Assignment 3: Proofs and Differential Invariants (Part 1)
15-424/15-624/15-824 Logical Foundations of Cyber-Physical Systems
TA: Katherine Cordwell (kcordwel@cs.cmu.edu)

Due Date: Thursday, October 10th, 11:59PM (no late days), worth 60 points
With optional checkpoint grading for the first three questions only if you submit responses to these by midnight on Friday, Oct 4

1. **Semantic soundness proofs: Loop edition.** Give a proof of soundness for the following axioms *using the semantics* of formulas and hybrid programs.

   (a) $([*;])\quad [(\alpha)^*]\phi \leftrightarrow \phi \wedge [\alpha;(\alpha)^*]\phi$

   (b) **Bonus.** $(\langle ** \rangle)\quad \langle \alpha^*;\alpha^*\rangle\phi \leftrightarrow \langle\alpha^*\rangle\phi$

2. **Practice using differential invariants.** Prove each of the following formulas using a differential invariant and any other proof rules presented in class that are needed to prove the property. Make sure to give brief justifications for the real arithmetic steps used in your proofs. You may not use the differential solution proof rules/axioms.

   (a) $x+y+z=10 \rightarrow [\{x'=-1, y'=2, z'=-1\}]x+y+z=10$

   (b) $x=0 \vee y=0 \vee z=0 \rightarrow [\{x'=-2x, y'=y, z'=z\}]xyz=0$

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

   (d) $x^4+y^5=0 \rightarrow [\{x'=10y^4, y'=-8x^3\}](x^4+y^5=0 \vee xy=12)$

   (e) $3xy-2x\neq k \rightarrow [\{x'=2kx, y'=-2ky, k'=-4kx\}]3xy-2x\neq k$

   (f) $3x^3y+2\geq 12 \rightarrow [\{x'=-12xyz, y'=36y^2z\}]3x^3y+2\geq 0$

3. **Practice using differential cuts.** Prove each of the following formulas using *differential cuts*, differential invariants and any other proof rules presented in class that are needed to prove the property. Make sure to give brief justifications for the real arithmetic steps used in your proofs. You may not use the differential solution proof rules/axioms.

   Hint: When applying the differential invariants rule, you might sometimes find that you need additional assumptions on terms. Use differential cuts to add these assumptions to your domain constraint.

   (a) $x^4+y^5=0 \wedge w=1 \rightarrow [\{x'=10y^4, y'=-8x^3, w'=x^4+y^5\}]w^{100}+25w^{92}-26=0$

   (b) $x=7 \wedge y\geq 2 \wedge z=12 \rightarrow [\{x'=3y, y'=y^4, z'=x-3\}]z\geq 3$

   (c) $x=1 \wedge y=5 \rightarrow [\{x'=x^2+1, y'=y^2xz, z'=85x^2y^3z^{15} \,\&\, z\geq 1\}]xy\geq 1$

   (d) $x\geq -1 \wedge y=1 \rightarrow [\{x'=x^2y, y'=y^2+y+1\}]x^3\geq -1$

4. **Differential axioms.** Briefly show that the following axioms for differentials are sound by giving a *semantics* proof for each axiom. Your proofs can and should take advantage of semantic definitions from lecture.

   (a) $(c())' = 0$

   (b) $(x)' = x'$

   (c) $(e \cdot f)' = (e)' \cdot f + e \cdot (f)'$

   Hint: Be careful with the notation. In part a, $c()$ is a function symbol that takes no arguments, i.e., it is a constant. In part b, $(x)'$ is the differential of the term x that is a variable, while x' is a differential symbol.

5. **Unsound differential invariant proof rules.** Differential invariants is a powerful technique for reasoning about ODEs in dL. It is crucial that their associated proof rules are sound. As we saw in lecture, the correctness of these proof rules can be very subtle. Show that the following candidate "proof rules" are unsound. Briefly explain your answer e.g., by explaining how you can derive a conclusion that is not valid.

   Hint: To show that a proof rule is unsound, find a counterexample, i.e., an instance of the rule where all the premises are valid, but the conclusion of the rule is not.

   (a) Assuming context (Γ, Δ) in inductive step.

$$\frac{\Gamma \vdash J, \Delta \qquad \Gamma, H \vdash [x' := f(x)](J)', \Delta \qquad J \vdash F}{\Gamma \vdash [\{x' = f(x) \,\&\, H\}]F, \Delta}$$

   (b) Assuming invariant inequality in inductive step.

$$\frac{\Gamma \vdash p \geq 0 \qquad p \geq 0 \vdash [x' := f(x)](p)' \geq 0}{\Gamma \vdash [\{x' = f(x)\}]p \geq 0}$$

6. **The sound of evolution domains.** The differential cut and differential weakening axioms/proof rules lets us manipulate the evolution domain constraint in proofs about differential equations. Here are a few more candidate differential equation axioms beyond those that you have encountered in class. For each unsound axiom, give a counterexample. For each sound axiom, *briefly* explain why it is sound. You do not have to give a full soundness proof.

   (a) Differential Vanilla Weakening: $[\{x' = f(x) \,\&\, H\}]H$

   (b) Differential Skip: $([\{x' = f(x) \,\&\, H\}]P) \to (H \to P)$

   (c) Self Loop: $[\{x' = f(x) \,\&\, H\}]P \leftrightarrow [(\{x' = f(x) \,\&\, H\})^*]P$

   (d) **Bonus (challenging).** Conjunctive Domains:

$$[\{x' = f(x) \,\&\, Q_1 \wedge Q_2\}]P \leftrightarrow \big([\{x' = f(x) \,\&\, Q_1\}]P \vee [\{x' = f(x) \,\&\, Q_2\}]P\big)$$