

Assignment 4: ODEs, Games, and Nondeterministic Assignments
15-424/15-624/15-824 Logical Foundations of Cyber-Physical Systems
TA: Katherine Cordwell (kcordwel@cs.cmu.edu)

Due Date: Friday, Oct 25th, 11:59PM (no late days), worth 60 points

1. **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 trigonometric functions (e.g., 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.
2. **Taylor series.** When an ODE cannot be solved exactly, a useful technique is to use a *Taylor series approximation* to get an upper or lower bound on the solution instead. Prove the following formula using the proof rules and axioms of dL:

$$x = 1 \wedge t = 0 \rightarrow [\{x' = x, t' = 1 \ \& \ x \geq 1\}]x \geq 1 + t + \frac{t^2}{2} \quad \text{[?]}$$

Recall that the solution of the ODE $x' = x$ (with initial value $x_0 = 1$) is $x(t) = e^t$, so the above formula expresses a lower bound for e^t (for all $t \geq 0$).

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

$$\alpha_U \stackrel{\text{def}}{=} \{x' = x - y^3, y' = x^3 + y\}$$

For your convenience, α_U is plotted in Figure 1. The origin is an equilibrium of α_U , i.e., a solution that starts at the origin will stay at the origin for all time. It follows that $x^4 + y^4 = 0$ is an invariant of the system.

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

$$\phi_U \stackrel{\text{def}}{=} x^4 + y^4 = 0 \rightarrow [\alpha_U]x^4 + y^4 = 0$$

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

- (b) Differential invariants may have failed us, but fortunately ϕ_U can be proved using *differential ghosts*. We have started the proof for you:

$$\begin{array}{c} \text{①} \quad \text{②} \\ \hline \text{premise} \quad z(x^4 + y^4) = 0 \wedge z > 0 \vdash [\alpha_U, z' = ??](z(x^4 + y^4) = 0 \wedge z > 0) \\ \text{dA} \quad \hline \quad \quad \quad x^4 + y^4 = 0 \vdash [\alpha_U]x^4 + y^4 = 0 \\ \text{→R} \quad \hline \quad \quad \quad \vdash x^4 + y^4 = 0 \rightarrow [\alpha_U]x^4 + y^4 = 0 \end{array}$$

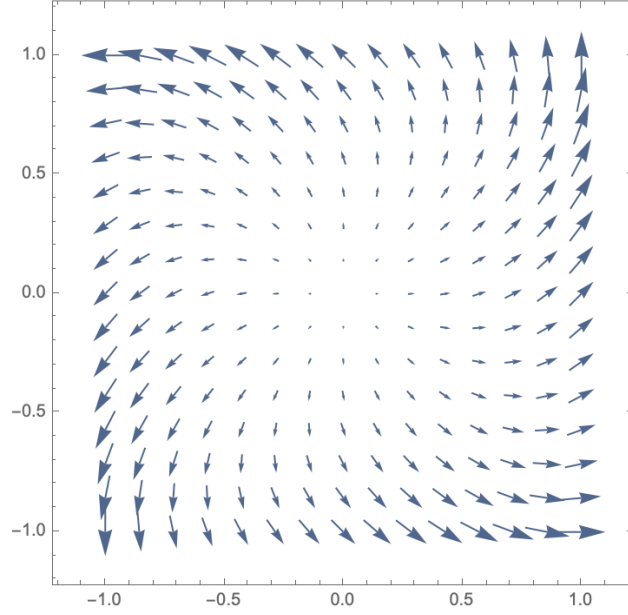


Figure 1: A plot of α_U .

This derivation uses the *differential auxiliaries* (dA) rule which, as we saw in class, is derived using differential ghosts. First, fill in **premise** and explain why it is provable in real arithmetic.

(c) Now, fill in ?? and complete the proof of ①, i.e., prove:

$$z(x^4 + y^4) = 0 \vdash [\alpha_U, z' = ??] z(x^4 + y^4) = 0$$

with ?? appropriately filled in.

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

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

with ?? appropriately filled in.

Hint: Use another differential ghost.

4. **Ghostly proof rules.** Recall the differential auxiliaries (dA) proof rule which can be derived from the differential ghosts axiom:

$$(dA) \quad \frac{\vdash F \leftrightarrow \exists y G \quad G \vdash [\{x' = f(x), y' = a(x) \cdot y + b(x) \& Q\}] G}{F \vdash [\{x' = f(x) \& Q\}] F}$$


This proof rule says that we can add an extra ghost variable y that follows a new differential equation $y' = a(x) \cdot y + b(x)$ that is linear in y . The extra variable can be

used to rewrite the invariant F in a way that makes it more amenable to proof using the other proof rules of **dL**.

In class, we saw how to use the following special instance of **dA** to prove interesting properties in the case where $F \equiv p > 0$ is a strict inequality:

$$(\text{dA}_{>}) \quad \frac{py^2 > 0 \vdash [\{x' = f(x), y' = a(x) \cdot y + b(x) \& Q\}]py^2 > 0}{p > 0 \vdash [\{x' = f(x) \& Q\}]p > 0}$$

Notice that we have omitted the left premise of **dA** in $\text{dA}_{>}$ because $p > 0 \leftrightarrow \exists y py^2 > 0$ is a provable formula of real arithmetic.


(a) In the same style as $\text{dA}_{>}$, write a proof rule called dA_{\geq} that would (soundly) allow you to prove properties of the form $F \equiv p \geq 0$. Briefly argue why your proposed proof rule is sound. 

(b) To test out your proposed dA_{\geq} proof rule, use it to prove the following property:

$$x \geq 1 \vdash [\{x' = 2 - 2x\}]x \geq 1$$


5. **Games and winning.** Answer these 3 questions for each of the following formulas:


- For which starting states does Angel have a winning strategy? (Recall that $\langle \alpha \rangle \phi$ means Angel has a strategy to win into ϕ for hybrid game α)
- Briefly describe Angel's winning strategy from those starting states.
- (Only applies to games where Angel has a winning strategy in at least one state). Say we let Demon pick **one occurrence of one** hybrid program operator and flip it between being an Angel or Demon operator, e.g. replacing **one** $\alpha \cup \beta$ with $\alpha \cap \beta$ or vice-versa. Can Demon make it so that Angel never has a winning strategy in any state?

(a) **A warm-up:** $\langle (x := 0 \cap x := 1)^\times \rangle x \geq 0$ 

(b) **Ups and downs:**

$$\langle ((x := x + 1 \cup \{x' = v\}^d); (y := y - 1 \cup \{y' = w\}^d))^* \rangle |x - y| \leq 1$$

(c) **A chase:** $\langle (w := w \cap w := -w); (v := v \cup v := -v); \{x' = v\}^d; \{y' = w\} \rangle x < y$ 

Hint: Try to give an intuitive reading to the hybrid games before thinking of Angel's strategies. 

6. **Games and proofs.** Consider the following formula:

$$x = 0 \wedge i = 0 \rightarrow \langle (i := i + 1; (\{x' = 1\} \cap \{x' = 2\}))^\times \rangle (x \geq 2 \cdot i \wedge x \leq 4 \cdot i)$$

- (a) First, give an intuitive explanation of what this formula says.
- (b) Prove this formula using the axioms and proof rules of **dGL**.

Hint:

- All the Demon operators like α^\times and $\alpha \cap \beta$ can be defined using the dual operator α^d . We strongly recommend you rewrite the above formula using the dual operator to avoid silly mistakes.
- Make sure to double-check that you have the right player making the choices at each point in the game.
- Most proof rules that we had for hybrid programs also work for hybrid games. The exceptions are given in LFCPS Chapter 17.
- “Most proof rules” includes the induction rule for loops.

7. **Games and invariants.** Define:

$$\begin{aligned}\alpha_1 &\equiv \{x' = v, v' = a, t' = 1 \ \& \ t \leq T\} \\ \alpha_2 &\equiv \{x' = v, v' = -B, t' = 1 \ \& \ v \geq 0\}\end{aligned}$$

Consider the following game:

$$\alpha \equiv t := 0; a := *; ?(0 \leq a \wedge a \leq A); T := *^d; ?(T > 0)^d; (\alpha_1 \cup \alpha_2)$$

The rules of the game can be read as follows:

- First, Angel picks an acceleration: $a := *; ?(0 \leq a \wedge a \leq A)$
- Next, Demon picks a positive timestep: $T := *^d; ?(T > 0)^d$
- Then, Angel then gets to either accelerate with acceleration a , or apply the brakes at $-B$ indefinitely until a stop.

Demon has a strategy to make the following formula valid, i.e. to win the game by preventing Angel from reaching the station, even though Angel is in control of the loop (α^*):

$$A > 0 \wedge B > 0 \wedge v = 0 \wedge x < station \rightarrow [\alpha^*]x < station$$

What is Demon’s invariant? Briefly explain why the invariant works.

$$\begin{array}{c} \text{loop} \quad \text{①} \quad \text{②} \\ \frac{\frac{\mathbb{R} \quad x = 0, i = 0 \vdash x \geq 2i \wedge x \leq 4i}{x = 0, i = 0 \vdash [(i := i + 1; (x' = 1 \cap x' = 2)^d)^*](x \geq 2i \wedge x \leq 4i)} \quad \text{①} \quad \text{②}}{\frac{\langle^d \rangle \quad x = 0, i = 0 \vdash \langle \langle (i := i + 1; (x' = 1 \cap x' = 2)^d)^* \rangle^d \rangle (x \geq 2i \wedge x \leq 4i)}{x = 0, i = 0 \vdash \langle \langle (i := i + 1; (x' = 1 \cap x' = 2))^{\times} \rangle \rangle (x \geq 2i \wedge x \leq 4i)}}\end{array}$$

Since the loop invariant is the postcondition, the postcondition branch ② closes by id (proof omitted). For the remaining premise ($\langle \cap \rangle$ step can be expanded further):

$$\begin{array}{c}
\langle \cap \rangle \frac{x \geq 2i, x \leq 4i \vdash \langle x' = 1 \rangle (x \geq 2(i+1) \wedge x \leq 4(i+1)) \quad x \geq 2i, x \leq 4i \vdash \langle x' = 2 \rangle (x \geq 2(i+1) \wedge x \leq 4(i+1))}{x \geq 2i, x \leq 4i \vdash \langle x' = 1 \cap x' = 2 \rangle (x \geq 2(i+1) \wedge x \leq 4(i+1))} \\
\langle ; \rangle, \langle := \rangle \frac{}{x \geq 2i, x \leq 4i \vdash \langle i := i+1; (x' = 1 \cap x' = 2) \rangle (x \geq 2i \wedge x \leq 4i)} \\
[d] \frac{}{x \geq 2i, x \leq 4i \vdash [i := i+1; (x' = 1 \cap x' = 2)^d] (x \geq 2i \wedge x \leq 4i)}
\end{array}$$

Final premises are similar, so just one is given here. Final step closes by QE in both cases by evolving the ODE forwards for the appropriate length of time.

$$\begin{array}{c}
* \\
\frac{\mathbb{R} \ x \geq 2i, x \leq 4i \vdash \exists t \geq 0 (x+t \geq 2(i+1) \wedge x+t \leq 4(i+1))}{\langle ' \rangle x \geq 2i, x \leq 4i \vdash \langle x' = 1 \rangle (x \geq 2(i+1) \wedge x \leq 4(i+1))}
\end{array}$$