Assignment 2: Loops and Proofs
15-424/15-624 Foundations of Cyber-Physical Systems
Course TA: Sarah Loos (sloos+fcps@cs.cmu.edu)

Due: **Beginning of class**, Wednesday 9/25/13
Total Points: 60

1. **Semantic Argument.** Let A, B be dL formulas. Suppose $A \leftrightarrow B$ is valid and A is valid. Is B valid? Use the semantics to prove or disprove.

2. **Valid, Satisfiable, or Unsatisfiable.** For each of the following dL formulas, determine if they are valid, satisfiable, and/or unsatisfiable. In the case where a problem contains an unspecified formula or hybrid program (for example ϕ, H, or α), then it is satisfiable only if it is satisfiable for all choices of the unspecified formulas and programs.

   (a) $[?false]false$
   (b) $[(?false)^*]false$
   (c) $[\{x' = 1 \ \& \ false\}]false$
   (d) $[(\{x' = 1 \ \& \ false\})^*]false$
   (e) $[\{x' = 1 \ \& \ true\}]\phi \leftrightarrow [\{x' = 1\}]\phi$ (where ϕ is any dL formula)
   (f) $[\{x' = 1 \ \& \ H\}]\phi \leftrightarrow [?H]\phi$ (where ϕ and H are any dL formulas)
   (g) $[\{x' = v, v' = 1 \ \& \ x \leq 10\}]\phi \leftrightarrow [\{x' = v, v' = 1\}; ?x \leq 10]\phi$
   (h) $[\alpha]true$ (where α can be any HP)
   (i) $[\alpha]false$ (where α can be any HP)
   (j) $[\alpha; ?H]H$ (where α can be any HP and H any dL formula)
   (k) $[t := 0; \ \{t' = 1 \ \& \ t \leq 10\}; ?t = 10](t = 10)$
   (l) $[t := 50; \{t' = 1 \ \& \ t \leq 10\}; ?t = 10](t = 10)$

3. **Looping and Diamonds.** Consider the following HP α.

$$\begin{aligned}\alpha \equiv (&t := 0; \\ &(v := 1 \cup (?h \geq 0; v := -1/3) \cup (?h \geq 0; v := -3/4)); \\ &\{h' = v, t' = 1 \ \& \ t \leq 1\}; \\ &?(t = 1))^*\end{aligned}$$

   (a) Recall that the diamond modality $\langle\alpha\rangle\phi$ holds if there exists at least one run of HP α such that ϕ holds. Assuming $h = 0$ initially, give a trace of HP α (i.e. a sequence of state values between transitions) such that the post condition $h = \frac{-5}{12}$ holds. (Hint: there is a solution which executes the loop at most four times.)
   (b) Is the dL formula $h = 0 \rightarrow \langle\alpha\rangle(h = \frac{-5}{12})$ valid? Explain.
   (c) Is the dL formula $h = 0 \rightarrow [\alpha](h = \frac{-5}{12})$ valid? Explain.

4. **Practice with hybrid programs.**

   (a) Nondeterministic Evolution: Rewrite the dL formula $[x' = 0 \ \& \ H]\phi$ as an equivalent formula which does not use nondeterministic evolution.

(b) While Loop: The C0 programming language, introduced in 15-122 Principles of Imperative Computation, allows programmers to define contracts which must be satisfied. The `@requires` contract defines initial conditions which must be met, while the `@ensures` contract defines a final condition the program must satisfy. The semantics of C0 are as expected and can be found online.
Translate this while loop in C0 to an equivalent hybrid program. Then create a dℒ formula using the HP that proves the contracts are satisfied. Since HPs don't have return statements, just ensure that the value of variable `res` is correct at the end of the HP. Hint: remember nondeterminism.

```
int exp (int k, int n)
//@requires n >= 0;
//@ensures \result >= 1;
//@ensures \result > n;
{ int res = 1; int i = 0;
  while (i < n) {
    res = res * k;
    i = i + 1;
  }
  return res;
}
```

5. **Soundness.** Give a proof of soundness for the test axiom ([?]): $[?H]\phi \leftrightarrow (H \rightarrow \phi)$
Hint: Use the semantics of hybrid programs and dℒ formulas.

6. **Practice with Proof Rules.** In each of the following, fill in the missing parts to give an instantiation of a given proof rule. In some cases, the name of the most appropriate proof rule to use is not given, and is left to you to fill it in. In each case, make sure that your instantiation is not only syntactically correct, but that the instantiation you chose makes it possible to prove the property.

$$\texttt{cut}\ \frac{(PART\ A) \qquad (PART\ B)}{(x \geq y \wedge z \geq 0) \vdash [x := x+1][y := y+1]x \geq y}$$

$$\texttt{hide left (aka Weakening or Wl)}\ \frac{(PART\ C)}{(x > y \wedge z \geq 0) \vdash [(x := x+1; y := y+1)]x > y}$$

$$(PART\ D)\ \frac{(PART\ E) \vdash v = 0}{(\forall h.2gh = 2gH - v^2) \vdash v = 0}$$

$$\texttt{loop invariant}\ \frac{(PART\ F) \qquad (PART\ G) \qquad (PART\ H)}{F \vdash [\alpha^*]G}$$

$$\texttt{loop invariant}\ \frac{(PART\ I) \qquad (PART\ J) \qquad (PART\ K)}{x < station \wedge B > 0 \wedge b > 0 \wedge b < B \wedge (PART\ L)}$$
$$\vdash [((a := -B \cup a := -b); x' = v, v' = a\ \&\ v \geq 0)^*](x \leq station)$$

7. **Write a Proof.** Using the proof rules you learned in class, construct a full proof for the dℒ formula. For your convenience, you can download a tex template here with the first rule application already filled in for you.
$$x \geq 1 \rightarrow [((v := 1 \cup v := 2); \{x' = v\ \&\ x \geq -1\})^*](x \geq 0)$$