Assignment 3: Proofs, Diamonds, and Differential Invariants
15-424/15-624 Foundations of Cyber-Physical Systems
Course TA: Sarah Loos (sloos+fcps@cs.cmu.edu)

Due: **Beginning of class**, Monday 10/7/13
Total Points: 60

1. **Diamond Axioms.** Complete the following proof rules for the diamond properties. Then prove that each of your rules is sound using a semantic argument.

$$(\langle{:=}\rangle)\ \frac{\ldots}{\vdash \langle x := \theta\rangle\phi} \qquad (\langle\cup\rangle)\ \frac{\ldots}{\vdash \langle \alpha \cup \beta\rangle\phi} \qquad (\langle ?\rangle)\ \frac{\ldots}{\vdash \langle ?H\rangle\phi}$$

2. **Composed Proof Rules.** We don't always have to prove soundness of a new proof rule by referring back to the semantics. Sometimes, what looks like a new proof rule can actually be proved by composing existing rules. Prove soundness for the following new proof rules by using a sequent proof to show they are just a composition of existing rules.

$$(R3.1)\ \frac{H \vdash [\alpha]\phi \qquad \vdash [\beta]\phi}{\vdash [(?H;\alpha) \cup \beta]\phi}$$

$$(R3.2)\ \frac{A \vdash B \qquad A \vdash [\alpha]E \qquad E \vdash [\alpha^*]B}{A \vdash [\alpha^*]B}$$

$$(R3.3)\ \frac{\phi, \psi(s(X_1,...,X_n), s(X_1,...,X_n)) \vdash \zeta(s(X_1,...,X_n))}{\phi \vdash \forall x\big((\forall y\ \psi(x,y)) \to \zeta(x)\big)}$$

Where s is a new (Skolem) function symbol and $X_1,..,X_n$ are all free logical variables of the original formula.

3. **Write a Proof.** Using the sequent proof rules you learned in class, construct a full proof for the $\mathsf{d}\mathcal{L}$ formula here.

$$(0 < b < B \wedge p \leq m \wedge v = 0) \\ \to [((a := -B \cup a := -b); \{p' = v, v' = a \ \&\ v \geq 0\})^*]p \leq m$$

For your convenience, you can download a tex template here with the first rule application already filled in for you.

4. **Easy as π.** In class we have started looking at some more interesting differential equations with curved motion. Use this new knowledge to create a hybrid program which has no transcendental literals or functions (example π, e, sin, cos), but at the end of execution has the exact value of π in a variable named pi. Does this mean that we can now use π in hybrid programs? If so, should we? Explain.

5. **Practice Using Differential Invariants.** Prove each of the following statements using a differential invariant and any other proof rules presented in class that are needed to prove the property.

   (a) $x^2 + 2xy + y^2 = 0 \rightarrow [\{x' = -10, y' = 10\}]x^2 + 2xy + y^2 = 0$

   (b) $x^3 + y^3 = 0 \rightarrow [\{x' = y^2, y' = -x^2\}]x^3 + y^3 = 0$

   (c) $x^2 + y^2 = 1 \rightarrow [\{x' = y, y' = -x\}]x^2 + y^2 = 1$