CSSE3100/7100 Reasoning about Programs Semester 1, 2017

Assignment 1: Background theory

Course coordinator: Graeme Smith **Due: 5pm, Thu 23 March**

The purpose of this assignment is to strengthen your understanding of the required background theory before we move on to techniques for verifying programs and deriving programs that are correct.

Answer each of the following questions. A single pdf file with your answers should be submitted to the Blackboard site by the due date.

1. Consider the following specification:

   $y : [x \neq 0, y = y_0/x]$

   (a) Write a new specification that divides y by x if x is non-zero, and sets y to 0 if x is 0.

   (b) Revise your specification from part (a) so that when x is 0 the specification does not choose any particular final value for y, but still terminates.

   (c) Explain *informally* (i.e., in English) the refinement relations that hold between the three specifications, the original one above and those from parts (a) and (b). Consider the perspective of the user of the specified program in your explanation.

2. Refine the following specification to a sequential composition of two assignments, neither of which uses the operation ‘raise to the fourth power’:

   $x, y : [\text{true}, x = z^2 \wedge y = z^4]$

3. Determine an expression for the weakest precondition of each of the items of code in the following Hoare triples with respect to the indicated postcondition. Use your result to argue *formally* either that the Hoare triple is a true or false, or that there is not enough information to determine its truth value.

   (a) $\{y < 10\}$ **if** $(x > 0 \vee y < 10) \rightarrow y := 10$ **fi** $\{\text{true}\}$

   (b) $\{P\}\ x := x + y\ \{P[x \backslash (x + y)]\}$

4. In a series of steps refine $y : [y < 10, y > 0]$ to

   if $(x > 0 \vee y < 10) \rightarrow y := 10$ **fi**

   Explain why it is not possible to refine this same specification to

   if $((x > 0) \wedge (y < 10)) \rightarrow y := 10$ **fi**

5. A **repeat** command has the form

   repeat S **until** B

   It executes S first, then evaluates B. If B is true it terminates, otherwise it repeats the **repeat** command from the beginning.

   Devise a refinement rule for the **repeat** command. The rule should be simple to apply, i.e., it should have minimal side conditions to prove. In particular, the side conditions should not be other refinement proofs.

Marking

The assignment is worth 10% of your final grade. Each question is worth 2 marks giving a total of 10 marks.

A mark of zero will be given for work with little or no academic merit.

Late submission

The submission of this assignment by the due date is the sole responsibility of the student. Students should not leave assignment preparation until the last minute and must plan their workloads to meet the deadline. It is your responsibility to manage your time effectively.

Assessment items received after the due date will receive a mark of zero unless you have been approved to submit the assessment item after the due date as set out in the Electronic Course Profile.

School Policy on Student Misconduct

You are required to read and understand the School Statement on Misconduct, available on the School's website at:

http://www.itee.uq.edu.au/itee-student-misconduct-including-plagiarism