Homework 4: Analysis Correctness

17-355/17-665/17-819: Program Analysis
Claire Le Goues*
clegoues@cs.cmu.edu

Due: Tuesday, February 18, 2029 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 *(5 points).* Submit your assignment through the Gradescope link on Canvas (supports PDF and jpgs/photos) by the due date. When submitting, indicate which pages of the PDF correspond to each homework question. Putting page breaks between questions makes this simpler. Typesetting is not required, but is strongly suggested; you may submit photos or scans of handwritten answers, but they must be clear and legible.

Proofs of correctness

Question 1, Unsoundness, *(20 points).* You implemented a simple sign analysis for WHILE3ADDRfor Homework 3. Recall that we also outlined a more precise sign analysis together in class, which tracks whether a value is less than zero (LT), greater than zero (GT), equal to zero (EQ), greater than or equal to zero (GE), less than or equal to zero (LE), non-zero (NZ), or unknown ($\top$).

Consider the following hypothetical but obviously incorrect flow function for the more precise sign analysis:

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

Prove that this function violates the criterion of local soundness (that is, there exists some 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 $\sigma = \alpha(E, n)$).

a) Define $\alpha(E)$[1] for this more precise sign analysis. *(5 points)*
b) Give an example E and I illustrating the local unsoundness. *(5 points)*
c) What is $\sigma = \alpha(E)$? *(1 points)*
d) If $P \vdash E, n \rightsquigarrow E', n'$, what is E', n'? *(2 points)*
e) What is $\alpha(E')$? *(1 points)*

*This homework was developed together with Jonathan Aldrich

[1]Note that for simplicity we continue to ignore n as an argument to α, as it is not relevant.

f) What is $\sigma' = f[\![I]\!](\sigma)$? *(3 points)*
g) Show that $\alpha(E') \not\sqsubseteq \sigma'$ *(3 points)*

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

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

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

(b) Give the height of the dataflow lattice mapping each variable to one of the lattice elements for the more precise sign analysis. The height should be expressed in terms of $|Var|$, the number of variables in scope. Briefly justify your answer. (5 points)[2]

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

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