Assignment 2: Program it Out
15-414/15-424 Bug Catching: Automated Program Verification

Due: **11:59pm**, Tuesday, February 4
Total Points: 50

1. **Find the precondition (10 points)** Consider the following program.

$$\alpha \equiv x := x + 1; ?(x > 0); y := y + x$$

Your job is to find a precondition P that makes the following DL formula valid, and prove that this is the case using the axioms introduced in lecture.

$$P \rightarrow [\alpha](x + 2y \geq 3)$$

Be sure to explain how you arrived at your precondition. *Hint: can you use the axioms directly to figure out the precondition, and reuse your work for the proof?*

2. **Not so fast... (15 points)** In the notes for Lecture 2, we somewhat casually concluded that the following two contracts for the `gcd` program were equivalent.

$$[\texttt{gcd}]\texttt{postdiv} \land [\texttt{gcd}]\texttt{postgrt}$$
$$[\texttt{gcd}](\texttt{postdiv} \land \texttt{postgrt})$$

Justify our conclusion by showing that the box modality distributes across conjunction. That is, use the semantics of DL to prove that the following formula is valid.

$$[\alpha]P \land [\alpha]Q \leftrightarrow [\alpha](P \land Q)$$

3. **Distributing disjunction (5 points)** Unfortunately, the box does not necessarily distribute over disjunction. In particular, if we extend our language with a command that assigns an arbitrary value to a variable, as shown in the following semantics, then distributivity may not hold.

$$[\![x := *]\!] = \{(\omega, \nu) : \text{for all variables } y \text{ except } x, \nu[\![y]\!] = \omega[\![y]\!]\}$$

That is, the only possible difference between the initial and final states after running $x := *$ is in $\nu[\![x]\!]$; it need not be equal to $\omega[\![x]\!]$, whereas for all other variables y, $\nu[\![y]\!] = \omega[\![y]\!]$.

Give an example of a program α that makes use of this command, and a postcondition $P \land Q$, for which $[\alpha]P \lor [\alpha]Q$ is not equivalent to $[\alpha](P \lor Q)$.

4. **New axiom (5 points)** On further thought, the new command $x := *$ from the previous problem may be useful to keep around. Design an axiom that allows you to reason about box modalities around it:

$$([:=*]) \quad [x := *]p(x) \leftrightarrow \ldots$$

The right side of this equivalence should not contain a box or diamond modality, but only first-order formulas.

5. **Prove it (15 points)** Show that your axiom $[:= *]$ is sound by adapting the soundness proof from $[:=]$ given in Lecture 5.