Homework 5: Analysis Correctness

17-355/17-665/17-819O: Program Analysis
Claire Le Goues and Jonathan Aldrich
clegoues@cs.cmu.edu, aldrich@cs.cmu.edu

Due: Thursday, February 22, 2018 11:59 pm

100 points total

Assignment Objectives:

- Prove a simple analysis correct; demonstrate the problem with an incorrect analysis.
- Gain experience with proof techniques over dataflow frameworks

Handin Instructions. Please submit your assignment on Canvas as a **PDF** by the due date. Name it **[your-andrew-id]-hw5.pdf**.

Proofs of correctness

Question 1, Unsoundness, *(25 points).* Consider the following hypothetical flow function for the simple sign analysis introduced in Homework 3 for WHILE3ADDR:

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

This flow function is "obviously" incorrect. However, to prove this, you must show that it violates the criterion of local soundness. 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. You may assume the less precise lattice from Question 2 in Homework 3.

a) Define $\alpha(E)$ for sign analysis. *(5 points)*
b) Find an example E and I illustrating the local unsoundness. What are E and I? *(5 points)*
c) What is $\sigma = \alpha(E)$? *(2 points)*
d) If $P \vdash E, n \rightsquigarrow E', n'$, what is E', n'? *(3 points)*
e) What is $\alpha(E')$? *(2 points)*
f) What is $\sigma' = f[\![I]\!](\sigma)$? *(4 points)*
g) Show that $\alpha(E') \not\sqsubseteq \sigma'$ *(4 points)*

Question 2, Flow functions, *(15 points).* Define a correct flow sign analysis function for addition in WHILE3ADDR, and then also define flow functions for copy, constant assignment, and (unconditional) jump. Assume ideal integer arithmetic. Your functions should be precise.

Question 3, Soundness, *(60 points).*

(a) Prove that your flow functions are monotonic. (25 points)

(b) Give the height of the dataflow lattice that maps each variable to one of the simple lattice elements from Question 2 in Homework 3. The height should be expressed in terms of $|Var|$, the number of variables in scope. Briefly justify your answer. (5 points)[1]

(c) Prove that your flow functions are locally sound with respect to the semantics for WHILE3ADDR. (30 points)

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