east)= green, t(west) can't become green. if t(east)= red it will also satisfy the property.
    - if s(east)=red and s(west)=green, then it can be easily seen in the Controller2 that if t(west)=green, t(east) can't become green. if t(west)= red it will also satisfy the property.