Assignment 1: Logically Safe
15-316 Software Foundations of Security and Privacy

Due: **11:59pm**, Tuesday 9/10/19
Total Points: 50

1. **Proof practice (10 points).** Conduct a proof in the propositional sequent calculus that the following formula is valid. Be sure to say which proof rules apply at each step, and only apply proof rules without making undocumented simplifications along the way. If your proof tree grows wider than the page, you may find it helpful to break into sub-trees, but please clearly label them so that we know where they should go!

$$((F \to G) \land (H \to I) \land (\neg G \lor \neg I)) \to (\neg F \lor \neg H)$$

Solution.

2. **Propositional soundness (10 points).** Use the semantics of $\neg$ to prove that the $\neg$R rule is sound by showing that the validity of the premises imply the validity of the conclusion.

$$(\neg\mathrm{R})\ \ \frac{\Gamma, P \vdash \Delta}{\Gamma \vdash \neg P, \Delta}$$

Solution.

3. **Missing assumptions (10 points)** Find a non-trivial (i.e., not $\bot$) assumption $\boldsymbol{\Gamma}$ sufficient to complete the following proof, and complete it.

$$\boldsymbol{\Gamma} \vdash [x := 7 * x + 1; \texttt{while}(x \geqslant 19)\,\{x := x - 19\}]x = 3$$

Note that it may help to first try completing the proof, and see how far you can get. Your partial proof may guide you directly to the correct assumption, but try to reduce your effort by finding a condition that causes the loop to execute as few times as possible.

Solution.

4. **Conditional assignments (10 points)** When rummaging through the syntax manual of other imperative programming language and comparing them to the while language considered in class, a clever student found that we totally neglected his favorite feature of conditional assignments. Indeed, the conditional assignment $x := Q\,?\,e1 \,:\, e2$ that assigns term $e1$ to variable x if formula Q is true and otherwise assigns term $e2$ to x is missing. Your job is to define a semantics $[\![x := Q\,?\,e1 \,:\, e2]\!]$ for the conditional assignment $x := Q\,?\,e1 \,:\, e2$ as the set of all pairs of initial and final states of running $x := Q\,?\,e1 \,:\, e2$. After having done so, your next task is to design a sound axiom for it:

$$([:=?:]) \quad [x := Q\,?\,e1 \,:\, e2]p(x) \leftrightarrow \ldots$$

Solution.

5. **Now prove it! (10 points).** Use the semantics from part 4 to prove that your axiom is sound, i.e., that it is a valid formula of dynamic logic.

   Solution.