College of Science – Computer Science

CSC385 – Modelling and Verification Techniques

May/June 2021

Release Time: **10:00 (Time Zone: BST)**

Deadline: **13:00 (Time Zone: BST)**

Alternative Assessment Information

- You ***MUST*** use your own copy of this assessment from Canvas. If you obtained this assessment document from a friend or elsewhere then delete this copy and use your own version from Canvas. If you experience difficulties to download the assessment, get in contact via the emails below.
- This is an open-book assessment. This means you may use your notes, textbooks, and other resources, including calculators. Copying from resources other than your notes requires referencing.
- You must submit before the deadline. Allow some spare time for technical submission issues.
- The total time for this assessment is 3 hours. This assessment is designed to be sat in a 2-hour window. An additional hour allows you time for accessing the paper, uploading your submission, and dealing with technical issues.
- It is suggested that you use Microsoft Word (or any other editor of your choice) to type your answers, then save as PDF when you are ready to submit. All submitted text (and code if present) must be word-processed, but you may include images (or photos of hand drawn images) as part of the document.
- This is an individual assessment. Under no circumstances are you to discuss any aspect of this assessment with anyone; nor are you allowed to share this document, ideas or solutions with others using email, social media, instant messaging, websites, or any other means. Your attempts at these questions must be entirely your own work. Those found to have collaborated with others will receive a mark of 0.

Special Instructions

Answer all questions.

Submission Instructions

- Please submit a **single PDF** file **named as your student number followed by the module code** (e.g. 123456-CSC789.pdf) via the submission link located on the module page in Canvas.

By submitting, electronically and/or hardcopy, you state that you fully understand and are complying with the university's policy on Academic Integrity and Academic Misconduct. The policy can be found at https://myuni.swansea.ac.uk/academic-life/academic-misconduct.

Originator(s): ***Ulrich Berger***

In case of queries email both: u.berger@swansea.ac.uk and H.Elliott@swansea.ac.uk

Question 1

We discussed two approaches to guaranteeing the correctness of programs: Testing and verification by a formal proof.

Briefly discuss the strengths and weaknesses of these methods.

[4 marks (2 for each method)]

Question 2

(a) Briefly describe the bisimulation game and explain how it characterises bisimilarity of processes.

[4 marks (2 for description, 2 for characterisation of bisimilarity]

(b) Suppose you are given a tool that can test determinism, deadlock freeness and bisimilarity of processes. Furthermore, suppose you are given two processes P and Q that are known to be deterministic.

Describe how the tool can be used to test whether P and Q are trace equivalent. Say which theoretical result makes this possible.

[4 marks (2 for description, 2 for theoretical result)]

(c) Give an example of two processes that are trace equivalent, but not bisimilar (you may draw diagrams). Justify your answer, that is, explain why the two process are trace equivalent, but not bisimilar.

[4 marks (2 for example, 2 for justification)]

Question 3

Consider the following processes describing a vending machine and a customer:

The vending machine, call it V, can do an action a (for 'accept') after which it is in a state, call it VA, where it accepts a coin c (that is, it can do an action c) after which it returns to the original state V.

Alternatively, V can do an action d (for 'deliver') after which it is in a state, call it VD, where it delivers tea (that is can do an action t) after which it returns to the original state V.

The customer, call her C, can pay with a coin (that is, do a c action) after which she is thirsty, that is, in the state CT. In the state CT she can drink tea (do action t) and return to the original state C.

(a) Write down the labelled transition systems of the vending machine and the customer, either by giving the sets of transitions, or by drawing the corresponding graphs. **[2 marks]**

(b) Write down CSP processes that define the vending machine and the customer. **[2 marks]**

(c) Write down a CSP process CV that describes the customer interacting with the vending machine. **[2 marks]**

(d) Decide whether the process CV is deadlock free. Justify your answer. **[2 marks]**

Question 4

During 30 days of lockdown Rhian does home schooling which means that, unlike in physical schooling, she can do her tasks in any order.

Rhian has to do five tasks every day: Maths (m), reading (r), spelling (s), art a and exercising (e).

Describe Rhian's activities during lockdown as a CSP process. After lockdown has ended the process shall successfully terminate. For simplicity we ignore weekends.

Minor syntax errors will not be penalised.

[9 marks]

Question 5

In the labs, we modelled an authentication protocol which is usually described in brief by the following rules:

(1) $A \longrightarrow B : \{\mathrm{N}_A, A\}_{\mathrm{pk}_B}$

(2) $B \longrightarrow A : \{\mathrm{N}_A, \mathrm{N}_B\}_{\mathrm{pk}_A}$

(3) $A \longrightarrow B : \{\mathrm{N}_B\}_{\mathrm{pk}_B}$

(a) Referring to the description above, explain this protocol. What is the purpose of the protocol? Which cryptographic mechanism is it based on?

[2 marks]

(b) Describe an attack on this protocol using a similar style of rules as above.

[2 marks]

(c) Describe how the protocol can be amended to prevent this attack.

[1 mark]

(d) We modelled the amended protocol by a process `System(t)`, specified its correctness by a process `SPEC`, and checked its correctness by a suitable assertion:

```
SYSTEM(t) = ENV(t) [| {| send, receive |} |] USERS

SPEC = know ? n : noncesI -> SPEC

assert SPEC [T= System(20) \ {| send, receive |}
```

In the following, 'explain' means giving an informal explanation showing an understanding of the modelling.

(i) Explain what the process `System(t)` means (describe its components and explain the way they are connected).

(ii) Explain what the assertion means. Explain all parts of it, in particular, explain the meaning of `\ {| send, receive |}` and why this part is necessary.

(iii) Explain which correctness guarantees the successful model checking of this assertion provides for the protocol.

[6 marks (2 marks each)]

Question 6

(a) Describe the main elements of program extraction from constructive proofs. Your description should include

- an explanation of the difference between constructive and classical logic;
- at least two examples illustrating the correspondence between formulas and proof rules on the one hand and types and program constructs on the other hand.

[3 marks]

(b) Suppose one has proven constructively the following formula (where the variables n, m range over natural numbers):

$$\forall n\, \exists m\, (m^2 \leq n < (m+1)^2)$$

(i) Give an informal description what the extracted program computes?

(ii) What result would the extracted program return when run with the number 10 as input?

[3 marks].

End of Paper