Assignment 3: Proofs, Diamonds, and Differential Invariants
15-424/15-624 Foundations of Cyber-Physical Systems
Course TAs: João Martins (jmartins@cs), Annika Peterson (apeterso@andrew)

Due: **Beginning of class**, Monday 10/6/14
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.

$$(\langle ; \rangle)\ \dfrac{\ldots}{\vdash \langle \alpha; \beta \rangle \phi} \qquad (\langle ? \rangle)\ \dfrac{\ldots}{\vdash \langle ?H \rangle \phi} \qquad (\langle *^n \rangle unwind)\ \dfrac{\ldots}{\vdash \langle \alpha^* \rangle \phi}$$

Hint: proof rules prove a little differently than axioms. For an axiom $\phi \leftrightarrow \psi$, we had to show that for any state ν, $\nu \models \phi \leftrightarrow \psi$. This means that ϕ and ψ agree to be both true or both false in each state. But they *can* both be false!

The soundness of a proof rule $\frac{\vdash \phi}{\vdash \psi}$ says that if the top is valid, the bottom is valid. So for proof rules, there's no possibility of ϕ or ψ being false in any state! To prove soundness of $\frac{\vdash \phi}{\vdash \psi}$, you assume that for all ν, $\nu \models \phi$. Then you try to prove that for all ν, $\nu \models \psi$. The difference is suble, but it's there! Make sure you understand it!

2. **Derived 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. We have provided the proof for R3.Ex for you.

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

$$[\cup]\ \dfrac{\wedge_r\ \dfrac{[;]\ \dfrac{[?]\ \dfrac{[\to_r]\ \dfrac{H \vdash [\alpha]\phi}{\vdash H \to [\alpha]\phi}}{\vdash [?H][\alpha]\phi}}{\vdash [?H;\alpha]\phi} \qquad \vdash [\beta]\phi}{\vdash [(?H;\alpha)]\phi \wedge [\beta]\phi}}{\vdash [(?H;\alpha) \cup \beta]\phi}$$

$$(R3.1)\ \dfrac{x > y \vdash \langle \alpha \rangle \phi, \langle \beta \rangle \phi \qquad y < 0 \vdash \langle \alpha \rangle \phi, \langle \beta \rangle \phi}{x > y \vee y < 0 \vdash \langle \alpha \cup \beta \rangle \phi}$$

$$(R3.2)\ \dfrac{\Gamma, \theta > 0 \vdash [\alpha]\phi}{\Gamma \vdash [x := \theta; ?(x > 0); \alpha]\phi}$$

$$(R3.3)\ \dfrac{\Gamma, \psi(s(X_1, ..., X_n)), Y > 0 \vdash \phi}{\Gamma, \exists x.\psi(x) \vdash \forall y > 0 \to \phi}$$

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

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. Don't forget to fill in the initial acceleration, which you've already calculated approximately a million times before! You can apply QE, but only once you've gotten rid of all the quantifiers. Please provide an informal justification for all nontrivial arithmetic. You can also split the tree, but make sure that you indicate which parts connect to which parts.

$$(\mathit{vel} > 0 \land \mathit{pos} < \mathit{station} \land t = 0 \land T > 0 \land \mathit{acc} = ?) \rightarrow$$

$$[(\mathit{pos}' = \mathit{vel}, \mathit{vel}' = \mathit{acc}, t' = 1 \ \& \ v \geq 0 \land t \leq T)^*; ?\mathit{vel} = 0]\mathit{pos} = \mathit{station}$$

For your convenience, you can download a tex template[1] 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) $xy = 0 \rightarrow [\{x' = -10xy, y' = 10y^2\}]xy = 0$

   (b) $y \neq 0 \land \frac{x}{y^2} = 1 \rightarrow [\{x' = 2x, y' = y \ \& \ y \neq 0\}]\frac{x}{y^2} = 1$

   (c) $x^4 + y^5 = 10 \rightarrow [\{x' = 10y^4, y' = -8x^3\}]x^4 + y^5 = 10$

   (d) $x + y \neq z \rightarrow [\{x' = 2x, y' = 4x, z' = 6x\}]x + y \neq z$

[1] http://symbolaris.com/course/fcps14/asst3-template.tex