Assignment 3 (Written): Dataflow Analysis

15-819O: Program Analysis
Jonathan Aldrich
jonathan.aldrich@cs.cmu.edu

Due: Monday, February 11, 2013 (11:59 pm)

100 points total

Turn in a PDF file electronically via Blackboard for Assignment 3. The file should contain the answers to the questions below. At the top of the document, state your name and andrew ID.

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:

$$f[\![x := y + z]\!](\sigma) = [x \mapsto +]\sigma$$

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 a program configuration E, n and an instruction I such that $P \vdash E, n \rightsquigarrow E', n'$ (where $P(n) = I$) and $\alpha(E', n') \not\sqsubseteq f[\![I]\!](\sigma)$ with $\sigma = \alpha(E, n)$. For simplification, we will ignore n as an argument to α as it is not relevant for this analysis. You may assume the less precise lattice from Question 2 in the first assignment.

Question 1.1 (5 points).

Define $\alpha(E)$ for sign analysis.

Question 1.2 (5 points).

Find a pair of E and I that illustrates the local unsoundness. What are E and I?

Question 1.3 (2 points).

What is $\sigma = \alpha(E)$?

Question 1.4 (3 points).

If $P \vdash E, n \rightsquigarrow E', n'$, what is E', n'?

Question 1.5 (2 points).

What is $\alpha(E')$?

Question 1.6 (4 points).

What is $\sigma' = f[\![I]\!](\sigma)$?

Question 1.7 (4 points).

Show that $\alpha(E') \not\sqsubseteq \sigma'$

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, and (unconditional) jump. Your definitions should assume ideal integer arithmetic. They should be precise.

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 2 in the first assignment. The height should be expressed in terms of $|Var|$, 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 5 (30 points).

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