

CS4120/4121/5120/5121—Spring 2018

Homework 4

Program Analysis

Due: Wednesday, April 18, 11:59PM

0 Updates

- None yet; watch this space.

1 Instructions

1.1 Partners

You may work alone or with *one* partner on this assignment. But remember that the course staff is happy to help with problems you run into. Use Piazza for questions, attend office hours, or set up meetings with any course staff member for help.

1.2 Homework structure

All problems are required of all students.

1.3 Tips

You may find the Dot and Graphviz packages helpful for drawing graphs. You can get these packages for multiple OSes from the [Graphviz download page](#).

2 Problems

1. Preventing the billion-dollar mistake

Accesses to null pointers are a frequent source of bugs and security vulnerabilities. To protect against these accesses, one option is to rely on hardware memory protection to prevent these accesses, but that protection is probably not available on embedded platforms. In this problem, you will design a dataflow analysis that ensures memory accesses do not go to memory address zero, by conservatively computing the set of expressions at each program point that can evaluate to zero. Accesses to memory location $[e]$ can then be prevented at a program point where e might be zero.

- What is the top element \top for this dataflow analysis?
- Define the ordering and the meet operator for elements in this lattice (including \top).
- Give dataflow equations for this analysis for each of the possible kinds of IR nodes. Recall that we had five IR node types: $x = e$, $[e_1] = e_2$, **if** e , **start**, **return** e . For simplicity, we will use a simpler syntax in which expressions can only occur as right-hand side of an

assignment to a variable: $x = e$, $[x_1] = x_2$, **if** x , **start**, **return** x where e can only take the forms n (constant), x , $x_1 + x_2$, and $[x]$.

Also, note that this is an analysis where, as with sparse conditional constant propagation, it is sometimes helpful to propagate different information along different exiting edges from an **if** node.

2. Defending against zombies with dataflow analysis

Let us define “undead” code as code that depends on a variable that is *always* uninitialized. When such undead code is removed, additional program regions may become undead due to the disappearance of variable declarations. The goal of this exercise is to remove all undead code from a function using only a single analysis pass. No variables will be assumed to be live-in at the start of the CFG.

- Design a dataflow analysis that can be used for cascading undead-code removal. Describe its ordering, the meet operator, the top element, as well as the flow function. Where necessary, be conservative. You only need to specify the flow function for assignments $x = expr$.
- Show that the flow functions you defined are monotonic, and either show that they are distributive or construct a counterexample.
- Show that one run of your analysis leads to the removal of the following grayed-out undead code (remember that meets are used at merge points in the CFG):

```
1 a = 1
2 if (f(a) > 0) {
3   c = c+1
4   d = 5
5 }
6 [d] = a+c
7 g = a+d
```

3. Control-flow analysis

For the control-flow graph in Figure 1, give the dominator tree, with back edges added as dashed edges. Identify the natural loops and the control tree, and for each loop in the control tree, indicate its set of nodes, its header node, and its exit edges.

3 Submission

Submit your solution as a PDF file on CMS. This file should contain your name, your NetID, all known issues you have with your solution, and the names of anyone with whom you have discussed the homework.

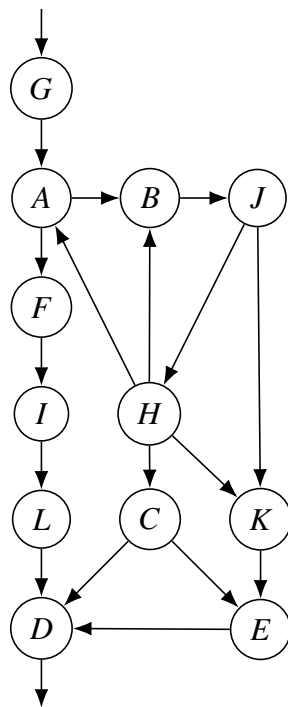


Figure 1: The control-flow graph for Problem 3