Model checking supervision questions

Dominic Mulligan

18th May 2017

A series of supervision questions on model checking for the Cambridge Computer Science Tripos Part II course "Hoare Logic and Model Checking". Current for academic year 2016–2017. Please report any mistakes or infelicities to Dominic Mulligan (e-mail: dpm36@cam.ac.uk).

Exercises are split into easy (marked with an "E"), medium (marked with an "M"), and hard (marked with a "H") based on my *ad hoc* and potentially misleading estimations.

1 Formal methods

Exercise 1.1. *(E) Compare and contrast the use of Hoare- (and Separation-) Logic with Model Checking. When would one use one approach over the other? What are the advantages and disadvantages of both?*

Exercise 1.2. *(E) Compare and constrast testing with Model Checking. What are the advantages of each? What are the disadvantages of each?*

Exercise 1.3. *(E) Many properties of systems can be characterised as "liveness" or "safety" properties. Informally, a liveness property asserts that something "good" will eventually happen, whereas a safety property asserts that something "bad" will never happen. Give three example liveness properties, and three example safety properties, that one may wish to establish of the control software for a prototype driverless car.*

Exercise 1.4. *(M) It is immediately obvious that an informal English-language system description can feasibly be modelled formally in many different ways. Further, English-language specifications of a system's behaviour can also feasibly be translated into temporal formulae in many different ways, potentially with slightly different meanings.*

Suppose, after graduation, you are tasked with verifying a heart pacemaker for an important medical device manufacturer by your employer. Your boss understands you sat through Part II "Hoare Logic and Model Checking" whilst at Cambridge, and requests that you use your well-developed Model Checking skills to provide the assurance that the customer requires. How would you ensure that the formal model of the pacemaker that you produce is an accurate reflection of the customer's implemented system? How would you ensure that the temporal properties that you are verifying are sufficient to establish that the pacemaker is suitable for use in humans?

2 Transition systems and models

Exercise 2.1. *(M) Matache Cargo Company operate an extensive road haulage fleet throughout Continental Europe and the British Isles. The company's haulage network is described in pictorial form in Figure 1. Here, nodes represent one of the company's cargo depots, situated in various important European locales, with edges between nodes asserting that an item of cargo can be moved from one depot to the next in the network by one of the company's trucks, in a non-stop journey.*

Suppose cargo items M and R originate in Madrid and Rome, respectively. Describe the possible movements of the two goods throughout the Matache Cargo Company's haulage network as a transition system. Make clear which state, or states, is the initial state. Note that goods can move forwards and backwards through the network, and also may reside in any one depot for an indeterminate length of time, waiting for available trucks to move them on.

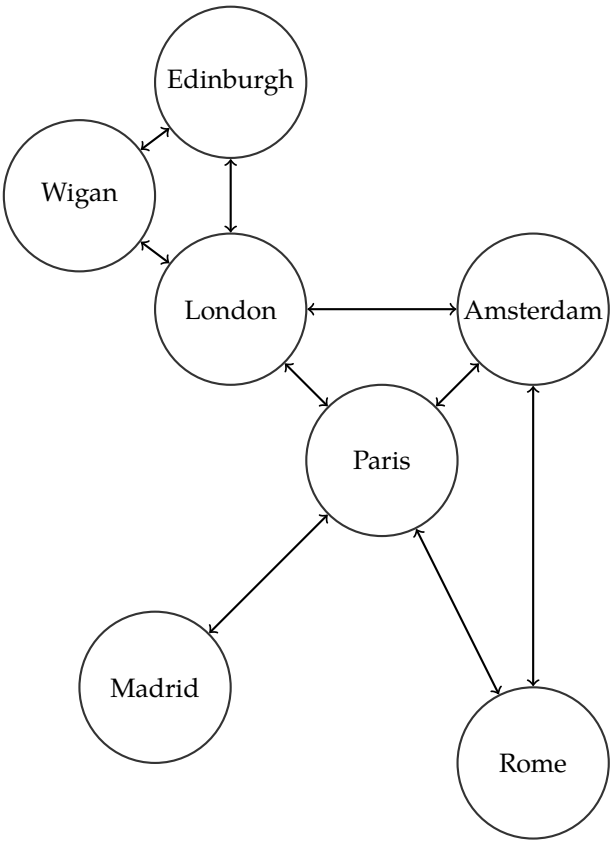

Figure 1: The Matache Cargo Company depots and haulage network

Exercise 2.2. *(M) Rawson, Rawson, Rawson, Woods, and Rawson Ltd. operate a sugar processing plant in rural East Anglia. Raw beet sugar is delivered to the processing plant by a truck from the Matache Cargo Company. A robotic crane then removes beet from the delivery truck and places it into one of three hoppers, picking a hopper arbitrarily to avoid wearing out any particular one (the company is infamously thrifty). Once a hopper is filled, beet is fed into Rawson, Rawson, Rawson, Woods, and Rawson Ltd's state of the art sugar extraction mechanism, with the hopper eventually emptied of its content.*

Using a suitable set of atomic propositions—e.g., `truck_present`, `beets_in_truck`, `crane_down`, `crane_up`, *and similar—produce a transition system which captures the possible state evolutions of the sugar processing plant described above. As an initial state, assume that no delivery truck is present, all hoppers are empty, and the crane is in an upright position.*

What difficulties did you have in translating the English language description of the sugar processing plant into a transition system? Did you make any assumptions when constructing the transition system of the sugar processing plant?

Exercise 2.3. *(E) Hardy Semiconductor of Yorkshire, plc. have produced a state-of-the-art non-deterministic increment/decrement subroutine, suitable for use in the control software of robotic cranes. An excerpt of the source code from this subroutine is below:*

```
n := 1;
while (*) do:
  n := n+1;
n := 0;
```

Here, `(*)` *is another subroutine, where the source is elided to prevent industrial espionage, that non-deterministically evaluates to true or false each time it is evaluated. Model this program as a transition system. Make clear which states are the start states of the system.*

Lastly, suggest a concrete representation for the transition system's state space.

Exercise 2.4. *(M) Svendsen Heavy Industries specialise in producing derivative chemical products from two base elements: carbon (C), and oxygen (O). Recall the following chemical reactions:*

$$\begin{aligned} 2O &\longrightarrow O_2 \\ C + O &\longrightarrow CO \\ 2C + O_2 &\longrightarrow 2CO \\ C + O_2 &\longrightarrow CO_2 \end{aligned}$$

Suppose the company's lunatic chief scientist, Dr. Kasper, loads a reaction vessel with 2 atoms of oxygen and 2 atoms of carbon one morning, and thereafter randomly starts flicking temperature and pressure dials so that the ensuing reactions are unpredictable. Use a transition system to model the possible chemical reactions that take place within the reaction vessel, using only the chemical reactions listed above.

Lastly, suggest a concrete representation for the transition system's state space.

Exercise 2.5. *(M) Recall a model for LTL and CTL is a right-serial transition system with an accompanying labelling function.*

Suppose $\mathcal{M}^1 = \langle S^1, S^1_0, \to^1, \mathcal{L}^1 \rangle$ and $\mathcal{M}^2 = \langle S^2, S^2_0, \to^2, \mathcal{L}^2 \rangle$ are two models over the same set of atomic propositions. Define a binary operation on models, $\mathcal{M}^1 \bowtie \mathcal{M}^2$, which produces a new model with state set $S^1 \uplus S^2$ ($\uplus$ is disjoint union on sets). Show that $\mathcal{M}^1 \bowtie \mathcal{M}^2$ is itself a model.

Exercise 2.6. *(H) Show that the simulation preorder $\mathcal{M}^1 \preceq \mathcal{M}^2$ between models is indeed a preorder, i.e. that it is reflexive and transitive.*

3 LTL

Exercise 3.1. *(E) Explain the difference between $\Box\Diamond$ p and $\Diamond\Box$ p, for* p *atomic. Do they express the same property? Do they imply each other?*

Exercise 3.2. *(E) Suppose* `halt`, `power_on`, `deadlock`, *and* `enabled` *are atomic propositions. Provide LTL formulae that capture the essence of the following temporal properties, or argue why they cannot be captured as LTL formulae:*

1. *"If the power is on, then it is always the case that the system will eventually halt".*
2. *"The machine will eventually deadlock or halt".*
3. *"If the power is on and the system is enabled then the machine will deadlock infinitely often".*
4. *"If the machine deadlocks then the power will eventually be turned off".*
5. *"If the power is on then it is possible for the machine to get to a state where it is not enabled and thereafter deadlocked".*
6. *"The machine will always deadlock infinitely often until the power is turned off".*

Exercise 3.3. *(M) Suppose $\mathcal{M}$ is the following model:*

- *States are taken to be the natural numbers strictly less than 6, i.e. $S = \{0, 1, 2, 3, 4, 5\}$. The initial state is $\{0\}$.*
- *The transition relation is $\rightarrow = \{(s, t) \mid s - t \leq 3$ for all $s, t \in S\}$. Here $s - t$ is a* truncating subtraction *on the natural numbers with cutoff 0, so $3 - 5 = 0$, and $3 - 1 = 2$ (i.e. if t is greater than or equal to s, then $s - t = 0$, otherwise subtraction behaves as one would expect).*
- *If $AP = \{\mathsf{e}, \mathsf{o}\}$ is the set of atomic propositions, then the labelling function $\mathcal{L} : S \rightarrow \mathbb{AP}$ is given by:*

$$\mathcal{L}(s) = \mathsf{e} \text{ if } s \text{ is even, or } \mathcal{L}(s) = \mathsf{o} \text{ otherwise}$$

Draw out the model, and then show or refute the following:

1. *Show that $\mathcal{M}$ is a valid model, in that it is right-serial, i.e. for every $s \in S$ there exists a $t \in S$ such that $s \rightarrow t$.*
2. *Exhibit a path π in $\mathcal{M}$ such that $\pi \models \Box\mathsf{e}$.*
3. *Exhibit a path π in $\mathcal{M}$ such that $\pi \models \Box(\mathsf{e} \rightarrow \bigcirc\mathsf{o})$.*
4. *Exhibit a path π in $\mathcal{M}$ such that $\pi \models \Diamond(\mathsf{o} \wedge \bigcirc\mathsf{e})$.*

Exercise 3.4. *(E) Define* bi-implication *$\phi \leftrightarrow \psi$ as a derived connective. Derive a precise meaning for $\pi \models \phi \leftrightarrow \psi$.*

Exercise 3.5. *(M) Define the* release *temporal modality ϕ `RELEASE` ψ as the dual of the* until *temporal modality, that is:*

$$\phi \texttt{ RELEASE } \psi \quad \stackrel{\texttt{def}}{=} \quad \neg(\neg\phi \texttt{ UNTIL } \neg\psi)$$

Describe in words an intuitive semantics for the release modality. Derive a precise meaning for $\pi \models \phi$ `RELEASE` ψ.

Exercise 3.6. *(M) Define the* weak until *temporal modality ϕ `WEAK` ψ as:*

$$\phi \texttt{ WEAK } \psi \quad \stackrel{\texttt{def}}{=} \quad (\phi \texttt{ UNTIL } \psi) \vee \Box\phi$$

Describe in words an intuitive semantics for the weak until modality. Derive a precise meaning for $\pi \models \phi$ `WEAK` ψ.

Exercise 3.7. *(H) Extend LTL with* past temporal connectives*: $\Box^{-1}\phi$, $\Diamond^{-1}\phi$, $\bigcirc^{-1}\phi$, and ϕ `UNTIL`$^{-1}$ ψ. Describe any changes to the notion of model that you must make to accommodate these past connectives. Derive precise meanings for $\pi \models \Box^{-1}\phi$, $\pi \models \Diamond^{-1}\phi$, and so on.*

Exercise 3.8. *(M) Define a notion of* semantic equivalence *for LTL formulae, $\phi \equiv \psi$, by:*

$$\phi \equiv \psi \quad \stackrel{\texttt{def}}{=} \quad \forall \mathcal{M}. \forall \pi \in \mathcal{M}. \mathcal{M}, \pi \models \phi \textit{ iff } \mathcal{M}, \pi \models \psi$$

Show that this "equivalence" is indeed an equivalence relation, by demonstrating that it is reflexive, symmetric, and transitive.

Exercise 3.9. *(M) Show the following semantic equivalences hold (where ϕ and ψ are arbitrary LTL formulae):*

1. $\top \vee \phi \equiv \top$
2. $\phi \wedge \psi \equiv \psi \wedge \phi$
3. $\neg(\phi \vee \psi) \equiv \neg\phi \wedge \neg\psi$

Exercise 3.10. *(H) Show the following semantic equivalences hold (where ϕ and ψ are arbitrary LTL formulae):*

1. $\neg \bigcirc \phi \equiv \bigcirc \neg\phi$
2. $\Diamond(\phi \vee \psi) \equiv \Diamond\phi \vee \Diamond\psi$
3. $\Box(\phi \wedge \psi) \equiv \Box\phi \wedge \Box\psi$

Exercise 3.11. *(H) Define an ordering on LTL formulae, $\phi \preceq \psi$, by:*

$$\phi \preceq \psi \quad \stackrel{\texttt{def}}{=} \quad \exists \xi. \phi \vee \xi \equiv \psi$$

1. *Show that this ordering is* well-defined *with respect to semantic equivalence. That is, if $\phi_1 \equiv \phi_2$ and $\psi_1 \equiv \psi_2$ then $\phi_1 \preceq \psi_1$ implies $\phi_2 \preceq \psi_2$.*
2. *Show that $\phi \preceq \top$ and $\bot \preceq \phi$ for all LTL formulae ϕ.*
3. *Show that the ordering is a preorder, that is, it is reflexive and transitive.*

Exercise 3.12. *(M) Define a notion of* validity *for LTL formulae, $\models \phi$, by:*

$$\models \phi \quad \stackrel{\texttt{def}}{=} \quad \forall \mathcal{M}. \forall \pi \in \mathcal{M}. \mathcal{M}, \pi \models \phi$$

Show that if $\phi \equiv \top$ then $\models \phi$. Derive as a consequence of this fact that $\models \phi \vee \neg\phi$ is an LTL validity.

Exercise 3.13. *(H) Show:*

1. *If $\models \phi \wedge \psi$ then $\models \phi$, and also $\models \psi$.*
2. *If $\models \phi$ and $\models \psi$ then $\models \phi \wedge \psi$.*
3. *If $\models \phi$ then $\models \phi \vee \psi$.*

4 CTL

Exercise 4.1. *(E) Suppose there are five philosophers sat around a table. Write* `philosopher_1_eats` *to assert that the first philosopher is eating,* `philosopher_2_eats` *to assert that the second philosopher is eating, and so on and so forth. Express the following claims about the state of the philosophers as CTL formulae:*

1. *"Philosopher 2 is the first philosopher to eat".*
2. *"Whenever philosopher 4 has finished eating, he cannot eat again until philosopher 1 has finished".*

3. *"Philosophers 5 and 3 will never eat at the same time".*

Exercise 4.2. *(E) Suppose* $\mathtt{p}$ *and* $\mathtt{q}$ *are atomic propositions. Provide natural language translations for the following CTL formulae:*

1. $\exists(\mathtt{p}\ \mathtt{UNTIL}\ \mathtt{q})$
2. $\forall(\Box\ \mathtt{p})$
3. $\exists\Diamond(\mathtt{p} \to \forall\Box\ \mathtt{q})$

Exercise 4.3. *(E) Write a CTL formula that expresses the fact that* $\mathtt{deadlock}$ *never occurs.*

Exercise 4.4. *(M) Suppose* $\mathcal{M}$ *is the following model:*

- *States are taken to be the natural numbers strictly less than 6, i.e.* $S = \{0, 1, 2, 3, 4, 5\}$*. The initial state is* $\{0\}$*.*
- *The transition relation is* $\to = \{(s, t) \mid \text{for all } s \in S, t \in S\}$*, i.e. all states may transition to any other state, with the underlying graph of the transition relation being fully connected.*
- *The set of atomic propositions* $AP = S \cup \{\mathtt{e}, \mathtt{o}\}$ *with the labelling function* $\mathcal{L} : S \to \mathbb{P}(AP)$ *given by:*

  $$\mathcal{L}(s) = \{s, \mathtt{e}\} \text{ if } s \text{ is even, or } \mathcal{L}(s) = \{s, \mathtt{o}\} \text{ otherwise}$$

  Note that the labelling function labels every state s *with its own "name", allowing us to refer to an explicit state within formulae.*

Show (or refute) the following:

1. *Show that* $\mathcal{M}$ *is a valid model, in that it is right-serial.*
2. *Show how one can encode in CTL the following claim: "every path beginning in state* 3 *has an infinite number of '*$\mathtt{e}$*' labels along it".*
3. *Show how one can encode in CTL the following claim: "beginning in state* 1 *it is possible to eventually reach state* 1 *again using a path that passes through state* 2*".*
4. *Show* $0 \models \forall(\Box(1 \to \exists\Diamond\ (2 \wedge \mathtt{e})))$*.*

Exercise 4.5. *(M) Define the existential* weak until *temporal modality* $\exists(\Phi\ \mathtt{WEAK}\ \Psi)$*, by:*

$$\exists(\Phi\ \mathtt{WEAK}\ \Psi) \quad \stackrel{\mathtt{def}}{=} \quad \exists(\Phi\ \mathtt{UNTIL}\ \Psi) \vee \exists\Box\Phi$$

Describe in words an intuitive semantics for the existential weak until modality. Derive a precise meaning for $s \models \exists(\Phi\ \mathtt{WEAK}\ \Psi)$*.*

Exercise 4.6. *(H) Show* $s \models \forall\Box\forall\Diamond p$ *if and only if* $\forall\pi \in Paths(s).\ \pi[i] \models p$ *for infinitely many* i*.*

Exercise 4.7. *(M) Show that semantic equivalence* $\Phi \equiv \Psi$ *is an equivalence relation, i.e. that it is* reflexive, symmetric, *and* transitive*.*

Exercise 4.8. *(M) Show that if* $\Phi_1 \equiv \Phi_2$ *and* $\Psi_1 \equiv \Psi_2$ *then:*

- $\Phi_1 \wedge \Psi_1 \equiv \Phi_2 \wedge \Psi_2$
- $\Phi_1 \to \Psi_1 \equiv \Phi_2 \to \Psi_2$
- $\forall(\Phi_1\ \mathtt{UNTIL}\ \Psi_1) \equiv \forall(\Phi_2\ \mathtt{UNTIL}\ \Psi_2)$

That is, semantic equivalence commutes with the structure of formulae.

Exercise 4.9. *(E) Show* $\neg\neg\Phi \equiv \Phi$*, i.e. that negation is* involutive*.*

Exercise 4.10. *(M) Show* $\Phi \vee (\Psi \wedge \Xi) \equiv (\Phi \vee \Psi) \wedge (\Phi \vee \Xi)$*, i.e. that disjunction* distributes *over conjunction.*

Exercise 4.11. *(H) Show that* $\exists\Diamond(\Phi \vee \Psi)$ *and* $\exists\Diamond\Phi \vee \exists\Diamond\Psi$ *are semantically equivalent.*

Exercise 4.12. *(E) Show that* $\Phi \wedge \Psi$ *and* $\Phi \vee \Psi$ *are* not *semantically equivalent.*

Exercise 4.13. *(H) Show that* $\forall\Diamond(\Phi \vee \Psi)$ *and* $\forall\Diamond\Phi \vee \forall\Diamond\Psi$ *are not semantically equivalent.*

5 CTL model checking

Exercise 5.1. *(H) Prove that every CTL formula has an equivalent Existential Normal Form (ENF) formula. Sketch a recursive algorithm, based on your proof, that converts a CTL formula into its ENF equivalent.*

Does the size of a formula increase or decrease when converted to ENF with your translation? Speculate on how this may affect the perennial LTL vs. CTL debate.

Exercise 5.2. *(E) Convert the following formulae into Existential Normal Form:*

1. $\forall(\Diamond(\phi \vee \psi))$
2. $\top \vee ((\exists\Diamond\bot) \wedge \phi)$
3. $\forall(\Box(\phi \rightarrow \forall\Diamond\psi))$

Exercise 5.3. *(H) Show that* $\exists(\Phi \texttt{ UNTIL } \Psi)$ *satisfies an* expansion *law, in that:*

$$\exists(\Phi \texttt{ UNTIL } \Psi) \equiv \Psi \vee (\Phi \wedge \exists\bigcirc\exists(\Phi \texttt{ UNTIL } \Psi))$$

Exercise 5.4. *(H) Show that* $\exists\Box\Phi$ *satisfies an* expansion *law, in that:*

$$\exists\Box\Phi \equiv \Phi \wedge \exists\bigcirc\exists\Box\Phi$$

Exercise 5.5. *(E) Show that if* $\Phi \equiv \Psi$ *then* $Sat(\Phi) = Sat(\Psi)$ *(in a fixed model,* $\mathcal{M}$*).*

Exercise 5.6. *(E) Describe* $Sat(\Phi \rightarrow \Psi)$ *and* $Sat(\bot)$ *(in a fixed model,* $\mathcal{M}$*).*

Exercise 5.7. *(M) Suppose* $\mathcal{M}$ *is the following model:*

- *States are taken to be the natural numbers strictly less than 6, i.e.* $S = \{0, 1, 2, 3, 4, 5\}$*. The initial state is* $\{0\}$*.*
- *The transition relation is* $\rightarrow = \{(s, t) \mid$ *for all* $s \in S, t \in S\}$*, i.e. all states may transition to any other state, with the underlying graph of the transition relation being fully connected.*
- *The set of atomic propositions* $AP = \{\mathtt{e}, \mathtt{o}\}$ *with the labelling function* $\mathcal{L} : S \rightarrow \mathbb{P}(AP)$ *given by:*

$$\mathcal{L}(s) = \{\mathtt{e}\} \text{ if } s \text{ is even, or } \mathcal{L}(s) = \{\mathtt{o}\} \text{ otherwise}$$

Compute the following:

1. *Convert* $\forall\Box(\mathtt{e} \rightarrow \exists\bigcirc\mathtt{o})$ *into Existential Normal Form.*
2. *Compute the satisfaction-set of the Existential Normal Form formula, obtained above, in model* $\mathcal{M}$ *using the recursive labelling algorithm presented in lectures. Fully explain your working.*
3. *Show, or refute, the claim that* $\mathcal{M}, 0 \models \forall\Box(\mathtt{e} \rightarrow \exists\bigcirc\mathtt{o})$*.*

6 NuSMV case studies

As a first step in becoming familiar with NuSMV, replay some of the NuSMV model checking examples, provided in lectures, on your own machine. Make sure you try both the NuSMV interactive and batch (command-line) modes. Use the interactive mode to generate example execution traces for all of the examples.

When familiar with the use of NuSMV, try the following exercises. Note that in all cases aspects of the scenario being modelled are intentionally left vague. Correctly modelling a particular scenario is as much an art as a science, and in each case you should provide arguments why your SMV models correctly capture the scenario at hand.

Exercise 6.1. *(H) Suppose Cambridgeshire County Council employ you to ensure that all traffic lights in the county are "safe". To check that you are qualified for the role, as a first step they wish you to model the interaction of a set of traffic lights at a simple crossroads with no pedestrian crossings.*

In particular, in this simplified scenario, two roads—one heading north-south, and the other east-west—meet and the flow of traffic is mediated by a set of traffic lights. In the United Kingdom, traffic lights progress from red (meaning stop), to red-amber (meaning prepare to go), to green (meaning go), to amber (meaning prepare to stop), back to red.

Complete the following:

1. *Describe some plausible properties in natural language that this set of traffic lights should possess, to convince Cambridgeshire County Council that the traffic lights are "safe" for deployment on public roads.*
2. *Model the traffic lights in NuSMV, using the SMV modelling language. Argue why your formal model correctly captures the scenario described above, and describe any assumptions made when modelling the traffic lights in NuSMV, if any.*
3. *Translate two of your natural language properties, described above, into LTL and show that your implementation meets these properties, using NuSMV's LTL model checking facilities.*

Exercise 6.2. *(H) Recall the following chemical reactions from Dr. Kasper's experiments, described previously:*

$$\begin{aligned} 2O &\longrightarrow O_2 \\ C + O &\longrightarrow CO \\ 2C + O_2 &\longrightarrow 2CO \\ C + O_2 &\longrightarrow CO_2 \end{aligned}$$

Dr. Kasper would like to know if, given a certain number of input carbon and oxygen atoms, there is any way for the contents of his reaction vessel to progress to a state where it contains three molecules of CO_2. Model the contents of the reaction vessel in NuSMV, assuming that the number of atoms and molecules of each type never exceeds 32. Use NuSMV's LTL model checking facilities to provide an answer to the question above. Describe any assumptions made when modelling the chemical reactions in NuSMV, if any.

Exercise 6.3. *(H) Impressed with your earlier success modelling a simple crossroads, Cambridgeshire County Council now request that you establish the safety of a more complex traffic lights arrangement. A single lane tunnel has traffic lights at both ends. Each traffic light has sensors which detect whether a car is waiting at the lights. Provided the tunnel is clear of traffic, a traffic light with cars waiting by it will eventually turn "green", allowing the waiting traffic through the tunnel. The state of the lights does not change unless there is waiting traffic.*

Model this scenario in NuSMV. Establish, via NuSMV's LTL model checking facilities, that your model does not permit traffic waiting at a traffic light to "go" whilst cars are passing through the tunnel in the opposite direction. Argue why your formal model correctly captures the scenario described above, and describe any assumptions made when modelling the traffic lights in NuSMV, if any.

Exercise 6.4. *(M) Recall the Matache Cargo Company's haulage network, mentioned previously. Model the movement of the goods M and R through this network in NuSMV, and establish by CTL model checking that it is possible for both goods to be delivered to Edinburgh from their starting locations. (In NuSMV, use the `CTLSPEC` block command embedded in an SMV source file, or the `check_ctlspec` command in interactive mode, to model check a CTL formula. Note that A encodes $\forall$ and E encodes $\exists$ in SMV's syntax for CTL formulae.)*

Can you use NuSMV to automatically generate a series of movements for the two goods through the network so that they will eventually be delivered to Edinburgh? How?

Exercise 6.5. *(M) NuSMV's non-determinism can be used to check the correctness of purely combinatorial circuits (i.e. circuits with no state). Here, the use of NuSMV "degenerates" to using the tool to merely check all possible truth assignments to the inputs of a circuit.*

Recall that the truth table for a half-adder circuit is (where A and B are inputs and C and S are outputs):

A	B	C	S
0	*0*	*0*	*0*
1	*0*	*0*	*1*
0	*1*	*0*	*1*
1	*1*	*1*	*0*

Recall also that a half-adder circuit can be implemented as a combination of an XOR and an AND gate. Write a NuSMV module implementing a half-adder in terms of an XOR and AND gate, and provide 4 LTL formulae that serve to demonstrate the correctness of your implementation, based on the truth table above. Use NuSMV's LTL model checking facilities to show that your half-adder module correctly implements a half-adder circuit.

7 Miscellaneous

Exercise 7.1. *(E) Suppose* `p` *and* `q` *are atomic propositions. In each of the two cases below, find a pair of LTL and CTL formulae that correctly capture the claims:*

1. *"*`p` *will never happen".*
2. *"Whenever* `p` *happens, eventually* `q` *will happen".*

Exercise 7.2. *(H) Suppose* `p` *is an atomic proposition. Show that the LTL formula* $\Diamond\Box$ `p` *and the CTL formula* $\forall\Diamond\forall\Box$ `p` *describe different properties.*

Hint: find a model that separates the two properties, in that one holds and the other does not in that particular model.

Exercise 7.3. *(H) Recall the grammar of CTL$\star$ state and path formulae from the lecture slides. Give plausible definitions, based on those for LTL and CTL, for the two satisfaction relations* $s \models \Phi$ *and* $\pi \models \phi$ *where* Φ *is a CTL$\star$ state formula and* ϕ *is a CTL$\star$ path formula.*