CS 6110 Software Correctness, Spring 2022
Lec10

Ganesh Gopalakrishnan
School of Computing
University of Utah
Salt Lake City, UT 84112

URL: bit.ly/cs6110s22

Slides for Lec10 : Agenda

- Worksheet on Murphi modeling (1)
  - Make you derive the model of a simple game in Murphi
  - Ask you to encode that game in Alloy in a similar fashion (Asg4)
    - You'll be shown a different way to solve this in Costello's tutorials (more verbose)
- Worksheet on our first experience with weak consistency
  - Make you experiment with a simple Java program to tell you about weak consistency
- Modeling weak consistency in Promela
  - Tell you how to check Peterson under TSO failing
- Asking you to check for weak consistency in Murphi
  - Part of Asg4
- So, Asg4 consists of
  - A model in Alloy similar to the Murphi model (succinct)
  - A model of TSO failing in Murphi

Murphi : the game of mwgc

- Worksheet on Murphi modeling (1)
  - Make you derive the model of a simple game in Murphi
- The game is that of the man, wolf, goat, and cabbage
  - They have to cross a river “safely”
  - Make a model-checker compute the moves
  - I’ll give you hints, you type and finish the model
- We will state the least amount of info and let state-space traversal do the solving for us

Murphi : the game of mwgc

- Worksheet on Murphi modeling (1)
  - Make you derive the model of a simple game in Murphi
- The game is that of the man, wolf, goat, and cabbage
  - They have to cross a river “safely”
  - Make a model-checker compute the moves
  - I’ll give you hints, you type and finish the model
- We will state the least amount of info and let state-space traversal do the solving for us

Outline of solution … you plz flesh out

- Declare four variables m,w,g,c as bools
- Rules: m goes with one other item
  - Items can’t go with m alone
  - Goal : all mwgc = true (on the right bank)
- Define a function safe(m,w,g,c : boolean): Boolean;
- Initialize mwgc to false
- Now the trick + questions
  - Are we safe at the beginning?
  - How do we specify all individual transitions s.t. they preserve safety?
- How do we trick a model-checker to print out the solution as an error trace?

Slides for Lec10 : Agenda

- Worksheet on Murphi modeling (1)
  - Make you derive the model of a simple game in Murphi
  - Ask you to encode that game in Alloy in a similar fashion (Asg4)
    - You'll be shown a different way to solve this in Costello's tutorials (more verbose)
- Worksheet on our first experience with weak consistency
  - Make you experiment with a simple Java program to tell you about weak consistency

Weak consistency experience

- Compile and run VGood.java and VGad.java as indicated on the class website (also in the class Git under Lec10)
- Read about Java volatiles here
  - http://tutorials.jenkov.com/java-concurrency/volatile.html
  - https://betterprogramming.pub/a-deep-dive-into-the-java-volatile-keyword-7e1b9f9df604
  - (Other docs are there too)
- Look at dekker_memory_model/ and the C++ examples there

Weak consistency simulation

- Peterson simulation in Promela
  - Study how Peterson's protocol for two processes can be
    - Run under Promela under "normal memory access"
    - Under TSO buffering

Asg4 work

- Modify 2_Peterson.m to achieve weak consistency simulation in Murphi

Last work item

- Roger Costello’s slides on Alloy (begin)