CSSE3100/7100 Reasoning about Programs Semester 1, 2017

Assignment 2: Verification

Course coordinator: Graeme Smith **Due: 5pm, Thu 13 April**

The purpose of this assignment is to apply techniques for verifying programs to a moderately complex program.

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

Part A (all students must do this part)

You have been asked to write a program to find the intersection of three integer sets. Each set is implemented as a sorted integer array (possibly empty). Your friend suggests the program below, in which the three sets are stored in arrays A, B and C, and their intersection in the array D.

$i, j, k, r := 0, 0, 0, 0;$
do $(i \neq A.\text{len} \vee j \neq B.\text{len} \vee k \neq C.\text{len}) \rightarrow$
  if $(A_i > B_j) \rightarrow j := j + 1$
  $[\!]$ $(B_j > C_k) \rightarrow k := k + 1$
  $[\!]$ $(C_k > A_i) \rightarrow i := i + 1$
  $[\!]$ $((A_i = B_j) \wedge (B_j = C_k)) \rightarrow i, j, k, r, D_r := i + 1, j + 1, k + 1, r + 1, A_i$
  fi
od

Assuming that D.len is large enough to store the intersection, i.e., $D.\text{len} \geq max(\{A.\text{len}, B.\text{len}, C.\text{len}\})$, use refinement to prove whether or not the above program is correct. If it is not correct then propose and informally justify a modification to the program that you believe would correct the error. You are not required to formally verify your modified program.

Your proof(s) should include all refinements steps and *semi-formal* proofs justifying each side condition, i.e., proofs similar to those in the lectures are sufficient for the side conditions (if a side condition proof is similar to a previous assignment proof you have provided, you may refer to the previous proof for justification). In your specification and other predicates, you may use the notation $sorted(A)$ to say that an array A is sorted, and $A \cap B$ to denote the intersection of arrays A and B. You may also use other functions provided that you define their meaning clearly.

Part B (only CSSE7100 students must do this part)

Your friend has suggested that the following rule is often more useful than the Strengthen Postcondition rule from the lectures.

If $P[w\backslash w_0] \wedge Q' \Rrightarrow Q$ then $w : [P, Q] \sqsubseteq w : [P, Q']$.

Is this rule correct? Justify your answer formally.

Marking

The assignment is worth 20% of your final grade.

For CSSE3100 students, Part A is worth 20 marks. 4 marks will be given for providing a correct specification, invariant and variant for the problem. The remaining 16 marks will be given if all required refinement steps are shown and justified, i.e., side conditions are argued to hold. CSSE3100 students do **not** need to do Part B.

For CSSE7100 students, Part A is worth 16 marks. 4 marks will be given for providing a correct specification, invariant and variant for the problem. The remaining 12 marks will be given if all required refinement steps are shown and justified, i.e., side conditions are argued to hold. Part B is worth 4 marks. Full marks will be given for a formal proof that the rule is correct, or a counter-example showing that it is incorrect.

For **all** students, 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