CSC 410F: Assignment 5

Due on November 20, 2017

Harman Sran **Ryan Downes** **Michael Li** **Steve Lu**

November 19, 2017

Problem 1

Four soldiers must cross a bridge - at most two at a time. The crossing soldier(s) must carry a torch - only one such torch is available. Each soldier crosses at a different time, and the crossers must stay together for the duration of the crossing. Can they cross in time?

(a)

Construct a model of this problem in NuSMV.

See comments in **soldiers.smv** for implementation details. In summary, we model all possible states as a four bit binary number - one bit for each soldier.

For example state **s1** represents **0001** - that is, soldier 4 is on the friendly side, and the other three are on the enemy side. Additionally, we track the torch's location with a boolean - **FALSE** when the torch is on the enemy side; we enforce that the torch must change sides on every transition - except on the final self-looping transition (at **s15**).

Then we have 16 possible states (represented by the four-bit binary form of 0 to 15). For next state transitions, we enumerate all valid next states from each state - based on the current location of the torch. We start on **s0** with torch = **FALSE**.

(b)

Can all soldiers eventually cross the bridge?

Yes; by sending two at a time from the enemy side to the friendly side, and only one back with the torch. Since we have a finite number of soldiers, eventually no one will be left on the enemy side.

(c)

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?

We specify the first property as the LTL specification:

$$G\ !\ ((\bigcirc torch = \neg torch) \cup (loc = s15)) \tag{1}$$

That is, there is never a point where we reach **s15** and that the torch always changes sides until then. The counterexample is the step by step scenario where all soldiers cross.

(d)

Is there a scenario in which only one soldier is left at the enemy side of the bridge?

Yes; by sending two over first, one back to the enemy side, and then another two over.

(e)

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?

We modify the LTL property to include the elapsed time at the current state:

$$G\ !\ ((\bigcirc torch = \neg torch) \cup (loc = s15\ \ \&\ \ elapsed < 61)) \tag{2}$$

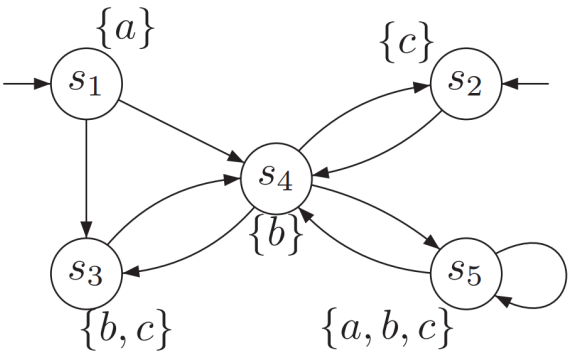
Then the counterexample is the step by step scenario where all soldiers cross within 60 minutes.

Implementation details are specified as comments in **soldiers.smv**; in summary, we introduce a new bounded integer, elapsed, ranging from 0 to 61. State transitions remain unchanged; for each valid transition, we increment elapsed appropriately - if elapsed will exceed 60 in the next transition, we lock it to 61 forever.

Both this and the earlier LTL property are included as working LTL specifications in **soldiers.smv**.

Problem 2

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.



(a)

$$\phi_1 = \Diamond\Box c \tag{3}$$

The TS **does not** model ϕ_1; consider the counterexample beginning at s_2 and going to s_4 and back to s_2 looping forever.

In this case, c never stabilizes and therefore eventually c stabilizes is a false statement.

(b)

$$\phi_2 = \Box\Diamond c \tag{4}$$

The TS **does** model ϕ_2; at any given state, either $\bigcirc c$ or $\bigcirc\bigcirc c$ holds.

(c)

$$\phi_3 = \bigcirc\neg c \implies \bigcirc\bigcirc c \tag{5}$$

The TS **does** model ϕ_3; the only state when the assumption $\bigcirc\neg c$ holds is when the next state is s_4, but $\bigcirc c$ holds at s_4 so the consequent $\bigcirc\bigcirc c$ holds.

Problem 2 continued on next page...

(d)

$$\phi_4 = a \cup \Box(b \vee c) \tag{6}$$

The TS **does** model ϕ_4. Starting at s_2, ϕ_4 holds because all reachable states have either b or c. The same is true when starting at s_1 - except for s_1 itself, but a holds at s_1 so the until is satisfied.

(e)

$$\phi_5 = (\bigcirc \bigcirc b) \cup (b \vee c) \tag{7}$$

The TS **does not** model ϕ_5; consider the counterexample $s_1 \to s_4 \to s_2$. $b \vee c$ is false at s_1, but b does not hold at s_2 - rendering the until unsatisfied.

Problem 3

Prove the equivalence or provide a counterexample.

(a)

$$\bigcirc\Diamond\phi \equiv \Diamond \bigcirc \phi \tag{8}$$

Proof. We expand the eventually operators and simplify:

$$\bigcirc(\mathrm{T} \cup \phi) \equiv \mathrm{T} \cup \bigcirc\phi \tag{9}$$
$$\bigcirc\mathrm{T} \cup \bigcirc\phi \equiv \mathrm{T} \cup \bigcirc\phi \tag{10}$$
$$\mathrm{T} \cup \bigcirc\phi \equiv \mathrm{T} \cup \bigcirc\phi \tag{11}$$

Thus the specification are equivalent. ■

(b)

$$\Box\Diamond\phi \implies \Box\Diamond\psi \equiv \Box(\phi \implies \Diamond\psi) \tag{12}$$

Proof. We prove the double implication to show that this is true.

Assume $\Box\Diamond\phi \implies \Box\Diamond\psi$; we have that if we have a path where ϕ recurs infinitely many times in the future, then ψ also recurs infinitely many times in the future - otherwise there is no other obligation on either ϕ or ψ. Then we have that the RHS also holds in this scheme - the RHS requires that anytime a ϕ occurs, a ψ must occur in the future sometime; when both are infinitely recurring, this holds trivially.

Assume $\Box(\phi \implies \Diamond\psi)$; we have that whenever we encounter a state with ϕ, then ψ will hold at some point in the future. If $\Box\Diamond\phi$ does not hold, then the LHS is holds trivially; if it does hold, then $\Box\Diamond\psi$ holds by our first assumption - whenever a one of our infinitely recurring ϕ's are encountered, ψ will hold at some future point, making the ψ's infinitely recurring as well.

By showing the double implication, we have that the specifications are equivalent. ■

(c)

$$(\Diamond\Box\phi_1) \wedge (\Diamond\Box\phi_2) \equiv \Diamond(\Box\phi_1 \wedge \Box\phi_2) \tag{13}$$

Proof. We prove the double implication to show that this is true.

Assume $(\Diamond\Box\phi_1) \wedge (\Diamond\Box\phi_2)$. We have that eventually ϕ_1 will always hold on our path, at some point X_0. Similarly, at some state onwards, ϕ_2 will always hold on our path, at some other point X_0'. Thus, at $MAX(X_0, X_0')$ both will hold together. But this is precisely the other specification (that eventually both hold true together, forever). Then, we have:

$$(\Diamond\Box\phi_1) \wedge (\Diamond\Box\phi_2) \implies \Diamond(\Box\phi_1 \wedge \Box\phi_2) \tag{14}$$

Assume $\Diamond(\Box\phi_1 \wedge \Box\phi_2)$; this says that eventually both hold true together, forever. Then both parts of the conjunction $(\Diamond\Box\phi_1) \wedge (\Diamond\Box\phi_2)$ hold since at that point (when both are true together forever), each holds independent of the other as well. Thus, we have shown:

$$\Diamond(\Box\phi_1 \wedge \Box\phi_2) \implies (\Diamond\Box\phi_1) \wedge (\Diamond\Box\phi_2) \tag{15}$$

Then, the specifications are equivalent. ■

(d)

$$\Diamond\Box\phi \implies \Box\Diamond\psi \equiv \Box(\phi \cup (\psi \vee \neg\phi)) \tag{16}$$

Proof. We prove the double implication to show that this is true; but first we simplify the RHS:

$$\Diamond\Box\phi \implies \Box\Diamond\psi \equiv \Box(\phi \cup (\phi \implies \psi)) \tag{17}$$

Assume $\Diamond\Box\phi \implies \Box\Diamond\psi$; there are exactly two cases to consider - when the antecedent is false and when it is true.

When the antecedent is false, the RHS holds trivially because the implication holds trivially as well - if we have *phi*, then the until is satisfied and we don't need to consider the implication, if we don't have *phi* then the implication holds trivially as mentioned.

When the antecedent is true, we have that there is a point in time, X_0 after which ϕ holds indefinitely, and that ψ recurs infinitely after X_0 as well. Before X_0, the RHS is satisfied since it is satisfied if either ϕ is true or false - at and after X_0 until is satisfied because ϕ holds indefinitely and the implication is eventually satisfied when ψ recurs.

Assume $\Box(\phi \cup (\phi \implies \psi))$, we will show that the LHS must always be true. The LHS can only be false if $\Diamond\Box\phi$ holds but $\Box\Diamond\psi$ does not. Assume $\Diamond\Box\phi$, then we have a point X_1 after which ϕ holds indefinitely. By our assumption of the RHS, the until must be satisfied - that is, there must always (by the always operator) be points where $\phi \implies \psi$ - but since ϕ is indefinitely true after X_1, ψ must be true at these infintely recurring points to satisfy both assumptions - thus we have $\Box\Diamond\psi$..
Then by showing that the double implication holds, we have that the specifications are equivalent. ■

(e)

$$\Box\phi \implies \Diamond\psi \equiv \phi \cup (\psi \vee \neg\phi) \tag{18}$$

This is not true, and we disprove by counterexample:

Proof. First we rewrite as:

$$\Box\phi \implies \Diamond\psi \equiv \phi \cup (\phi \implies \psi) \tag{19}$$

Consider a TS where ϕ always holds - then per the LHS, all paths in the TS must satisfy $\Diamond\psi$. Additionally any "sub path" of the path in question also has the property that ϕ always holds and hence it also must satisfy $\Diamond\psi$.

Consider checking the same TS for $TS \models RHS$; after the first time ψ holds, the TS's obligation for ψ ends - this is weaker than the LHS specification, which requires $\Diamond\psi$ at all times.

Thus, the specifications are not equivalent. ■

Problem 4

Let ϕ and ψ be LTL formulae. Precisely define the following new operators by providing LTL formulae for them:

(a)

"At Next" (ϕ N ψ): at the next point in time where ψ holds, ϕ also holds.

$$\phi \text{ N } \psi = \neg\psi \cup (\psi \wedge \phi) \tag{20}$$

(b)

"While" (ϕ W ψ): ϕ holds at least as long as ψ does.

$$\phi \text{ W } \psi = (\phi \wedge \psi) \cup \neg\psi \tag{21}$$

Problem 4 continued on next page...

(c)

"Before" (ϕ B ψ): if ψ holds at some point in the future, ϕ holds before.

$$\phi \text{ B } \psi = (\neg\psi \wedge \Diamond\psi) \implies (\neg\psi \wedge \bigcirc\neg\psi) \cup \phi \tag{22}$$