Homework 4: Analysis Correctness

17-355/17-665/17-819: Program Analysis
Rohan Padhye

Due: Thursday, February 17, 2022 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. 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, *(15 points).* You implemented a simple sign analysis for WHILE3ADDR for Homework 3. Now, consider the following hypothetical but obviously incorrect flow function for simple sign analysis:

$$f[\![x := a + b]\!](\sigma) = \sigma[x \mapsto \text{Pos}]$$

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 $P \vdash \langle E, n\rangle \rightsquigarrow \langle E', n'\rangle$ (where $P(n) = I$) and $\alpha(E') \not\sqsubseteq f[\![I]\!](\sigma)$ where $\sigma = \alpha(E)$) [1].

a) Give an example E and I illustrating the local unsoundness. *(5 points)*
b) What is $\sigma = \alpha(E)$? *(1 points)*
c) If $P \vdash \langle E, n\rangle \rightsquigarrow \langle E', n'\rangle$, what is $\langle E', n'\rangle$? *(2 points)*
d) What is $\alpha(E')$? *(1 points)*
e) What is $\sigma' = f[\![I]\!](\sigma)$? *(3 points)*
f) Show that $\alpha(E') \not\sqsubseteq \sigma'$ *(3 points)*

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

Question 2, Flow function, *(5 points).* Define a sound flow function for addition ($x := a + b$). Assume ideal integer arithmetic. You can lookup your implementation in HW3 if you want to use the same one.

Hint: Consider structuring your flow function in a similar manner to the example provided for multiplication in the parity analysis from recitation. This will help minimize the number of cases you will need to prove in the next question.

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

(a) Prove that your flow function (from Q2) is monotonic. *(20 points)*

(b) Give the height of the "lifted" dataflow lattice which maps each variable to one of the lattice elements for sign analysis (i.e, the set of all σ values of the form $Var \rightarrow L$). The height should be expressed in terms of $|Var|$, the number of variables in scope. Briefly justify your answer. *(15 points)*

(c) Prove that your flow function (from Q2) is locally sound with respect to the semantics for WHILE3ADDR. *(25 points)*

Question 4, Precision, *(20 points).*

Recall that a flow function is distributive iff $f(\sigma_1) \sqcup f(\sigma_2) = f(\sigma_1 \sqcup \sigma_2)$ always holds true. Is your flow function for addition as defined in Q2 distributive over $\sqcup$? If yes, prove it (hint: it will be similar to the proof of monotonicity). If no, demonstrate a violation of the distributive law by giving appropriate values for σ_1, σ_2, and showing that:

$$f[\![x := a + b]\!](\sigma_1) \sqcup f[\![x := a + b]\!](\sigma_2) \sqsubseteq f[\![x := a + b]\!](\sigma_1 \sqcup \sigma_2)$$

(20 points)