CSSE4630 Semester Two Final Examination 2020 (PART B [70%])

Question 1 [30 marks total] We want to implement a static analysis for checking that every local variable is initialised before it is used. We choose as abstract state lattice the (inverse) powerset of variables (Vars) occurring in the given program, ordered by the superset relation. So we have:

$$\begin{aligned} \bot &= \mathit{Vars} \\ \top &= \{\} \\ s \sqcup t &= s \cap t \end{aligned}$$

Here are the constraint rules for this static analysis. For a control-flow-graph (CFG) node v of the form:

$$\begin{aligned} [\![X = E]\!] &= \mathit{JOIN}(v) \cup \{X\} \\ [\![\mathit{var}\ X_1, \ldots, X_n]\!] &= \mathit{JOIN}(v) \setminus \{X_1, \ldots, X_n\} \end{aligned}$$

and for all other CFG nodes we have just $[\![v]\!] = \mathit{JOIN}(v)$. Note that $\mathit{JOIN}(v) = \bigsqcup_{w \in \mathit{pred}(v)} [\![w]\!]$, where $\mathit{pred}(v)$ is the set of predecessor nodes of v in the CFG.

Using the results from initialised variables analysis, a programming error detection tool could now emit warnings for usages of possibly-uninitialised variables.

In this question you will analyse the following simple TIP function to show that a warning would be emitted at the return statement. You can assume that the input y is initialised by the caller.

```
f(y) {
    var x;
    if (y > 0) {
        x = 1 - y;
    }
    output 1 - y;
    return x;
}
```

a. **[8 marks]** Write all the constraints generated for each of the six nodes of the CFG for the function (including the ENTRY node).

b. **[6 marks]** Solve those constraints and write the final solution for each node.

c. **[3 marks]** Explain the general conditions that would cause this analysis tool to generate a warning for an expression E at a node v.

d. **[3 marks]** For the above example program, use the results of your analysis to explain why a warning would be emitted at the return statement.

e. **[6 marks]** Write a TIP program where this initialised-variables error detection tool would emit a spurious warning. That is, a program in which there are no reads from uninitialised variables in any execution, but the initialised variables analysis is too imprecise to show it.

f. **[4 marks]** Suggest some ways in which the precision of the analysis might be improved, in order to reduce the likelihood of such spurious warnings.

CONTINUED

Question 2 [20 marks total] An alternative way to formulate initialised variables analysis would be to use the following map lattice instead of the powerset lattice:

$$\mathit{States} = \mathit{Vars} \to \mathit{Init}$$

where Init is a lattice with two elements $\{\mathit{Initialised}, \mathit{NotIninitialised}\}$ (you can abbreviate these to I and N, respectively). A warning will be generated at a read of a variable x if the abstract analysis state maps x to N.

a. **[4 marks]** How should we order the two elements? That is, which one is top and which one is bottom? Draw the Init lattice as a Hasse diagram.

b. **[8 marks]** Write out the evaluation tables for the greatest lower bound (⊓) and least upper bound (⊔) operators. For example:

⊓	I	N
I	?	?
N	?	?

⊔	I	N
I	?	?
N	?	?

c. **[4 marks]** The constraint rules for assignment and variable declarations must be modified to fit with this alternative lattice. Write the new assignment rule.

d. **[4 marks]** Write the new variable declaration rule.

Question 3 [20 marks total] Recall that concolic testing uses a mixture of concrete and symbolic execution of a program.

a. **[8 marks]** Explain the goal of concolic testing, and give a brief overview of how it works (2-3 sentences).

b. **[12 marks]** Use concolic testing to test the following TIP function, starting with inputs $x = 0, y = 0$. Write down the sequence (or tree) of test cases that it would find. State clearly each time you invoke the SMT solver, showing the inputs to the SMT solver, and the outputs that it returns.

```
testme(x, y) {
  var z;
  z = 2 * y + 1;
  if ((x + y) > 10) {
    if (z == x) {
      error 17;
    }
    error 13;
  }
  return z;
}
```

Question 4 [0 marks] Please use this space to specify any assumptions you have made in completing the exam and which questions those assumptions relate to. You may also include queries you may have made with respect to a particular question, should you have been able to 'raise your hand' in an examination room.

END OF PART B OF EXAMINATION