Assignment 3: Proofs and Differential Invariants (Part 1)
15-424/15-624/15-824 Logical Foundations of Cyber-Physical Systems

TAs: Irene Li (mengzeli@andrew.cmu.edu)
Yong Kiam Tan (yongkiat@cs.cmu.edu)

Due Date: Thursday, October 11th, 11:59PM (no late days), worth 60 points

1. **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) $xy = 0 \rightarrow [\{x' = -10xy, y' = 10y^2\}]xy = 0$
   (b) $\frac{x}{y^2} = 1 \rightarrow [\{x' = 2x, y' = y \,\&\, y \neq 0\}]\frac{x}{y^2} = 1$
   (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) $xy + x \geq 1 \rightarrow [\{x' = x^2y, y' = -xy\}]xy + x \geq 1$

2. **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) $x = 2 \wedge y = 2 \wedge z \geq 4 \rightarrow [\{x' = x^2, y' = x - 2, z' = y - 1\}]z \geq 4$
   (b) $x = 1 \wedge y = 5 \rightarrow [\{x' = x^2 + 1, y' = y^2x\}]xy \geq 1$
   (c) $x \geq -1 \wedge y = 1 \rightarrow [\{x' = x^2y, y' = y^2 + y + 1\}]x^3 \geq -1$

3. **Exploring differential ghosts.** For this question, we shall investigate an invariant for the following pair of differential equations:

$$\alpha_S \overset{\text{def}}{\equiv} \{x' = y - x, y' = -x - y\}$$
$$\alpha_U \overset{\text{def}}{\equiv} \{x' = x - y, y' = x + y\}$$

   For your convenience, these two differential equations are plotted in Figure 1. The origin (red dot) is an equilibrium for both differential equations because their right-hand sides evaluate to zero at the origin. Thus, a solution that starts at the origin will

stay at the origin for all time. We can describe the origin with a "circle" of radius 0, so $x^2 + y^2 = 0$ is an invariant of both systems.

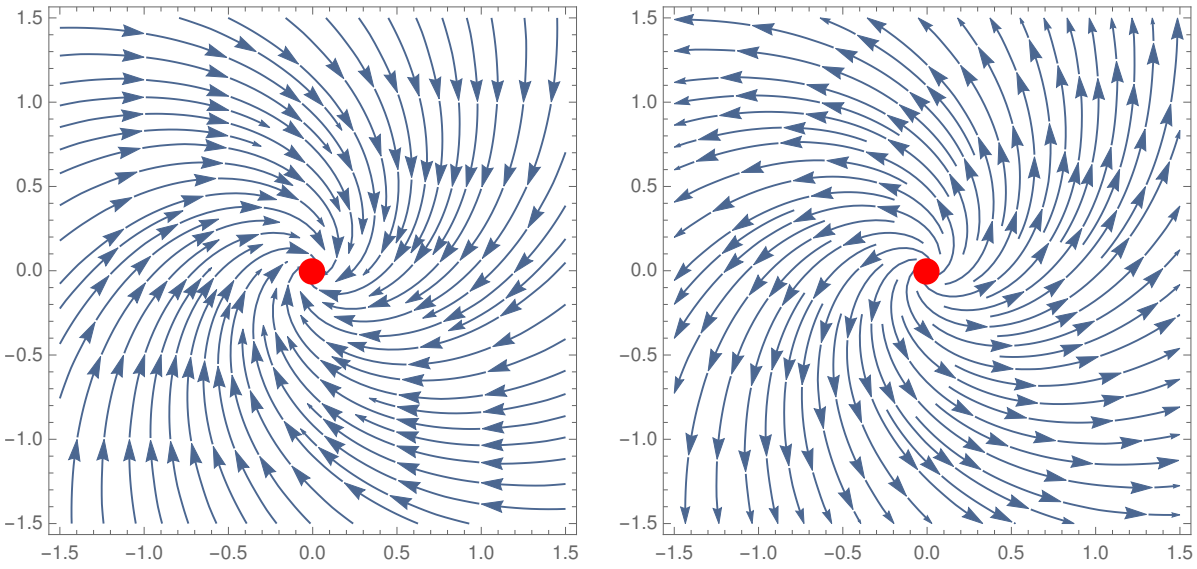

Figure 1: A plot of α_S on the left, and α_U on the right.

(a) Try to prove the invariant for α_S using *differential invariants* only, i.e., attempt to prove the formula:

$$\phi_S \overset{\text{def}}{\equiv} x^2 + y^2 = 0 \rightarrow [\alpha_S]x^2 + y^2 = 0$$

Highlight where your proof fails, and intuitively explain why it failed with reference to Figure 1.

(b) We can rephrase the invariant as an inequality. In real arithmetic, the following formula is provable:

$$x^2 + y^2 = 0 \leftrightarrow x^2 + y^2 \leq 0$$

Using a *monotonicity step*, rewrite the invariant to $x^2 + y^2 \leq 0$ and prove the formula ϕ_S.

(c) The above generalization technique will not work for proving the invariant:

$$\phi_U \overset{\text{def}}{\equiv} x^2 + y^2 = 0 \rightarrow [\alpha_U]x^2 + y^2 = 0$$

Instead, ϕ_U can be proved using *differential ghosts*. We do not (yet) expect you to find the appropriate differential ghost equation yourselves, so we have started the proof for you.

$$\dfrac{\dfrac{\dfrac{}{\textcircled{\star}} \quad \dfrac{\textcircled{1} \qquad \textcircled{2}}{z(x^2+y^2)=0 \wedge z>0 \vdash [\alpha_U, z'=-2z]\big(z(x^2+y^2)=0 \wedge z>0\big)}}{x^2+y^2=0 \vdash [\alpha_U]x^2+y^2=0}\,\text{dA}}{\vdash x^2+y^2=0 \rightarrow [\alpha_U]x^2+y^2=0}\,{}^{[]\wedge,\wedge\text{L},\wedge\text{R}}\,{}_{\rightarrow\text{R}}$$

This derivation uses the *differential auxiliaries* (dA) rule which, as we saw in class, is derived using differential ghosts. In the dA step, we left out the following premise $\textcircled{\star}$ which is provable in real arithmetic:

$$\vdash x^2+y^2=0 \leftrightarrow \exists z\,(z>0 \wedge z(x^2+y^2)=0)$$

The derivation above yields two open premises ① and ②. Complete the proof from ①, i.e., prove:

$$z(x^2+y^2)=0 \vdash [\alpha_U, z'=-2z]z(x^2+y^2)=0$$

(d) Complete the proof from ②, i.e., prove:

$$z>0 \vdash [\alpha_U, z'=-2z]z>0$$

Hint: You will need to use another differential ghost.

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 and lemmas 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: $([\{x' = f(x) \,\&\, H\}]P) \rightarrow (H \rightarrow P)$

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

   (d) **Bonus (very difficult).** Conjunctive Domains:

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