Recitation 7: More on Ghosts
15-424/15-624/15-824 Logical Foundations of Cyber-Physical Systems

Notes by Brandon Bohrer/Yong Kiam Tan.
Edits by Katherine Cordwell (kcordwel@cs.cmu.edu)

1 Motivation and Learning Objectives

The main goal of this recitation is for you to get comfortable with differential ghosts. Additionally, will explore differential equations in a couple of different settings: drag on a parachuter, and boxes sliding down slopes. So we will gain some practice with modeling systems as well as with doing proofs with differential ghosts.

2 Intro to Ghosts

Remember that we've divided our differential equations axioms into two classes: ones where we can syntactically get information about ODEs, and ones where the user must provide insight. Differential ghosts fall into this second category. You, as a user, will be adding a variable to your hybrid program.

There are two kinds of ghosts: discrete and differential. Let's review the relevant axioms/proof rules.

$$\text{(iG)}\quad \frac{\Gamma \vdash [y := e]p, \Delta}{\Gamma \vdash p, \Delta} \qquad (y \text{ fresh})$$

$$\text{(DG)}\quad [\{x' = f(x)\,\&\,Q\}]P \leftrightarrow \exists y [\{x' = f(x), y' = a(x)\cdot y + b(x)\,\&\,Q\}]P \qquad (y \text{ fresh})$$

$$\text{(dG)}\quad \frac{\Gamma \vdash \exists y [\{x' = f(x), y' = a(x)\cdot y + b(x)\,\&\,Q\}]P, \Delta}{\Gamma \vdash [\{x' = f(x)\,\&\,Q\}]P, \Delta} \qquad (y \text{ fresh})$$

The discrete ghost proof rule (iG) is often used to remember some initial state for ODEs (it's used, for example, in the implementation of the solve axiom in KeYmaera X). The differential ghosts axiom (DG) and proof rule (dG) are often used when differential invariants fail. This can happen if the property that you are trying to prove is getting less true over time and thus is not inductive (think loss or decay or something like that).

There's a lot going on in the proof rule (dG). In particular, what's up with the linearity restriction? To understand, let's go back to an example from lecture and consider the ODEs $\{x' = 1, y' = 1 + y^2\}$.

Exercise 1:
What's the solution?
Answer: $x = t, y = \tan(t)$
We can check this by computing: $y' = \frac{d}{dt}\tan(t) = \sec^2(t) = 1 + \tan^2(t) = 1 + y^2$.

Now, say we were to prove $x = 0 \vdash [x' = 1]x \leq 6$ and say that we decide to use $y' = 1+y^2$ as our ghost.

$$\text{bad dG}\ \dfrac{\exists\text{R}\ \dfrac{\dfrac{\vdots}{x = 0, y = 0 \vdash [x' = 1, y' = y^2 + 1]x \leq 6}}{x = 0 \vdash \exists y[x' = 1, y' = y^2 + 1]x \leq 6}}{x = 0 \vdash [x' = 1]x \leq 6}$$

Here, we've forgotten about the linearity restriction in the bad dG step. Forgetting about the linearity restriction gives us a problem, because the solution to $\tan(t)$ blows up before $\frac{\pi}{2}$. So $x = 0, y = 0 \vdash [x' = 1, y' = y^2 + 1]x \leq 6$ is actually valid, because the dynamics $x' = 1, y' = y^2 + 1$ ensure that time can never evolve past $\frac{\pi}{2}$.

However, $x = 0 \vdash [x' = 1]x \leq 6$ is clearly *not valid*, because if we start in a state where $x = 0$ and evolve until $t = 7$, for example, we'll end with $x = 7$ and $7 > 6$. So forgetting about the linearity restriction is unsound. In fact, KeYmaera X may refuse to work if you try to use any ghost that doesn't look linear in shape, even if it is actually linear (so put your ghosts into an explicitly linear format for a smooth proving experience).

Sometimes it's useful to take (dG) and build in a cut, $M[\cdot]$ step to get a variation:

$$\text{(dA)}\quad \dfrac{P \vdash \exists y R \qquad R \vdash [\{x' = f(x), y' = a(x) \cdot y + b(x)\ \&\ Q\}]R}{P \vdash [\{x' = f(x)\,\&\,Q\}]P}$$

Some intuition: Rewriting our invariant can make differential invariants proofs easier. So we hope that by changing P to R, we've set ourselves up well for dI. And the new variable y is under an $\exists$ because we want the freedom to choose a convenient starting value for y. Then we don't know how long the ODE will run for, so we need to be able to get back to P from R no matter what value y ended up with.

(dA) is helpful because it gives us a slightly more structured proof flow. But it also leaves us with some questions: How can we choose R? How can we choose the ghost ODE?

The first choice depends on P. But we can make some guesses based on the shape of P. For example, $p > 0 \leftrightarrow \exists y\ py^2 > 0$ is provable, and we can use this to get a special instance of dA:

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

Here, we've already taken out the left premise since it's provable in real arithmetic (in general, if you apply (dA), do not remove this premise–unless you are using a special rule that we have provided, like (dA$_{>}$)).

Exercise 2:
What is this omitted premise, and why is it valid?
Answer: The omitted premise is $p > 0 \leftrightarrow \exists y\ py^2 > 0$. It is valid because it's true in all states: if $p \leq 0$, then there does not exist such a y, so both $p > 0$ and $\exists y\ py^2 > 0$ are false. If instead $p > 0$, then taking $y = 1$, we have $py^2 > 0$, so both $p > 0$ and $\exists y\ py^2 > 0$ are true.

So, we can use the shape of P to guide our choice of R—this makes progress on our first question. What about our second question? When we're trying to figure out the ghost ODE, that's a little more involved. It'll usually depend on the actual ODE/invariant we have.

3 Examples

Let's do some small examples before we dive into more involved modeling examples.

3.1 Discrete Ghosts Example

First, a discrete ghosts example.

$$\text{iG}\,\dfrac{\text{[:=]}_{=}\,\dfrac{\text{dC}\,\dfrac{\textcircled{1} \qquad \textcircled{2}}{t=0,k=1,k_0=1 \vdash [\{k'=2,t'=1\&t\geq 0\}]k\geq 1}}{t=0,k=1\vdash [k_0:=1][\{k'=2,t'=1\&t\geq 0\}]k\geq 1}}{t=0,k=1\vdash [\{k'=2,t'=1\&t\geq 0\}]k\geq 1}$$

Let's start with branch ①. Abbreviate $t=0,k=1,k_0=1$ by Γ.

$$\text{cut}\,\dfrac{\mathbb{R}\,\dfrac{*}{\Gamma\vdash k=k_0+2t} \qquad \text{dI}\,\dfrac{[':=]\,\dfrac{\text{id}\,\dfrac{*}{t\geq 0\vdash 2=2}}{t\geq 0\vdash [k':=2][t':=1]k'=2t'}}{\Gamma,k=k_0+2t\vdash [\{k'=2,t'=1\&t\geq 0\}]k=k_0+2t}}{\Gamma\vdash [\{k'=2,t'=1\&t\geq 0\}]k=k_0+2t}$$

Now, let's close branch ②:

$$\text{dW}\,\dfrac{\mathbb{R}\,\dfrac{*}{k_0=1,\,t\geq 0,k=k_0+2t\vdash k\geq 1}}{t=0,k=1,k_0=1\vdash [\{k'=2,t'=1\&t\geq 0\wedge k=k_0+2t\}]k\geq 1}$$

Here, the key is that the assumption $k_0=1$ is constant and can be safely kept around in the premises after we apply diff weaken, even though $k=1$ disappears (since it is not constant).

Note: Since it is often very useful to be able to mention the initial values of variables when working with dC/dI, KeYmaera X provides the special keyword "old(·)" which you can use to refer to the initial values of variables before an ODE when using a differential cut.

3.2 Differential Ghosts Examples

These examples are taken from exercises in the textbook. They are meant to illustrate a general technique for figuring out an appropriate ghost ODE.

Let's say we want to prove $x^5 > 0 \vdash [x' = -2x]x^5 > 0$ is valid. Since x is decreasing along the ODE, this property is getting less true over time, which makes us think to use differential ghosts. Further, the shape $x^5 > 0$ suggests that we use ($\mathrm{dA}_>$). What we don't know is what our ghost ODE should be. But that's okay!! Let's start our proof *anyways* and see if we can fill in the ghost ODE later.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{\vdash 2x^5y(??) - 10x^5y^2 \geq 0}\,\mathbb{R}}{\vdash 2x^5y(??) + 5x^4(-2x)y^2 \geq 0}\,\mathbb{R}}{\vdash [x' := -2x][y' := 5y]2x^5yy' + 5x^4x'y^2 \geq 0}}{x^5y^2 > 0 \vdash [\{x' = -2x, y' = ??\}]x^5y^2 > 0}\,\mathrm{dI}}{x^5 > 0 \vdash [\{x' = -2x\}]x^5 > 0}\,\mathrm{dA}_>$$

Here, our task is to find an assignment for ?? that is linear in y to close the proof. It works to choose ?? to be $5y$. Now we can go back and fill in our prooftree:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{\vdash 10x^5y^2 - 10x^5y^2 \geq 0}\,\mathbb{R}}{\vdash 2x^5y(5y) + 5x^4(-2x)y^2 \geq 0}\,\mathbb{R}}{\vdash [x' := -2x][y' := 5y]2x^5yy' + 5x^4x'y^2 \geq 0}}{x^5y^2 > 0 \vdash [\{x' = -2x, y' = 5y\}]x^5y^2 > 0}\,\mathrm{dI}}{x^5 > 0 \vdash [\{x' = -2x\}]x^5 > 0}\,\mathrm{dA}_>$$

Let's try another example. Here we want to prove $x < 0 \vdash [\{x' = -x\}]x < 0$. This is trickier because we first have to choose what new invariant to replace $x < 0$ with. Well, let's see... What if we try something similar to ($\mathrm{dA}_>$), but changed to account for the $<$? We can do that! Notice that $x < 0 \leftrightarrow \exists y\ xy^2 < 0$ is valid.

Exercise 3:
Convince yourself that this is indeed valid.
Note: It's easy to use dA wrong. Take great care to ensure that your new invariant is a sound replacement.

As before, let's start our ghosts proof and fill in our ODE later.

$$\dfrac{\dfrac{*}{\vdash x < 0 \leftrightarrow \exists y\ xy^2 < 0}\,\mathbb{R} \qquad \dfrac{\dfrac{\dfrac{*}{\vdash -xy^2 + 2xy(??) \leq 0}\,\mathbb{R}}{\vdash [x' := -x][y' :=??]x'y^2 + 2xyy' \leq 0}}{xy^2 < 0 \vdash [\{x' = -x, y' = ??\}]xy^2 < 0}\,\mathrm{dI}}{x < 0 \vdash [\{x' = -x\}]x < 0}\,\mathrm{dA}_>$$

Our task is to find a replacement for ?? that is linear in y and closes the proof. We could choose $?? = \frac{1}{2}y$. This choice is not unique. We could also choose, for example, $\frac{1}{2}y - xy$ (why?).

4 James Bond the Parachuter

Now that we have some practice with differential ghosts proofs, let's try modeling something. Consider an object in freefall with drag, such as James Bond performing a high-altitude-low-opening (HALO) jump in Tomorrow Never Dies[1].

To model this problem, let's start with the drag equation from physics:

$$D = \frac{1}{2} C_D \cdot \rho \cdot v^2 \cdot A$$

where ρ is the density of air, C_D is an experimentally determined coefficient of drag, v is velocity and A is the surface area on which the drag force is exerted.

Any time physics gives us equations, we should look for a way to simplify them. Let's say we're just interested in how Bond moves after his parachute is open since that seems like an interesting case. If his parachute is open the surface area A is basically constant. What about air density? That will change throughout a skydive because the density at 30,000 feet is much different from that on the ground, but remember this is specifically a *low opening* jump, so we won't even have the parachute open until we're pretty close to the ground, say 1000ft if Bond is feeling lucky, which he is. So constant density is also a pretty good approximation! And since C_D is an experimentally-determined constant, we might as well roll all the constants together:

$$c \equiv \frac{1}{2} C_D \cdot A \cdot \rho$$

And we can just express the entire rest of model in terms of that one constant, giving us a very simple equation for drag force now:

$$F_D \equiv c \cdot v^2$$

where the constant c is positive.

What other forces should we look at? Well, Bond probably doesn't have much lift, nor much thrust, so let's just look at gravity, which we will model as usual. Now we have a complete ODE to describe Bond's motion:

$$\alpha \equiv \{x' = v, v' = c \cdot v^2 - g\}$$

What does the evolution of this ODE look like? Initially when he opens his parachute, the drag will make him slow down. But then as v^2 decreases, the drag will get less and less until eventually it is effectively cancelled out by gravity and he stops accelerating.

Here's a fun question to try and solve: What is the velocity where Bond stops slowing down? This is a practical question, too: It gives us a lower bound on his landing velocity. If his parachute were too small, this would allow us to formally prove that having too small a parachute results in having too high of an impact velocity, which would lead to near-certain death. We don't like high impact velocities.

[1] Brandon is very creative with his examples. We were admittedly less creative in recitation. Fortunately, this section is mostly his writing, so you're in for a treat!

To solve for this "limiting velocity", set the acceleration to 0 and solve:

$$v' = 0 \text{ implies } c \cdot v^2 - g = 0 \text{ implies } v = \pm\sqrt{\frac{g}{c}}$$

Now, we would only actually reach that exact velocity after infinity time; rather we have $\sqrt{\frac{g}{c}}$ as a lower bound on speed and more specifically $-\sqrt{\frac{g}{c}}$ as an upper bound on velocity because we know we're falling. Let's try to prove this upper bound by DI (note that it's reasonable to put the velocity in the preconditions because we assume we're already falling quite fast when the parachute opens). We can also assume that we have all the necessary assumptions on g, c, etc. in Γ_{const}.

$$\Gamma_{\text{const}}, v < -\sqrt{\frac{g}{c}} \vdash [\alpha]v < -\sqrt{\frac{g}{c}}$$

Remember that $\sqrt{\frac{g}{c}}$ is just a constant, so DI will ask us to prove $v' \leq 0$. DI wants us to say the inequality is either stable over time, or is getting more true over time. But wait! It *doesn't* get more true! It gets more false! It just gets *less more* false over time, and so it never gets all the way to being actually false! To put that less cryptically, v keeps stepping closer and closer to $\sqrt{\frac{g}{c}}$ but the steps keep getting smaller so it never actually gets there.

What are we gonna do? Conceptually, the problem here is that some of our velocity "vanished into the ether". Any proof that explains why $-\sqrt{\frac{g}{c}}$ is an invariant is going to have to talk about all the velocity that we lost due to drag, and explain why that velocity isn't too much. But we don't have a variable to tell us how much velocity we lost from drag, so not only will $v < -\sqrt{\frac{g}{c}}$ fail as an invariant, but *any* invariant we write with the available variables will also fail. **because we need to reason about the lost velocity, we can't prove this until we have a variable for lost velocity**. BUT WE'RE IN LUCK! DIFFERENTIAL GHOSTS ALLOW US TO ADD VARIABLES. LET'S USE THE (dA) PROOF RULE!

> As an aside, here's some intuition for why we like differential ghosts and how we can use them:
>
> - If you can't prove your differential invariant with the variables you have right now, you can invent a new variable to account for "the stuff that went away"
> - When you invent a variable, you'll want and need to say how it changes over time
> - When you invent a variable, you'll also want to rewrite the invariant so it uses your new variable. You probably want this rewriting to make a subsequent differential invariants proof feasible/easier.

Let's start by rewriting this ODE in the simplest way possible, and we'll see why that's no good either. We said intuitively the new variable should be "velocity we lost", so we can

make it exactly that, by making $g(x,y) \equiv g - c \cdot v^2$. Since the new variable stands for "lost velocity" let's call it L.

$$\alpha_2 \equiv \{x' = v, v' = c \cdot v^2 - g, L' = -c \cdot v^2 + g\}$$

And then we will rewrite the postcondition $v \leq -\sqrt{\frac{g}{c}}$ as

$$\exists L. v = v_0 + L \wedge L \geq 0 \wedge L \leq -\sqrt{\frac{g}{c}} - v_0$$

Where v refers to the current velocity and v_0 the initial velocity (if we wanted to introduce the variable v_0 during the middle of proof, we could do so using a *discrete ghost*, which is a story for a different day). What this says is the amount of velocity we lost is small enough that it never makes us go past the terminal velocity and also the velocity is always equal to initial velocity minus the loss. This should be equivalent to our initial postcondition, but there's a problem. This is actually pretty hard to prove by DI. In fact the invariant $L \leq -\sqrt{\frac{g}{c}} - v_0$ is essential if we want to prove the original procondition, but this has exactly the same issue we had trying to prove the original precondition by DI: The invariant gets less and less true over time even though it never gets false.

Well what was the point of doing all this nonsense? Did we just waste a bunch of time learning a proof technique that didn't help? No! Even if two formulas are semantically equivalent, differential invariants might solve one of them completely automatically and get totally stuck on the other one. The dI rule exploits the *differential structure* of a formula, which comes from its syntax, not its semantics. So even though we added a totally new variable, we still don't have the right differential structure. In general, guessing the right differential structure can be hard, but remember that we sometimes have special cases of the dA proof rule that work well for simple formulas. Specifically, here's a formulation of differential assignment that works for formulas of the form $e < 0$:

$$(\mathrm{dA}_<) \quad \frac{y^2 \cdot e = -1 \vdash [\{x' = f(x), y' = a(x) \cdot y + b(x) \;\&\; Q\}] y^2 \cdot e = -1}{e < 0 \vdash [\{x' = f(x) \,\&\, Q\}] e < 0}$$

Exercise 4:
What premise have we omitted, and why is it valid?
Answer: The omitted premise is $e < 0 \leftrightarrow \exists y \; y^2 \cdot e = -1$. It's valid by the following reasoning: If e is 0, $y^2 \cdot e$ is zero, and if e is positive, $y^2 \cdot e$ would always be positive or zero at best (since y^2 is nonnegative), so $y^2 \cdot e = -1$ only happens if e is negative. And it's always possible when $e < 0$ by setting $y = \sqrt{-e}$.

Since we've checked that this premise is always true, we don't have to list it as a branch when you write down the proof rule.

Further, since we're going to use differential invariants after applying ($\mathrm{dA}_<$), we can predict that "all" we need to do in our proof is find a definition of $a(x) \cdot y + b(x)$ such that $y^2 \cdot (e)' + e \cdot 2y(a(x) \cdot y + b(x)) = 0$ is valid. Sadly, this is not nearly as intuitive as our previous idea of "L is the lost velocity". At the same time, we have a much better chance that the proof will go through, because now we're doing DI on a formula that really v with

the loss, avoiding the problem we had before trying to prove a branch where L appeared by itself without v. Less inspiring, but equally relevant, is the fact that we can do this part mechanically, as we will demonstrate using our parachuting example.

First of all, how do we express our postcondition as $e < 0$ anyway? Not too hard: we pick $e = v + \sqrt{\frac{g}{c}}$ and then $e < 0$ is the same as $v < -\sqrt{\frac{g}{c}}$.

Now let's take $(y^2 \cdot (e)' + e \cdot 2 \cdot y \cdot g(y,x) = 0)$ and solve for $g(y,x)$:

$$
\begin{aligned}
& y^2 \cdot (e)' + e \cdot 2 \cdot y \cdot g(y,x) = 0 \\
\iff & y^2 \cdot \left(v + \sqrt{\frac{g}{c}}\right)' + \left(v + \sqrt{\frac{g}{c}}\right) \cdot 2 \cdot y \cdot g(y,x) = 0 \\
\iff & y^2 \cdot v' + \left(v + \sqrt{\frac{g}{c}}\right) \cdot 2 \cdot y \cdot g(y,x) = 0 \\
\iff & \left(v + \sqrt{\frac{g}{c}}\right) \cdot 2 \cdot y \cdot g(y,x) = -y^2 \cdot v' \\
\iff & g(y,x) = \frac{-y^2 \cdot v'}{\left(v + \sqrt{\frac{g}{c}}\right) \cdot 2 \cdot y} \\
\iff & g(y,x) = \frac{-y \cdot v'}{\left(v + \sqrt{\frac{g}{c}}\right) \cdot 2}
\end{aligned}
$$

At this point we should be mildly alarmed. One of the greatest sins we can commit in life is division by zero, and we're dividing by something scary, because actually right now we're in the middle of trying to prove that $v + \sqrt{\frac{g}{c}}$ isn't zero. So maybe we got into a circular argument. But actually if we substitute for v' and do some clever arithmetic we can get out of this mess:

$$
\begin{aligned}
g(y,x) &= \frac{-y \cdot v'}{\left(v + \sqrt{\frac{g}{c}}\right) \cdot 2} \\
\iff g(y,x) &= \frac{-y \cdot (c \cdot v^2 - g)}{\left(v + \sqrt{\frac{g}{c}}\right) \cdot 2} \\
\iff g(y,x) &= \frac{-y \cdot c \cdot (v^2 - (g/c))}{\left(v + \sqrt{\frac{g}{c}}\right) \cdot 2} \\
\iff g(y,x) &= \frac{-y \cdot c \cdot \left(v - \sqrt{\frac{g}{c}}\right)\left(v + \sqrt{\frac{g}{c}}\right)}{\left(v + \sqrt{\frac{g}{c}}\right) \cdot 2} \\
\iff g(y,x) &= \frac{-y \cdot c \cdot \left(v - \sqrt{\frac{g}{c}}\right)}{2}
\end{aligned}
$$

Where the trick here was applying the identity $a^2 - b^2 = (a+b)(a-b)$ to simplify the denominator. Now the denominator is 2, which we can trust to not be 0.

You'll notice we didn't use any fancy proof rules while doing this derivation. There's a good reason for that: we don't have to do this derivation in dL. If we did it wrong, then when we use differential assignment in KeYmaera X we would just end up with branch that doesn't prove. This derivation is something we do on paper to figure out the right input for our ghost ODE.

So now that we know the right thing let's go back and apply DA. If we did our job right, DI will finish it. For the sake of clarity, we write out lots of intermediate arithmetic steps:

$$\mathrm{dA}_{<}\,\frac{\mathrm{dI}\,\frac{\mathrm{derive}\,\frac{[':=]\,\frac{\mathbb{R}\,\frac{\mathbb{R}\,\frac{\mathbb{R}\,\frac{*}{\Gamma_{\text{const}} \vdash (cv^2-g) = (v^2-\frac{g}{c})\cdot c}}{\Gamma_{\text{const}} \vdash (cv^2-g) = \left(v+\sqrt{\frac{g}{c}}\right)\cdot\left(c\left(v-\sqrt{\frac{g}{c}}\right)\right)}}{\Gamma_{\text{const}} \vdash y^2\cdot(cv^2-g) = \left(v+\sqrt{\frac{g}{c}}\right)\cdot y^2\cdot\left(c\left(v-\sqrt{\frac{g}{c}}\right)\right)}}{\Gamma_{\text{const}} \vdash y^2\cdot(cv^2-g) + \left(v+\sqrt{\frac{g}{c}}\right)\cdot 2y\cdot y\cdot\left(-\frac{1}{2}\cdot c\left(v-\sqrt{\frac{g}{c}}\right)\right) = 0}}{\Gamma_{\text{const}} \vdash [v' := cv^2-g][y' := y\cdot\left(-\frac{1}{2}\cdot c\left(v+\sqrt{\frac{g}{c}}\right)\right)]y^2\cdot v' + \left(v+\sqrt{\frac{g}{c}}\right)\cdot 2y\cdot y' = 0}}{\Gamma_{\text{const}} \vdash [v' := cv^2-g][y' := y\cdot\left(-\frac{1}{2}\cdot c\left(v+\sqrt{\frac{g}{c}}\right)\right)]y^2\cdot\left(v+\sqrt{\frac{g}{c}}\right)' + \left(v+\sqrt{\frac{g}{c}}\right)\cdot 2y\cdot y' = 0}}{\Gamma_{\text{const}}, y^2\cdot\left(v+\sqrt{\frac{g}{c}}\right) = -1 \vdash [v' = cv^2-g, y' = y\cdot\left(-\frac{1}{2}\cdot c\left(v+\sqrt{\frac{g}{c}}\right)\right)]y^2\cdot\left(v+\sqrt{\frac{g}{c}}\right) = -1}}{\Gamma_{\text{const}}, v+\sqrt{\frac{g}{c}} < 0 \vdash [v' = cv^2-g]\left(v+\sqrt{\frac{g}{c}} < 0\right)}$$

5 Ping Pong with Air Resistance

For our next model, we will revisit our recurring ping pong example and add in air resistance. Hopefully the words *air resistance* bring differential ghosts to mind (since "air resistance" suggests "loss"). **Note: In recitation we didn't really have time for this section.**

Our continuous dynamics are:

$$\{x' = v, v' = -v^2, t' = 1 \,\&\, t \leq T\}$$

Recall that $v > 0$ initially. This ODE models air resistance which acts in the opposite direction, slowing velocity down with deceleration proportional to v^2. For simplicity, the constant of proportionality is set to 1.

Exercise 5:
Recall/derive the solution to the system.
Answer: The solution of this system (where x_0, v_0 are the initial values of x, v respectively and $v_0 > 0$) is

$$v(t) = \frac{v_0}{1+v_0 t}$$
$$x(t) = \ln(v_0 t + 1) + x_0$$

Keep the solution in mind for everything we do next: it is instructive to see how its properties translate over to ODE invariants that we prove (and vice versa).

Exercise 6:
Is the formula that we just proved for the simpler dynamics still valid if we replaced the ODEs with this more complicated dynamics?
Answer: Yes, one could think of the simpler dynamics as a "worst case" scenario where the air resistance is negligible. The ball will always fly further to the right in this worst case compared to when there is some air resistance.

Now, since the ball is flying with positive velocity to the right we might expect that $l \leq x$ should be the simpler one to prove of the two conjuncts in the postcondition. This intuition will actually turn out to be incorrect, but let us follow our noses for now and try to prove the right conjunct $x \leq r$ first:

$$v > 0 \land t = 0 \land l \leq x \land x + vT \leq r \rightarrow [\{x' = v, v' = -v^2, t' = 1 \,\&\, t \leq T\}]x \leq r$$

In contrast to our previous proof, we no longer have a closed form expression for x in terms of polynomials (or rational functions), so simply cutting in the solution will not work.

Exercise 7:
What should we do next? (Hint: use the physical intuition)
Answer: Instead of proving that $x = x_0 + v_0 t$ is an invariant for the ODE, we could instead try to prove it as an upper bound, i.e., $x \leq x_0 + v_0 t$ because that is what our physical intuition told us.

Let us start by doing the main part of the proof. As explained earlier, we have also introduced fresh variables x_0, v_0 that store the initial values of x, v respectively. The arithmetic at the end works because we know the domain constraint $t \leq T$

$$\dfrac{\dfrac{\dfrac{*}{v_0 > 0, l \leq x_0, x_0 + v_0 T \leq r, t \leq T \land x \leq x_0 + v_0 t \vdash x \leq r}\,\mathbb{R}}{v_0 > 0, t = 0, x = x_0, v = v_0, l \leq x_0, x_0 + v_0 T \leq r \vdash [\{\cdots \,\&\, t \leq T \land x \leq x_0 + v_0 t\}]x \leq r \quad \textcircled{1}}\,\text{dW}}{v_0 > 0, t = 0, x = x_0, v = v_0, l \leq x_0, x_0 + v_0 T \leq r \vdash [\{x' = v, v' = -v^2, t' = 1 \,\&\, t \leq T\}]x \leq r}\,\text{dC}$$

This proof would of course only work if the dC step's other premise, ①, works out. The premise in ① is:

$$v_0 > 0, t = 0, x = x_0, v = v_0, l \leq x_0, x_0 + v_0 T \leq r \vdash [\{x' = v, v' = -v^2, t' = 1 \,\&\, t \leq T\}]x \leq x_0 + v_0 t$$

If we tried to use dI to prove this, we would get stuck. Here is the relevant calculation:

$$\begin{aligned}(x \leq x_0 + v_0 t)' &\equiv (x)' \leq (x_0 + v_0 t)' \\ &\equiv x' \leq v_0 t' \\ &\equiv v \leq v_0\end{aligned}$$

Note: For brevity, we will abuse notation and substitute for the primed variables with their respective RHSes in the ODEs in our calculations for this section. You

should NOT do this in a formal proof but it is fine in rough work, as long as that is clearly stated.

This failed because the dI step does not know much about v yet: we only have $t \leq T$ in the domain constraint.

We actually need to first add $v \leq v_0$ to the domain constraint with a dC step before the aforementioned dI would succeed. Fortunately, this latter step is straightforward because $-v^2 \leq 0$ is a provable in real arithmetic:

$$\begin{aligned}(v \leq v_0)' &\equiv (v)' \leq 0 \\ &\equiv -v^2 \leq 0\end{aligned}$$

That finishes off the proof of safety with respect to the right boundary. Let us now return to the other branch of the proof which we thought was easy:

$$v > 0 \land t = 0 \land l \leq x \land x + vT \leq r \rightarrow [\{x' = v, v' = -v^2, t' = 1 \,\&\, t \leq T\}] l \leq x$$

Exercise 8:
What is a good starting point?
Answer: It's always reasonable to try dI—if it works you're done, and if it fails, the computation can still provide useful information. Here, dI does not work:

$$\begin{aligned}(l \leq x)' &\equiv 0 \leq x' \\ &\equiv 0 \leq v\end{aligned}$$

Following our noses like before, we will need to first prove a property about v before trying dI. We could try to use dI to prove that $v > 0$ is an invariant since we already know $v > 0$ is true initially. However, the calculation would not work out, because $-v^2$ could be negative, and so the premise of dI would not be valid:

$$\begin{aligned}(v > 0)' &\equiv v' \geq 0 \\ &\equiv -v^2 \geq 0\end{aligned}$$

It is actually true that $v > 0$ is an invariant of the ODE, but the proof is much more intricate than just a simple dI.

Exercise 9:
What should we do next?
Answer: You should be thinking differential ghosts here, because the property we're trying to prove is getting less true over time. More specifically, you could be thinking about the $\text{dA}_>$ rule, since $v > 0$ fits the shape for this rule.

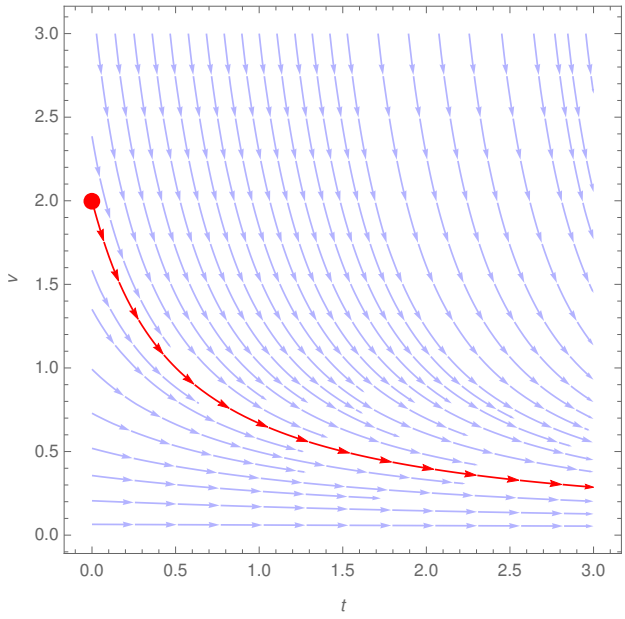
Exercise 10:

The $\text{dA}_>$ rule still requires us to pick a choice of ghost ODE. What ghost ODE should we use for proving $v > 0$ invariant?
Answer: We can figure this out by starting the computation and solving for what we need. In particular, suppose we tried to prove $vy^2 > 0$ using dI.

$$\begin{aligned}(vy^2 > 0)' &\equiv v'y^2 + v(2yy') \geq 0 \\ &\equiv -v^2y^2 + v(2yy') \geq 0\end{aligned}$$

Exercise 11:
What could we pick for y' to make the above formula valid?
Answer: If we set $y' = \frac{vy}{2}$, then the LHS of the inequality cancels out.
Note: In KeYmaera X you have to be fairly careful when writing down a differential ghost. So we should probably rearrange this to linear form, e.g., with $y' = \frac{v}{2}y$.

Let's revisit why proving $v > 0$ invariant was so difficult whereas proving for $v \leq v_0$ seemed to be so much easier. The issue becomes especially clear once we visualize the ODE $v' = -v^2$ with a velocity-time plot:



For an initial value where $v > 0$ (the red point), the value of v decreases towards 0 along the differential equation. In other words, it is getting "worse" over time, although it never quite reaches $v = 0$. This makes it difficult to prove with dI, because dI works for proving properties that become "more true" over time. Recall that for an inequality $v > 0$, dI requires that its derivative is non-negative along solutions to the ODE, which is clearly not the case here.

Contrast this with the case for $v \leq v_0$. Notice that, regardless of where the initial value of v is, its value will always be decreasing towards 0 i.e., $v \leq v_0$ is getting "more true" over time. This makes it well suited for a dI proof.

Exercise 12:
Our ping pong model carefully avoided the special case where $v = 0$. In fact, all of the formulas that we considered would still work if we assumed $v \geq 0$ instead of $v > 0$. Work through the proofs with this assumption and examine which part(s) of the proofs need to be changed.