CSC3304 2011-12: Coursework 1

Aims

Improve knowledge and experience of applying model checking for the verification of software and hardware systems. Specifically to gain experience of using the modelling language PROMELA and the verification tool SPIN.

Objectives

1. To deepen your understanding of the role of model checking technology in the development of software and hardware systems.
2. To gain experience in conducting research in the literature, structuring and presenting a technical report.

Coursework Description

There are two separate deliverables for this course work:

a. Part 1: Complete a short research report (1200 words max, excluding references).
b. Part 2: Develop a model of a system using PROMELA and SPIN, and verify the correctness of your model with respect to some correctness requirements.

Assessment (Deadline: 2nd December 2011)

This coursework carries 20% of the total mark for the module. It is marked out of a total of 20 on the following basis:

Part 1 (Research report): 8 marks composed of:
Technical soundness (Logical structure, demonstrate understanding of chosen topic): 5
Presentation (use of good sources, well cited, clarity of style and layout): 3

Part 2 (Model Checking Exercise): 12 marks (See relevant section for breakdown of marks).

Part 1

Short Model Checking Research Report

Model checking tools can be used to verify a wide variety of systems. You can find a great deal of published literature and practical applications of model checking from a variety of sources.

Your task is to conduct research into a “real world” application of model checking that is of interest to you, and prepare a short report (Not more than 1200 words).

In your report describe the context, and the software / hardware system(s) that required verification. Explain the properties that required verification, and why model checking was chosen. Describe briefly the model checking tool and language used, and explain the methodology and how they were used to model and verify the systems intended.

Part 2

A Model Checking Exercise (Implement using PROMELA/SPIN)

Read the following description and then answer the questions which follow it.

Pablo's restaurant lets customers place orders using a table display without the need for any waiters. After an order has been placed, it is picked up by the chef who then prepares the order and sends it to the correct customer directly using a futuristic automated channel. An order includes a choice of one of {starter, main, desert, drink}, and the customer ID. The chef places the prepared order in the Service channel from where the customer can pick it up. The procedure for customers and chefs is as follows:

Customers:

- Each customer chooses arbitrarily among the possible choices, composes and sends out her/his order.
- The customer waits then for his/her order to arrive and takes it if it is addressed to her/him.
- Afterwards, the customer can either; make another choice and place an order; or leave the restaurant.

Chefs:

- A chef takes an order from the order channel and prepares the meal.
- The finished meal is then put in the service channel waiting for the customer to pick it up.

a) Implement the proctype chef, and 2 or 3 customer processes according to the specified protocol. Explain how you ensure that a customer takes only his/her order and not an order belonging to someone else. Label your code appropriately identifying the main states. Check your model for absence of invalid end states (deadlock). Use Spin to give a rough indication that the system behaves as expected using simulation. (5 marks)

b) Pablo's restaurant is extremely popular, and the owner (Pablo) would like to ensure that the greatest possible number of customers enjoy the experience. Modify your model so that a customer can make a maximum of 4 orders before he/she has to leave, and that he/she can have a maximum of 1 of each of the menu choices. Create an assertion (or a Never claim) and use SPIN to verify this correctness requirement. (5 marks)

c) Include within your model an additional possibility: After making a choice on the menu display, customers might not send the order through the order channel and prefer instead to go into think state, and then either make a new choice, or leave the restaurant. (Check customer and chef processes for absence of deadlock and modify your design appropriately to eliminate any errors). (2 marks)

Plagiarism:

The University has strict policies for penalising plagiarism, and all work submitted for assessment must be your own work. This does not prohibit discussion among students about coursework - indeed; such discussion to increase understanding is positively encouraged. However the answers submitted must be your original contribution, written and designed by you. It is permissible to include some material drawn directly from other sources (if you think this benefits the report part of the submission), but such non-original material must be explicitly declared to be a quotation from an external source - and that source must be listed.

Submission

The submission (**Through NESS**) is required as either a tar or a zip. Include within your folder:

Part1:

- PDF or MS Word document (1200 words max, excluding references)

Part2:

- 3 PROMELA models as ***.pml files
- Clearly named relevant simulation and verification output files. (Output data can be alternatively included in your rationale document)
- A well-structured PDF or MS Word document with a header on each page providing your name and student number. The document should explain the reasoning behind your solutions.

You may request further clarification by email from Ellis Solaiman: ellis.solaiman@ncl.ac.uk

Deadline: 2nd December 2011