Assignment 3 (Written): Dataflow Analysis Correctness

17-819M: Program Analysis
Jonathan Aldrich (jonathan.aldrich@cs.cmu.edu)

100 points total

Turn in a file to the Blackboard dropbox in PDF or Word format.

Assignment Objectives:

- Prove a simple dataflow analysis correct, and demonstrate the problem with an incorrect dataflow analysis.

1 Local Soundness (25 points)

Consider the following hypothetical flow function for sign analysis:

$$f_{\text{SA}}(\sigma,\ x{=}y{+}z) = [x \mapsto +]\sigma$$

This flow function is "obviously" incorrect. However, to prove that it is incorrect, you must show that it violates the criterion of local soundness defined in class. That is, you must find an environment η and a statement S such that $\eta \mapsto_S \eta'$ (executing S on the memory η yields new memory values η') and $\alpha_{\text{SA}}(\eta') \not\sqsubseteq f_{\text{SA}}(\sigma, S)$ with $\sigma = \alpha_{\text{SA}}(\eta)$. You may assume the less precise lattice from Question 1.2 in the last assignment.

Question 1.1 (5 points).

Define α_{SA} for sign analysis.

Question 1.2 (5 points).

Find a pair of η and S that illustrates the local unsoundness. What are η and S?

Question 1.3 (2 points).

What is $\sigma = \alpha_{\text{SA}}(\eta)$?

Question 1.4 (3 points).

If $\eta \mapsto_S \eta'$, what is η'?

Question 1.5 (2 points).

What is $\alpha_{\text{SA}}(\eta')$?

Question 1.6 (4 points).

What is $\sigma' = f_{\text{SA}}(\sigma, S)$?

Question 1.7 (4 points).

Show that $\alpha_{\text{SA}}(\eta') \not\sqsubseteq \sigma'$

2 Analysis Correctness (75 points)

Question 2 (20 points).

Define a correct flow sign analysis function for addition. Also define flow functions for copy, constant assignment, jump and branch_nz. Your definitions should assume ideal integer arithmetic. They should be precise, but the rule for the branch_nz need not be flow sensitive.

Question 3 (20 points).

Show (i.e. prove) that your flow functions are monotonic.

Question 4 (5 points).

Give the height of the dataflow lattice that maps each variable to one of the simple lattice elements from question 1.2 in the previous assignment. The height should be expressed in terms of v, the number of variables in scope. Briefly justify your answer.

Note that together with the monotonicity of your flow functions, termination of your analysis is guaranteed.

Question 4 (30 points).

Prove that your flow functions are locally sound with respect to the semantics given in class.