Assignment 3: Proofs and Differential Invariants (Part 1)
15-424/15-624/15-824 Foundations of Cyber-Physical Systems
Course TAs: Nathan Fulton (nathanfu@cs), Anastassia Kornilova (akornilo@andrew)

Due: **Beginning of class**, Tuesday 2/23
Total Points: 30

1. **A Differential Proof Rule.** Determine if the following proof rule is sound or unsound, then prove your conjecture using a semantic argument.

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

   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. **Differential Axioms.** Determine if the following axioms are sound or unsound, then prove your conjecture using a semantic argument.

   (a) $(x^2)' = 2xx'$
   (b) $(y^5)' = 5y^4$
   (c) $([x' = f(x) \& H]P) \rightarrow (H \rightarrow P)$
   (d) $(x)' = x'$
   (e) $(d \cdot e)' = (d)' \cdot e + d \cdot (e)'$

   Question (d) is subtle – $(x)'$ is the prime operator applied to the term x, while x' is a differential symbol.

3. **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. Do not use differential solution proof rules/axioms.

   (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) $x + y \neq z \rightarrow [\{x' = 2x, y' = 4x, z' = 6x\}]x + y \neq z$
   (e) $x \geq 0 \land y \geq 0 \rightarrow [x' = y, y' = 1](x \geq 0 \land y \geq 0)$