CSC410

Assignment 5

Due on Monday November 20, 2017 before 11am

Problem 1

(50 points) Four wounded soldiers find themselves behind enemy lines and try to flee to their home land. The enemy is chasing them and in the middle of the night, they arrive at a bridge that spans a river which is the border between the two countries at war. The bridge has been damaged and can only carry two soldiers at a time. Furthermore, several landmines have been placed on the bridge and a torch is needed to sidestep all the mines. The soldiers only have a single torch and they are not equally injured. The extent of their wounds have an effect on the time it takes to get across. The time needed for soldiers to pass the bridge are respectively 5, 10, 20, and 25 minutes respectively.

(a) (20 points) Construct a model of this problem in NuSMV and then reduce the question ?can all soldiers cross the bridge in 60 minutes or less? to model checking problem by stating the question as an LTL property.

Make sure that your model will include all possible scenarios for crossings (even pointless ones such as one soldier takes the torch to the other side and then comes back). Like our homework 2, it is not your job to partially solve the problem and encode any solution into the model. The model should just rule out moves that are made impossible by the storyline above. Anything move that can be taken (by the stupidest possible problem solver) should be part of the model.

Next, we use the model and the power of model checker to solve the problem given different requirements for the solution. The solution requirements are listed below. For each item, one property (i.e. one LTL formula), checked through the model is the answer that we require.

(b) (5 points) Can all soldiers eventually cross the bridge? Note that this is a yes/no question.

(c) (5 points) Can you rephrase the first property so that you get the model checker to tell you the step-by-step scenario under which all soldiers can cross the bridge?

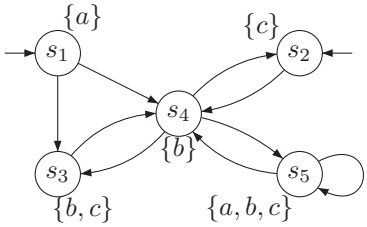
(d) (5 points) Is there a scenario in which only one soldier is left at the enemy side of the bridge? (yes/no question)

(e) (5 points) Can you rephrase property (c) so that you get the model checker to tell you how to get all soldiers across the bridge within 60 minutes?

Submission Guidelines. You will use the model checker NuSMV for the purpose of this exercise. It is installed on the teaching clusters. You will submit a text file called soldiers.smv which will contain the model and the properties listed (in the same order as the itemized list above).

Problem 2

(10 points) Consider the transition system TS over the set of atomic propositions $AP = \{a, b, c\}$:



Decide for each of the following LTL formulae ϕ_i below, whether $TS \models \phi_i$. Justify your answers. Informal, but solid justifications suffice. If $TS \not\models \phi_i$, provide a counterexample as your justification.

$$
\begin{array}{lcll}
\phi_1 & = & \Diamond\Box c & \text{Eventually Always C} \\
\phi_2 & = & \Box\Diamond c & \text{Always Eventually C} \\
\phi_3 & = & \bigcirc\neg c \implies \bigcirc\bigcirc c & \text{Next not C -> next next C} \\
\phi_4 & = & a \,\mathtt{U}\, \Box(b \vee c) & \text{a Until Always (b OR c)} \\
\phi_5 & = & (\bigcirc\bigcirc b) \,\mathtt{U}\, (b \vee c) & \text{(next next b) until (b or c)}
\end{array}
$$

Problem 3

(31 points) Which of the following equivalences are correct? Prove the equivalence or provide a counterexample that illustrates that the formula on the left and the formula on the right are not equivalent. For proofs, you are allowed to use the equalities that were already presented to you in class. But keep in mind that they may not solve all items. You need to refer to semantic definition of operators to get some of the proofs through. Naturally, you can do all the proofs directly using the semantic definitions.

(a) $\bigcirc\Diamond\phi \equiv \Diamond\bigcirc\phi$

(b) $\Box\Diamond\phi \implies \Box\Diamond\psi \equiv \Box(\phi \implies \Diamond\psi)$

(c) $(\Diamond\Box\phi_1) \wedge (\Diamond\Box\phi_2) \equiv \Diamond(\Box\phi_1 \wedge \Box\phi_2)$

(d) $\Diamond\Box\phi \implies \Box\Diamond\psi \equiv \Box(\phi \,\mathtt{U}(\psi \vee \neg\phi))$

(e) $\Box\phi \implies \Diamond\psi \equiv \phi \,\mathtt{U}(\psi \vee \neg\phi)$

Reminder: for the purposes of proving (or disproving) the equalities, you can either use the direct semantics of $\Box$ and $\Diamond$ or use equalities $\Diamond\phi \equiv \mathit{true}\,\mathtt{U}\,\phi$ and $\Box\phi \equiv \neg\Diamond\neg\phi$.

Problem 4

(9 points) Let ϕ and ψ be LTL formulae. Consider the following new operators.

(a) "At next" ($\phi \,\mathtt{N}\, \psi$): at the next point in time where ψ holds (is true), ϕ also holds.

(b) "While" ($\phi \,\mathtt{W}\, \psi$): ϕ holds at least as long as ψ does.

(c) "Before" ($\phi \,\mathtt{B}\, \psi$): if ψ holds at some point in the future, ϕ holds before.

Make the definitions of these informally stated operators precise by providing LTL formulae that formalize their intuitive meaning.