Recitation 6: Differential Invariants and Differential Cuts
15-424/15-624/15-824 Logical Foundations of Cyber-Physical Systems

Notes by: Brandon Bohrer
Edits by: Yong Kiam Tan (yongkiat@cs.cmu.edu)

1 Announcements

- Theory 3 and Lab 3 now available.
- Lab 3 has 3 submissions: Checkpoint, Betabot, and Veribot. Please take careful note of the deadlines listed in the handout.

2 Review: Assignment 2

In recitation we discussed common mistakes on the assignments, but we will not give out solutions in the recitation notes. If you have questions, come talk to us.

3 Motivation and Learning Objectives

We shall start the recitation by reviewing the ODE axioms of dL that we have seen in class: differential invariants, differential cuts, and differential ghosts. By piecing these axioms together with the other basic ODE axioms, we can derive powerful *proof rules* for reasoning about ODEs.

Using these proof rules, we will take another look at the time-triggered ping-pong model from last week. Specifically, we will focus on proving properties about the ODEs used to model the motion of the ball. The aforementioned proof rules can be used to prove more advanced properties of these ODEs.

4 Axioms and Proof Rules for Differential Equations

The differential equations axioms for dL can be roughly characterized into two groups. In the first group, we have the basic "helper" axioms that allow us to syntactically extract information from an ODE. The latter group of axioms are the ones that require proof insights from the user.

4.1 ODE Helper Axioms

The differential effect and differential weakening axioms belong to the first group of helper axioms:

$$\text{(DE)}\quad [\{x' = f(x)\,\&\,Q\}]P \leftrightarrow [\{x' = f(x)\,\&\,Q\}][x' := f(x)]P$$

$$\text{(DW)}\quad [\{x' = f(x)\,\&\,Q\}]P \leftrightarrow [\{x' = f(x)\,\&\,Q\}](Q \rightarrow P)$$

The differential effect axiom (DE) extracts information about the differential equations $x' = f(x)$. It internalizes that along any solution to the differential equation, the differential variables x' must take on the correct values, i.e., the values of the RHS $f(x)$. In order to prove a postcondition P of an ODE, the RHS of axiom DE says that it suffices to prove the postcondition $[x' := f(x)]P$ instead. The assignment $x' := f(x)$ allows us replace all of the differential variables in P with their respective right-hand sides.

Similarly, the differential weakening axiom (DW) extracts information about the domain constraint Q. Just like the differential variables must take on the correct values, the domain constraint Q must be satisfied along any solution to the differential equation. Therefore, in order to prove a postcondition P of an ODE, the RHS of axiom DW says that it suffices to prove the postcondition $Q \rightarrow P$ instead, where we are allowed to assume that the domain constraint Q is still true at the end of a solution.

It is straightforward to derive proof rules for these two axioms using G. Notice in both cases that the use of G forces us to drop the assumptions Γ, Δ in the context:

$$\text{(dE)}\quad \frac{Q \vdash [x' := f(x)]P}{\Gamma \vdash [\{x' = f(x)\,\&\,Q\}]P, \Delta}$$

$$\text{(dW)}\quad \frac{Q \vdash P}{\Gamma \vdash [\{x' = f(x)\,\&\,Q\}]P, \Delta}$$

Exercise 1:
Work through the derivation of both proof rules. Make sure you see where the additional context has to be dropped in both rules.
Answer:

$$\cfrac{\cfrac{Q \vdash P}{\Gamma \vdash [\{x' = f(x)\,\&\,Q\}](Q \rightarrow P), \Delta}\,{\scriptstyle \text{G},\rightarrow\text{R}}}{\Gamma \vdash [\{x' = f(x)\,\&\,Q\}]P, \Delta}\,{\scriptstyle \text{DW}}$$

$$\cfrac{\cfrac{Q \vdash [x' := f(x)]P}{\Gamma \vdash [\{x' = f(x)\,\&\,Q\}][x' := f(x)]P, \Delta}\,{\scriptstyle \text{dW}}}{\Gamma \vdash [\{x' = f(x)\,\&\,Q\}]P, \Delta}\,{\scriptstyle \text{DE}}$$

As usual, constant assumptions in the context can be kept and KeYmaera X will do this for you automatically. By themselves, however, the dE and dW proof rules are not very useful. It is the next group of axioms for ODEs which really allow us to start proving interesting properties. They are the differential invariant, differential cut, and differential ghost axioms, listed here for easy reference:

(DI) $\big([\{x' = f(x)\,\&\,Q\}]P \leftrightarrow [?Q]P\big) \leftarrow (Q \rightarrow [\{x' = f(x)\,\&\,Q\}](P)')$

(DC) $\big([\{x' = f(x)\,\&\,Q\}]P \leftrightarrow [\{x' = f(x)\,\&\,Q \wedge C\}]P\big) \leftarrow [\{x' = f(x)\,\&\,Q\}]C$

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

4.2 Differential Invariants

The differential invariants axiom is the core workhorse axiom for proving properties of ODEs. In particular, it gives us a link between postcondition P and its differential $(P)'$. This is the crucial insight that we discussed last week: instead of working directly with the solution, we shall instead work with their derivatives (and thus, the ODEs) directly.

The notation $(P)'$ can be understood as a generalization of the differential of terms $(e)'$ to a differential on formulas. It is defined inductively, with the following base cases for the atomic comparison formulas:

$$
\begin{aligned}
&(e = k)' \equiv (e)' = (k)' \\
&(e \leq k)' \equiv (e)' \leq (k)' \qquad \text{(accordingly for } \geq) \\
&(e < k)' \equiv (e)' \leq (k)' \qquad \text{(accordingly for } >) \\
&(e \neq k)' \equiv (e)' = (k)'
\end{aligned}
$$

Note: The differential of $(e < k)'$ could also be defined as $(e)' < (k)'$. This would also be sound, but just more restrictive than the one given above.

Let us look specifically at the $e = k$ case for some intuition:

(DI$_=$) $\big([\{x' = f(x)\}]e = k \leftarrow e = k\big) \leftarrow ([\{x' = f(x)\}](e)' = (k)')$

In this equational case, the axiom says that in order to prove that $e = k$ is true along all solutions to the ODE, it suffices to show that $e = k$ is true initially and that $(e)' = (k)'$ is true along all solutions to the ODE. Why might this be the case? The answer comes from the crucial differential lemma from last week.

Remember that differentials $(e)'$ have the same value as the derivative of e along solutions of an ODE. Therefore, if the values of terms e and k start off equal, and the value of their derivatives stay equal along the solution, then the values e and k also stay equal along the solution, i.e., $e = k$ is true along the solution.

Exercise 2:

Where should we add back the domain constraints in the DI$_=$ axiom, and why (intuitively)?

Answer: By the original DI axiom, the equational case with domain constraints is as follows:

(DI$_=$) $\big([\{x' = f(x)\,\&\,Q\}]e = k \leftrightarrow [?Q]P\big) \leftarrow (Q \rightarrow [\{x' = f(x)\,\&\,Q\}](e)' = (k)')$

Recall that the domain constraint Q of an ODE must be obeyed at *all times*, including at the start. Thus, in an initial state where Q is false, the formula $[\{x' = f(x)\,\&\,Q\}]e = k$ is vacuously true. The DI$_=$ axiom tells us exactly that, because both $[?Q]P$ and $Q \rightarrow [\{x' = f(x)\,\&\,Q\}](e)' = (k)'$ would be vacuously true in such a state.

More interestingly, we now only need to prove $[\{x' = f(x) \,\&\, Q\}](e)' = (k)'$, rather than $[\{x' = f(x)\}](e)' = (k)'$. Recall additionally, that the axiom DW allows us to assume Q when proving the postcondition of an ODE. Thus, we can now prove $(e)' = (k)'$ while assuming the domain constraint Q. This intuition can be more easily seen from the proof rule:

$$(\text{dI}_=)\ \frac{Q \vdash [x' := f(x)](e)' = (k)'}{\Gamma, e = k \vdash [\{x' = f(x) \,\&\, Q\}]e = k, \Delta}$$

Exercise 3:
Derive this proof rule from the $\text{DI}_=$ axiom.
Answer: This derives using dE which in turn derived from dW.

As an aside: why do we want to write down these proof rules when we could have just derived them from the axioms? Proof rules provide a useful summary of the standard way in which we would put the axioms together to prove a desired postcondition. They are well suited, e.g., for use as top-level tactics in KeYmaera X, because that is what you would want to work with rather than applying the axioms step by step every single time you want to prove that something is invariant for the ODEs.

The intuition behind the other base cases is similar to the $e = k$ case. In order to prove that $e \geq k$ (resp. $e > k$) is true along a solution of the ODE, we will require that $e \geq k$ (resp. $e > k$) initially, and that $(e)' \geq (k)'$ along that solution, or in other words, the value of the derivative of e is always greater or equal to that of k along the solutions.

For $e \neq k$, it is initially slightly surprising that we instead need to show that $(e)' = (k)'$ along the ODE rather than $(e)' \neq (k)'$. This surprise should clear up, however, once we realize that checking $(e)' \neq (k)'$ is insufficient to ensure that $e \neq k$ stays true along the ODE. As an example, consider the following sequent:

$$x \neq y \vdash [\{x' = 1, y' = -1\}]x \neq y$$

Exercise 4:
Is this sequent valid? Why or why not?
Answer: It is clearly not valid: consider an initial state where $x < y$, then since the ODEs increase x while decreasing y, their values should eventually meet somewhere along the solution to the ODE.

If we had defined $(e \neq k)' \equiv (e)' \neq (k)'$, however, we would have easily proved the above property (unsoundly):

$$\cfrac{\cfrac{\cfrac{*}{\vdash 1 \neq -1}}{\vdash [x' := 1][y' := -1]x' \neq y'}[':=]}{x \neq y \vdash [\{x' = 1, y' = -1\}]x \neq y}\,??$$

Finally, the $(\cdot)'$ operator can be extended to conjunctive and disjunctive formulas inductively. This extension can also be thought of as a mnemonic device, since we already saw in class that both the $\wedge$ and $\vee$ cases can be derived from the base cases using the other proof rules of dL.

$$(P \wedge Q)' \equiv (P)' \wedge (Q)'$$
$$(P \vee Q)' \equiv (P)' \wedge (Q)'$$

Like the $\neq$ case, the $\vee$ case is slightly surprising: it requires that we prove $(P)' \wedge (Q)'$ rather than $(P)' \vee (Q)'$ as we might expect if we simply extended the $(\cdot)'$ operator naively. One way of understanding this difference is to consider the $e \neq k$ case we saw above.

In real arithmetic, the formula $e \neq k$ can be re-written equivalently as $e > k \vee e < k$. If we simply defined the differential of a disjunction to be $(P)' \vee (Q)'$, then the differential of $e > k \vee e < k$ case would be $(e)' \geq (k)' \vee (e)' \leq (k)'$ which is a valid formula in real arithmetic. So we have just proved that $e \neq k$ is an invariant of any ODE we ever wanted simply by rewriting it into another form. In contrast, the correct definition yields $(e)' \geq (k)' \wedge (e)' \leq (k)'$, which is equivalent to $(e)' = (k)'$, as expected. To summarize, the proof rule for differential invariants is:

$$\text{(dI)}\ \frac{Q \vdash [x' := f(x)](P)'}{\Gamma, P \vdash [\{x' = f(x) \,\&\, Q\}]P, \Delta}$$

Exercise 5:
Derive this proof rule (similar to the derivation of $\text{dI}_=$).

4.3 Differential Cuts

The differential cuts axiom (DC) is very much like the usual cut rule from sequent calculus, except it allows us to cut and assume new formulas in the domain constraint of a differential equation rather than the antecedents. The proof rule for differential cuts is a straight forward rephrasing of the DC axiom with two premises:

$$\text{(dC)}\ \frac{\Gamma \vdash [\{x' = f(x) \,\&\, Q\}]C, \Delta \qquad \Gamma \vdash [\{x' = f(x) \,\&\, Q \wedge C\}]P, \Delta}{\Gamma \vdash [\{x' = f(x) \,\&\, Q\}]P, \Delta}$$

Exercise 6:
Convince yourself that this rule derives from DC.

The right premise of dC allows us to additionally assume the cut C in the domain constraint when proving postcondition P. In particular, if we subsequently use dI, in the right premise, we now get to assume $Q \wedge C$ when proving $(P)'$:

$$\text{dC}\ \frac{\Gamma \vdash [\{x' = f(x) \,\&\, Q\}]C, \Delta \qquad \text{dI}\ \dfrac{Q \wedge C \vdash [x' := f(x)](P)'}{\Gamma \vdash [\{x' = f(x) \,\&\, Q \wedge C\}]P, \Delta}}{\Gamma \vdash [\{x' = f(x) \,\&\, Q\}]P, \Delta}$$

As an aside, whereas the usual cut rule in logic can be removed by a cut elimination theorem, the dC principle cannot be eliminated without losing the ability to prove some ODE properties in dL. In other words, if we restricted ourselves to using dI without ever using dC, we would not be able to prove some true properties of ODEs that we could have with dC. We will see more about the proof theory of the ODE axioms in dL next week.

The next ODE reasoning principle further increases the proof theoretic strength of dI and dC. In fact, it is powerful enough to let us prove any algebraic postcondition of an ODE (if it is true), i.e., a sequent of the form:[1]

$$\Gamma \vdash [x' = f(x)]p = 0$$

4.4 Differential Ghosts

The differential ghosts axiom is surprisingly simple given its proof theoretic power. Its corresponding proof rule simply allows us to write down a new differential equation with a fresh variable y:

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

Since y is fresh, the axiom even allows us to choose any initial value for y for the existential quantifier. There is one syntactic restriction on the newly introduced ODE: the right-hand side of the ODE must be *linear* in y. This restriction seems rather onerous initially: after all, it was the non-linear ODEs with nasty solutions that motivated us towards studying ODEs directly rather than their solutions. However, this linearity restriction is critical for soundness of the DG axiom.[2]

Note: The explanation of dA,dA$_>$ was rushed in recitation. These notes may help to clear matters up (see also LFCPS Chapter 12).

It is helpful to package up dG with a cut,M[·] step in order to derive the differential auxiliaries proof rule.

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

The idea behind dA is in order to prove an invariant P, we could rephrase it equivalently in terms of the newly introduced ghost variable y. However, the proof rule still leaves open two questions: 1) how should we choose the replacement R? 2) how should we choose the ghost ODE $y' = a(x)\cdot y + b(x)$?

The first choice will be dependent on the precise formula P, but we already saw one very useful choice when $P \equiv p > 0$. In real arithmetic, the formula $p > 0 \leftrightarrow \exists y\, py^2 > 0$ is provable. We can write down this special instance of dA:[3]

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

Note that the left premise of dA no longer appears in dA$_>$ because it is provable in real arithmetic.

The second choice of the ghost ODE in both dA and dA$_>$ is more difficult and will usually depend on the actual ODE and invariant that we are trying to prove. We will see an example of this as we explore the ping pong model from last week.

[1] We will not cover this result (and its extensions) in the course, but feel free to ask at office hours or Piazza if you are interested.

[2] The newly introduced ODE could otherwise restrict the existence duration of the original ODE.

[3] This instance is actually slightly more general than the one we saw in class. It also works better with KeYmaera X.

5 Ping Pong with Air Resistance

We shall now refine the ping pong model from last week using a better model of physics. For simplicity, let us drop the loop and instead just focus on ensuring the safety property with respect to the ODEs. In particular, let us consider a formula of the form:

$$Pre \rightarrow [\{x' = f(x) \,\&\, t \leq T\}]l \leq x \leq r$$

where $x' = f(x)$ is a system of equations (including a clock) which we will have to determine, and Pre is the preconditions that we will be assuming of the ball.

To further simplify things, we shall assume that the initial velocity is positive, i.e., $v > 0$, so that the ball is flying towards the right boundary.

Note: We rushed through the intuition behind both models in order to get to actually doing the proofs in KeYmaera X. The intuition behind each proof step is explained in these notes.

Note: In class, we moved over to doing proofs in KeYmaera X instead of writing all of the derivations out.

5.1 Recall: Simple Model

Recall our reasoning behind the time-triggered control from last week: after making a control decision, in the worst case, we can only react T seconds later. We therefore need to start at least distance vT away from r for the safety postcondition $x \leq r$ to work. On the other hand, if we are currently flying towards the right boundary, then intuitively we should never be able to violate the left boundary – we are flying away from it! Thus, $l \leq x$ should be true as well, assuming that we start in a position $l \leq x$. In other words, the following formula is valid:

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

Exercise 7:
What are the steps needed in the proof?
Answer: As we saw last week, this ODE is simple enough that it can be solved. Thus, all we need to do is to use dC to add the solution of the differential equations to the domain constraint.

Note: For brevity, the initial ∧L and →R unfolding steps in all subsequent derivations have been skipped.

We already saw how to do the proof of the right premise of the dC step using dI last week so those steps are omitted here. A dW step allows us to complete the proof:

$$\dfrac{\dfrac{\dfrac{*}{T > 0, v > 0, l \leq x_0, x_0 + vT \leq r \vdash t \leq T \land x = x_0 + vt \rightarrow l \leq x \leq r}\,\mathbb{R}}{T > 0, v > 0, t = 0, x = x_0, l \leq x_0, x_0 + vT \leq r \vdash [\{x' = v, t' = 1 \,\&\, t \leq T \land x = x_0 + vt\}]l \leq x \leq r}\,\text{dW}}{T > 0, v > 0, t = 0, x = x_0, l \leq x_0, x_0 + vT \leq r \vdash [\{x' = v, t' = 1 \,\&\, t \leq T\}]l \leq x \leq r}\,\text{dC}$$

Exercise 8:
What is wrong with the above proof, and how should it be fixed?
Answer: Firstly, we have secretly introduced the new variable x_0 to store the initial value of x. The conclusion of the proof rule does not quite match up to the formula that we actually started with! Fortunately, we do have license do this: one way is to use the iG,$[:=]_=$ proof rules that we have already seen in class to introduce the ghost variable x_0:[4]

$$\dfrac{\dfrac{\dfrac{v>0,t=0,x=x_0,l\leq x_0,x_0+vT\leq r\vdash[\{x'=v,t'=1\,\&\,t\leq T\}]l\leq x\geq r}{v>0,t=0,l\leq x,x+vT\leq r,x_0=x\vdash[\{x'=v,t'=1\,\&\,t\leq T\}]l\leq x\geq r}[:=]_=}{v>0,t=0,l\leq x,x+vT\leq r\vdash[x_0:=x][\{x'=v,t'=1\,\&\,t\leq T\}]l\leq x\geq r}\,\text{iG}}{v>0,t=0,l\leq x,x+vT\leq r\vdash[\{x'=v,t'=1\,\&\,t\leq T\}]l\leq x\geq r}$$

It is very useful to be able to mention the initial values of variables when working with invariants so KeYmaera X provides the special keyword "old(·)" which you can use to refer to the initial values of variables before an ODE when specifying invariants.
Note: This model is called rec6simple in the archive. In class, we also noted that we could have proved this model simply using KeYmaera X's ODE automation (which solves the ODEs).

There is a more serious problem though. The real arithmetic step at the end does not actually work for the left boundary! If we looked at it closely, there is no lower bound on t, so in fact the premise after the dW step is not valid because t could take on very negative values.

To correct the proof, we would actually need to add an additional dC step to prove that $t\geq 0$ is an invariant of the ODE before using dW.

This is a common pattern in dI,dC proofs: you will often need to first cut in some properties using dC before your desired dI steps will work. Admittedly though, the dC of $t\geq 0$ is still rather boring and we shall encounter more interesting cuts in the next model.

5.2 Air Resistance Model

Following what we did last week, let us add an additional differential equation for velocity so that the overall ODE system becomes:

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

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 9:
Recall/derive the solution to the system.

[4] An alternative method is to simply cut in $\exists x_0\, x=x_0$, which is provable in real arithmetic, and then remove the existential quantifier with ∃L.

Answer: The solution of this system (where x_0, v_0 are the initial values of x, v respectively and $v_0 > 0$) from last week 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 10:
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:

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

Note: This model is called rec6right in the archive. We also noted that KeYmaera X could not figure out the proof automatically for this new model.

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 11:
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 $t \leq T$

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

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 actually 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 calculations, as long as that is clearly stated.

The reason why dI failed is clear: the domain constraint 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:

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

Note: This model is called rec6left in the archive. We noted that KeYmaera X managed to figure out this proof automatically.

What did KeYmaera X actually do to prove this for us? Let us try and recreate the proof.

Exercise 12:

What is the first step in the proof?

Answer: A straightforward dI would not work:

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

Like before, we will need to first prove a property about v before trying dI. We could try 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:

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

Note: The following exercise is inspired by a comment from a student in recitation.

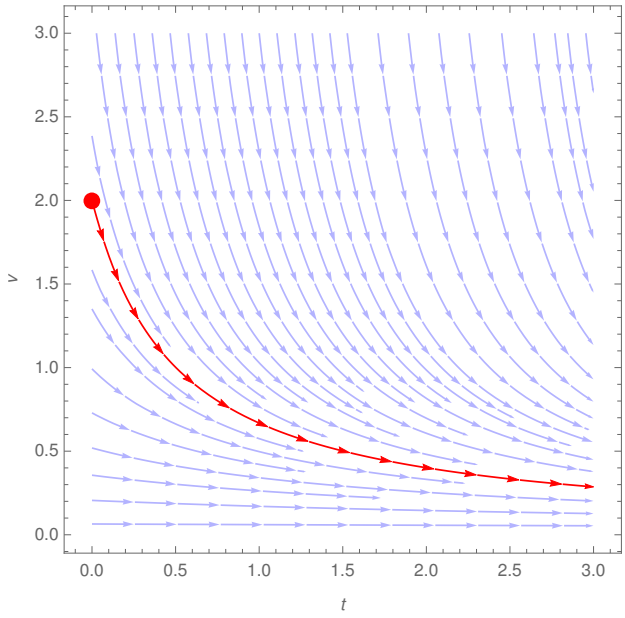
Exercise 13:
Is it even the case that $v > 0$ would be true along the ODE? After all, if v starts at some small positive value, it seems like its ODE $v' = -v^2$ would cause it to eventually be negative – this means that the ball might violate the left boundary after all!
Answer: It is actually true that $v > 0$ is an invariant of the ODE, but the proof is much more intricate than just a simple dI. The intuition is that, even though $v' = -v^2$ causes v to tend towards 0, it never actually reaches 0 because the rate of decrease also decreases as v decreases. This type of property is symptomatic of a proof that requires a differential ghost. We will use the $\text{dA}_>$ rule that we saw earlier.

Exercise 14:
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: Using the "spooky cloud" procedure in class, we can figure out what the ODE has to be. 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 15:
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. For example, the ghost equation has to be explicitly rearranged to be in linear form, e.g., with $y' = \frac{v}{2}y$.
Note: The next part is advanced material and is mainly here for completeness and intuition. We did not have time to cover this in detail at recitation.

Finally, let us 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 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 16:
The ping pong models we considered in this recitation 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 of the proofs need to be changed.