Automated Reasoning

Lecture 14: Coursework 2
Model Checking with NuSMV

Robert Atkey
bob.atkey@ed.ac.uk

Friday 6th March 2015
Overview

The coursework is in 2 parts:

1. Exercises with Temporal Logic
   1.1 Exercises on LTL (15 marks)
   1.2 Exercises on CTL (20 marks)

2. Verifying a Toy Telephone Exchange
   2.1 Properties to Verify (30 marks)
   2.2 Model bug to fix (15 marks)
   2.3 Principles of LTL Model Checking (20 marks)

This coursework is worth 20% of your overall mark for the course.

The deadline is 2pm, Friday 20th March 2015.
Objectives of the Coursework

1. Acquire familiarity with the semantics of LTL formulas.
2. Acquire familiarity with the semantics of CTL formulas.
3. Experience in specifying a (toy) system using LTL and CTL.
4. Debugging a system using LTL model checking.
5. Exploring the principles of LTL model checking.
6. In general, gain knowledge of what model checking is capable of.
2.1 LTL

Write this model in NuSMV:

Use NuSMV to analyse some LTL properties ($G\ a$, $a\ U\ b$, ...):  
1. Determine whether each property is valid (i.e., true for all paths)  
2. Get NuSMV to generate a path that satisfies the formula
2.2 CTL

Equivalence of CTL formulas (*CTL will be covered in the next lecture*)

You are given a list of pairs of CTL formulas, you have to determine whether or not each pair is equivalent.

\[
\phi \equiv \psi \iff (\forall M \ s. M, s \models \phi \iff M, s \models \psi)
\]

For each pair:

- If they are equivalent, then explain why, with reference to the semantics of CTL.
- If they are not equivalent, then give a NuSMV model that distinguishes them.
An example: the formulas $\text{EF } \phi$ and $\text{EG } \phi$.

Not equivalent, this model distinguishes them:

For this model, $\text{EF } \phi$ is true, but $\text{EG } \phi$ is false.
Verifying a Toy Telephone Exchange

The file `exchange.smv` contains a model of a simple telephone exchange.

Two phones are connected.

At every time step, they can either dial, reject, pickup or hangup.
3.2 Properties to Verify

You are given several properties to state in temporal logic, and to verify against the model using NuSMV.

1. 5 properties in LTL
2. 2 properties in CTL

Note: As literally stated, some of the properties are not true. You will have to refine the property with additional assumptions in order to get it to hold for the model. But remember to stay true to the “spirit” of the property stated.
The telephone exchange model has a bug. The bug is highlighted by the failure of the following property to verify:

At any time, if the state is waiting and phone1 dials, and then at the next step hangs up, then at the time step after that, the phones should not be connected.

You have to:

1. Express this property in LTL, and get NuSMV to demonstrate a counterexample.
2. Explain what the bug is
3. Fix the model

You can use bounded model checking to get shorter counterexamples.
Principles of LTL model checking

*LTL Model Checking will be covered next week*

Roughly, LTL model checking works by the following process:

1. Start with some formula $\phi$.
2. Negate it: $\neg \phi$.
3. Convert $\neg \phi$ to a finite state automaton: a *Büchi* automaton.
4. Construct the *intersection* of the formula’s automaton and the model’s automaton.
5. Check to see whether the resulting automaton’s language is empty.

For this question: you carry out these steps (using NuSMV) for the formula:

$$G \left( (\text{state} = \text{waiting} \land \text{phone1} = \text{dial}) \rightarrow X \text{ringing2} \right)$$
This time: Coursework 2
  ▶ LTL and CTL
  ▶ Verifying a simple telephone exchange

Next time:
  ▶ CTL: Computation Tree Logic
  ▶ A Branching-time temporal logic