Recitation 7: ODEs Proofs and Hybrid Games
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

- Reminder: midterm next week, come to lecture on Tuesday with questions.
- Lab 3 Betabot due on **Thursday**. Please come for office hours or arrange a time if you have trouble with lab assignments.
- Likewise, there is no recitation for the next two weeks. Please ask on Piazza/office hours/etc., if you need help with Lab 3 Veribot.

2 Review: Lab 2 Veribot

Lab 2 Veribot will be reviewed at additional office hours (Friday, 12 Oct, 4-5PM) rather than recitation.

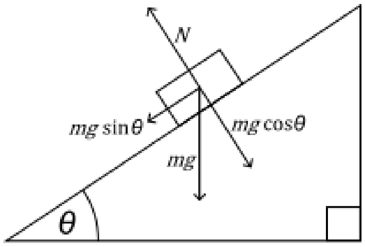
3 Motivation and Learning Objectives

The first part of this recitation reviews the differential equations reasoning principles that we saw last week. This time, we will explore differential equations in a new setting: boxes sliding down slopes. The properties we will prove about this example are relatively straightforward consequences from physics. Our main objective here is to gain some routine practice with modeling systems and doing proofs with differential invariants and differential cuts.

We will then start looking at simple hybrid game questions to gain familiarity with the dual operator that we just saw in class.

4 Slippery Slopes

The first model that we shall explore is a box sliding down a frictionless slope. This is not a physics course, so we will just look at Wikipedia for a useful illustration of this situation:



From the picture, we see that the box is being driven parallel down the slope by a force $mg\sin(\theta)$. For our purposes, we shall work with accelerations and so we will assume that the box has unit mass, i.e., with $m = 1$.

To set us up for the question we will be asking next, we shall work in Cartesian coordinates i.e., in the xy-plane. In that case, we will need to describe the motion of the box along both coordinate axes.

4.1 One Slippery Slope

The coordinates simply change according to their respective components of the velocities:

$$x' = v_x, y' = v_y$$

However, since the box is *accelerating*, we will also need to model these velocities changing as it slides down the slope. Using basic trigonometry, we have:

$$v_x' = g\sin(\theta)\cos(\theta), v_y' = -g\sin^2(\theta)$$

This all makes sense, *except* the right hand sides of these ODEs are not quite polynomials so we cannot actually write these down in dL. To fix this issue, we will have to rewrite these trigonometric functions away.

Exercise 1:
How?
Answer: For this purpose, we shall introduce two new variables w, h which represent the width, height of the slope respectively. Since we will actually only be concerned with the steepness of the slope rather than its precise length we can, without loss of generality, assume that the length of the diagonal $w^2 + h^2 = 1$. Thus, we can write $\sin(\theta) = h, \cos(\theta) = w$ and use this to rewrite the ODEs for velocity as follows:

$$v_x' = gwh, v_y' = -gh^2$$

Now that we have set up a system of ODEs, let us see whether we can prove interesting properties about it. Recall that the box was accelerating down the slope at rate $g\sin(\theta) = gh$. If its initial velocity was 0, then the distance it moves after time t should be given by $\frac{1}{2}ght^2$.

To help us write this down formally, it is useful to start with some abbreviations. First, the assumptions on the constants:

$$\Gamma \overset{\text{def}}{\equiv} g > 0, h^2 + w^2 = 1, h > 0, w > 0$$

Next, the system of ODEs with an additional clock equation $t' = 1$:

$$\alpha \overset{\text{def}}{\equiv} \{x' = v_x, y' = v_y, v_x' = gwh, v_y' = -gh^2, t' = 1\}$$

Finally, some assumptions on the initial values of the variables:

$$Init \overset{\text{def}}{\equiv} t = 0, x = x_0, y = y_0, v_x = 0, v_y = 0$$

This is the sequent we want to prove valid:

$$\Gamma, Init \vdash [\alpha](x - x_0)^2 + (y - y_0)^2 = (\frac{1}{2}ght^2)^2$$

In order to avoid writing down square roots we have written down the *squared* distance in the postcondition. This results in a fourth power of t appearing on the right.

There are several ways we can prove this sequent. First, the system of ODEs that we have written down is actually solvable, so it is possible to simply solve and ask QE. Second, we could try a direct proof using dI,dC which is possible, but would not be very pleasant.

Exercise 2:

How else could we prove this sequent?

Answer: A third option, which is the approach we will try next, is to instead prove a more straightforward postcondition that implies what we want. Recall that we have already factored the velocity into the x and y directions. We could simply give the closed form expression for the positions moved in both of these directions. For the horizontal x direction, we shall prove the following sequent:

$$\Gamma, Init \vdash [\alpha]x - x_0 = \frac{1}{2}gwht^2 \tag{1}$$

Let us try a straightforward dI:

$$\begin{array}{rc}
 & \vdash v_x = \tfrac{1}{2}gwh(2t) \\ \cline{2-2}
[' {:=}] & \vdash [x' := v_x][t' := 1]x' = \tfrac{1}{2}gh^2(2tt') \\ \cline{2-2}
\mathrm{dI} & \Gamma, Init \vdash [\alpha]x - x_0 = \tfrac{1}{2}gwht^2
\end{array}$$

As we have seen several times already, the proof fails because we do not have enough information about v_x. We do get a hint, however, that we should first try a differential cut of $v_x = \frac{1}{2}gwh(2t)$. This cut proves fine:

$$\begin{array}{rc}
 & * \\ \cline{2-2}
\mathbb{R} & \vdash gwh = gwh \\ \cline{2-2}
[' {:=}] & \vdash [v_x' := gwh][t' := 1]v_x' = gwht' \\ \cline{2-2}
\mathrm{dI} & \Gamma, Init \vdash [\alpha]v_x = \tfrac{1}{2}gwh(2t)
\end{array}$$

It allows us to complete our earlier proof by first using a dC:

$$\begin{array}{rc}
 & * \\ \cline{2-2}
\mathbb{R} & v_x = \tfrac{1}{2}gwh(2t) \vdash v_x = \tfrac{1}{2}gwh(2t) \\ \cline{2-2}
[' {:=}] & v_x = \tfrac{1}{2}gwh(2t) \vdash [x' := v_x][t' := 1]x' = \tfrac{1}{2}gwh(2tt') \\ \cline{2-2}
\mathrm{dI} & \Gamma, Init \vdash [\{\alpha \,\&\, v_x = \tfrac{1}{2}gwh(2t)\}]x - x_0 = \tfrac{1}{2}gwht^2 \\ \cline{2-2}
\mathrm{dC} & \Gamma, Init \vdash [\alpha]x - x_0 = \tfrac{1}{2}gwht^2
\end{array}$$

The vertical y direction can be proved similarly, i.e., this sequent is also valid:

$$\Gamma, \mathit{Init} \vdash [\alpha]y - y_0 = \frac{1}{2}gh^2t^2 \tag{2}$$

Using Equations 1 and 2, we can now prove the Euclidean distance property that we wanted using an M[·] step. The M[·] step works because if the equations $y - y_0 = -\frac{1}{2}gh^2t^2$ and $x - x_0 = \frac{1}{2}gwht^2$ are true, then using the assumption $w^2 + h^2 = 1$ we have:

$$\begin{aligned}(y - y_0)^2 + (x - x_0)^2 &= (\frac{1}{2}gh^2t^2)^2 + (\frac{1}{2}gwht^2)^2 \\ &= (\frac{1}{2}ght^2)^2(h^2 + w^2) \\ &= (\frac{1}{2}ght^2)^2\end{aligned}$$

$${\scriptstyle \mathrm{M}[\cdot]}\,\dfrac{{\scriptstyle []\wedge,\wedge\mathrm{R}}\,\dfrac{\dfrac{1}{\Gamma, \mathit{Init} \vdash [\alpha]x - x_0 = \frac{1}{2}gwht^2} \qquad \dfrac{2}{\Gamma, \mathit{Init} \vdash [\alpha]y - y_0 = -\frac{1}{2}gh^2t^2}}{\Gamma, \mathit{Init} \vdash [\alpha](x - x_0 = \frac{1}{2}gwht^2 \wedge y - y_0 = -\frac{1}{2}gh^2t^2)}}{\Gamma, \mathit{Init} \vdash [\alpha](x - x_0)^2 + (y - y_0)^2 = (\frac{1}{2}ght^2)^2}$$

Note: We skipped the next exercise in recitation, it briefly describes another way in which the distance can be calculated using dI.

Exercise 3:
There is a fourth related option. We can make use of the fact that we already know the box is sliding down the slope. How?
Answer: Since the box is sliding down the slope, the following will also be an invariant:

$$y_0 - y = \frac{h}{w}(x - x_0) \tag{3}$$

This will, in turn, require us to prove the following invariant on velocities which follows easily by dI:

$$-v_y = \frac{h}{w}v_x$$

This approach is somewhat more satisfying because it gives us an actual invariant about the motion of the box that is independent of time. Using Equations 3 and 1, it is also possible to deduce the distance moved by the box.

The main takeaway messages here is that directly attempting to use dI may not always be the best option. Rephrasing the question could make it easier to prove.

4.2 Two Slippery Slopes

Suppose you were in a competition where you were asked to build a slope so that the boxes slide down and hit the floor as fast as possible. From ordinary physical intuition, it should be clear that steeper slopes will allow the box to slide downwards faster. Let us try to model and prove this formally.

Suppose that we have another one of these boxes on a separate slope with a steeper incline. We can model this situation by using a smaller width ρ, but using a higher value for the new incline's height σ. We shall similarly enforce $\rho^2 + \sigma^2 = 1$.

For clarity, let the coordinates of the new box be a, b. Following very much the same derivation that we did for the first box, the following system of ODEs can be used to describe the motion of the second box:

$$a' = v_a, b' = v_b$$
$$v_a' = g\rho\sigma, v_b' = -g\sigma^2$$

Suppose that both boxes were initially started at rest. We shall prove that the vertical distance traveled by the box on the steeper slope is always greater than that of the other box.

Exercise 4:
To make sure everyone has practice writing down models we shall work through this example together.
Answer: We already know the model of physics: we can just glue the ODEs for both two boxes together.

$$\beta \overset{\text{def}}{\equiv} \{x' = v_x, y' = v_y, v_x' = gwh, v_y' = -gh^2, a' = v_a, b' = v_b, v_a' = g\rho\sigma, v_b' = -g\sigma^2, t' = 1\}$$

What should the initial conditions be? We certainly need all of our *constant* assumptions. Always remember to write these down: KeYmaera X and dL formulas/sequents do not know what assumptions you are making on constants unless they are written down. We will also add in our assumption that the new slope is steeper i.e., $\sigma > h$:

$$\Gamma \overset{\text{def}}{\equiv} g > 0, h^2 + w^2 = 1, h > 0, w > 0, \sigma^2 + \rho^2 = 1, \sigma > 0, \rho > 0, \sigma > h$$

We will also need some initial assumptions about the positions of the boxes. In order for the competition to be fair, let us just assume that they start at the same coordinates at rest:

$$Init \overset{\text{def}}{\equiv} t = 0, x = x_0, y = y_0, v_x = 0, v_y = 0, a = x_0, b = y_0, v_a = 0, v_b = 0$$

Finally, we need to write down a postcondition for this system. Remember that writing down postconditions that clearly correspond to what we want makes your model easier to understand.

$$Safe \overset{\text{def}}{\equiv} y \geq b$$

This is what we will want to prove:

$$\Gamma, \mathit{Init} \vdash [\beta] y \geq b$$

In contrast our earlier question for the single slope model, this question is a lot simpler and we will be able to tackle it with straightforward dI,dC. With the foresight of our earlier proof, we can do a rough dI calculation first, which tells us that we need to show $v_y \geq v_b$. This proves easily with dI:

$$\text{dI}\,\dfrac{['{:=}]\,\dfrac{\mathbb{R}\,\dfrac{*}{\Gamma \vdash -gh^2 \geq -g\rho^2}}{\Gamma \vdash [v_y' := -gh^2][v_b' := -g\rho^2] v_y' \geq v_b'}}{\Gamma, \mathit{Init} \vdash [\beta] v_y \geq v_b}$$

Thus, a dC completes the proof our our desired property:

$$\text{dC}\,\dfrac{\text{dI}\,\dfrac{['{:=}]\,\dfrac{\mathbb{R}\,\dfrac{*}{\Gamma, v_y \geq v_b \vdash v_y \geq v_b}}{\Gamma, v_y \geq v_b \vdash [x_y' := v_y][x_b' := v_b] v_y' \geq v_b'}}{\Gamma, \mathit{Init} \vdash [\{\beta \,\&\, v_y \geq v_b\}] y \geq b}}{\Gamma, \mathit{Init} \vdash [\beta] y \geq b}$$

Another interesting question is how to we can choose the slops so that the box moves the greatest distance horizontally. This is not as obvious physically: if the slope were completely flat, then the box would not be moving. On the other hand, if the slope were completely vertical, then the box would drop straight to the floor but not move very far horizontally.

Let us try and see if dI can give us some hints. Suppose that we want to pick inclines that allow us to show $x \geq a$. Using the argument we had above, we would need to first show $v_x \geq v_a$, and thus $gwh \geq g\rho\sigma$.

Recall that $h^2 + w^2 = 1$ and $h > 0$ so we may rewrite h with $h = \sqrt{1 - w^2}$ (and similarly for ρ, σ). In other words, we only need to find the maximum value of the function $f(x) = x\sqrt{1 - x^2}$ for $0 \leq x \leq 1$. This maximum value is attained at $x = \frac{1}{\sqrt{2}}$, so the maximum horizontal speed is attained with $h = w = \frac{1}{\sqrt{2}}$, i.e., a 45 degree incline.

4.3 One Slippery Slope with a Spring

Note: We skipped this section in recitation. It explains a more advanced model for the slippery slope with an addition of a spring.

Let us change our single box model further and suppose that the box is now attached to a spring that acts on the box parallel to the slope. The spring is initially at rest.

Exercise 5:
How can we extend our ODEs to model this situation?
Answer: Reversing the trigonometric calculations we did earlier, we know that if the box has traveled a horizontal distance $x - x_0$ along the slope, then its distance traveled along the slope is given by $\frac{x - x_0}{w}$.

Therefore, we can model the restoring acceleration due to the spring by modifying our differential equations for velocity:

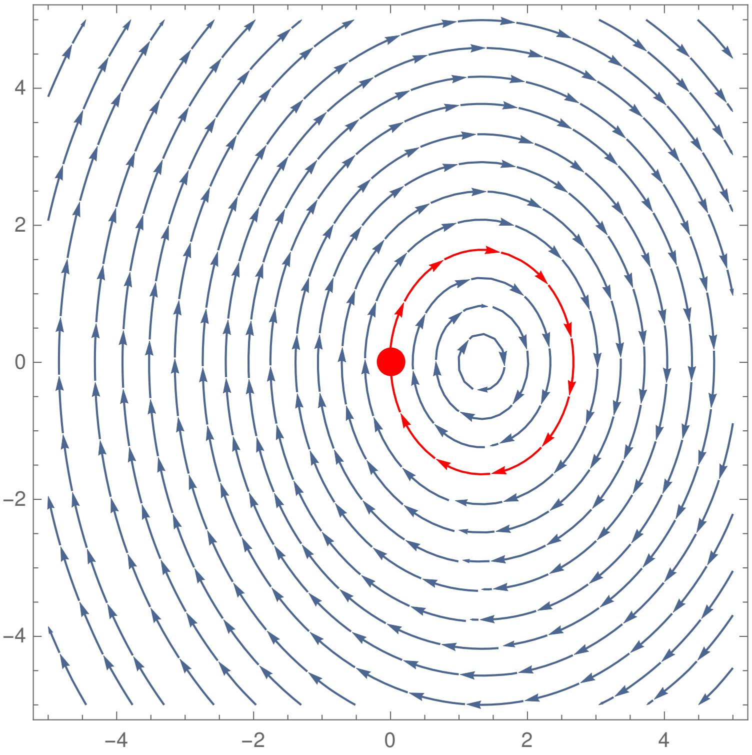
$$v_x' = w(gh - k\frac{x - x_0}{w}), v_y' = -h(gh - k\frac{x - x_0}{w})$$

This quickly becomes a huge mess, so let us focus on studying the x direction only and set $x_0 = 0$. The ODEs describing motion in the horizontal direction can be written as:

$$x' = v_x, v_x' = c - kx$$

where $c = wgh > 0$ is a positive constant, and $k > 0$ is the spring constant.

We may be interested in bounding the horizontal position of the box and perhaps its horizontal velocity. To do this, observe that this simplified system actually describes an oscillator so it will oscillate about the center $v_x = 0, x = \frac{c}{k}$. This is evident once the ODEs are plotted; . Here is the velocity-position plot for $c = 2, k = \frac{3}{2}$. The velocity is plotted vertically while position is plotted horizontally.



From the plot, it is easy to see that the maximum horizontal position of the box is $x \leq 2\frac{c}{k}$. If we tried to prove this right away with dI, we would fail. The technique we have been using so far of cutting in extra invariants would not work either: it tells us to cut in $v \leq 0$, which would not be provable for the above system.

Exercise 6:
How else should we prove this?

Answer: Recall back to Recitation 5 where we actually already encountered a similar situation. We can describe the ellipse by:

$$\frac{(x-\frac{c}{k})^2}{(\frac{c}{k})^2} + \frac{v_x^2}{\frac{c^2}{k}} = 1$$

This implies, in particular that the maximum horizontal position is given by $x = 2\frac{c}{k}$, while the maximum horizontal speed is given by $|v_x| = \sqrt{\frac{c^2}{k}}$.

Exercise 7:
Work through the dI calculation and convince yourself that it works.

Notice that the final approach we discussed at the start of this lecture really shines here. Instead of doing all of the above calculations for the y coordinate again, we can simply use the relationship from Equation 3 to obtain bounds on y.

5 Hybrid Games

Note: We started off this section by watching Geri's Game from Pixar. Watch it online if you have not already done so. It is a useful illustration of how the dual operator works.

The syntax of hybrid games extends that of hybrid programs with the dual operator:

$$\alpha, \beta ::= x := e \mid ?Q \mid \{x' = f(x) \,\&\, Q\} \mid \alpha \cup \beta \mid \alpha;\beta \mid \alpha^* \mid \alpha^d$$

At first glance, this is a simple syntactic extension. We shall see in a few lectures, however, that the semantics of hybrid games is radically different from that of hybrid programs. This is a timely reminder that the meaning of a piece of syntax is really only given by its semantics and nothing else. We have not yet looked the semantics so this recitation will mainly focus on modeling modeling some simple scenarios.

First, let us recap the useful Demon versions of operators that we have seen in class:

Angel	Demon	Definition with Duals
$\alpha \cup \beta$	$\alpha \cap \beta$	$(\alpha^d \cup \beta^d)^d$
α^*	$\alpha^\times$	$((\alpha^d)^*)^d$
$\alpha;\beta$	$\alpha;\beta$	$\alpha;\beta$
$x := e$	$x := e$	$x := e$
$\{x' = f(x) \,\&\, Q\}$	$\{x' = f(x) \,\&\, Q\}^d$	$\{x' = f(x) \,\&\, Q\}^d$
$?H$	$?H^d$	$?H^d$

Notice that the sequential composition and assignment operators do not have duals. Intuitively, there is no choice involved for these operators, so it does not matter who is making the choice.

We have also seen in class that $\langle\alpha\rangle P$ means "Angel wins" while $[\alpha]P$ means "Demon wins". Let us think about the dual operators with respect to these modalities.

Exercise 8:
When is $\langle ?H^d\rangle P$ true? What about $[?H^d]P$?
Answer: In the former, Angel wins if H is false in the current state, or if P is true (i.e., $H \to P$). In the latter, Demon wins if the test succeeds and also P is true (i.e., $H \wedge P$).

Exercise 9:
When is $\langle\alpha \cap \beta\rangle P$ true? What about $[\alpha \cap \beta]P$?
Answer: For $\langle\alpha \cap \beta\rangle P$, we require that no matter if Demon picked program α or β, Angel can play that game to win into postcondition P. In contrast, $[\alpha \cap \beta]P$ is true if Demon can pick either α or β so that no matter how the game unfolds in the chosen game, Demon wins into postcondition P.

Exercise 10:
When is $\langle\{x' = f(x) \,\&\, Q\}^d\rangle P$ true? What about $[\{x' = f(x) \,\&\, Q\}^d]P$?
Answer: In the former, Demon controls how long the ODEs are ran. Therefore, Angel wins if for all runs of the ODE the postcondition P is true at the end of the solution. In the latter, Demon can choose how long to run the ODE, and so Demon wins when there is some run of the ODE such that postcondition P is true.[1]

5.1 A Bus Chase

We will be interested in the following real life scenario[2]: Suppose that Brandon lives some distance d away from the school. Each morning, he has two choices for getting to school: 1) take the bus, 2) walk towards school. Of course, if Brandon gets tired along the way, then he could also stop walking and just wait for the bus to arrive.

We would like to know if there a strategy for Brandon so that he can always get to school on time, e.g., within T minutes. Let us model this situation more precisely. We will assume that the current position of Brandon is x (with his house at $x = 0$), the bus is at position b (initially $b < 0$), and the school is at position d. For simplicity, the school is infinitely large so Brandon is in the school whenever $x \geq d$.

We can write a discrete controller for Brandon that models his instantaneous decision to walk or wait for the bus. In addition, if Brandon is already on the bus (which we model by $x = b$), then his velocity is faster (because the bus drives quickly). Brandon's walking speed is given by W, while the bus cruising speed is given by V.

$$\alpha \equiv ?x = b; v_x := V \cup v_x := W \cup v_x := 0$$

[1] All of the above can be seen from the following derived axiom of dGL, which we will see later in class. $\langle\alpha^d\rangle P \leftrightarrow [\alpha]P$.

[2] According to the TA of the last iteration of this course.

Exercise 11:
If Brandon is already on the bus, what do the choices $v_x := W \cup v_x := 0$ mean?
Answer: Intuitively, this just says that Brandon gets off the bus and starts walking (or waits for the next bus). It is not clear why Brandon would want to do this, but it is part of the control allowed in our model.

Next, let us model the bus. This will be a demonic bus, and so it really does not want you to be able to board it. However, if Brandon has already boarded the bus, then it is forced to move at its cruising speed. Otherwise, all bets are off and the bus could accelerate, brake or even reverse arbitrarily as it pleases.

$$\beta \equiv \textbf{if } x = b \textbf{ then } v_b := V; a_b := 0 \textbf{ else } a_b := *$$

Finally, after Brandon and the bus have both made their decision, we will let the physics of the real world run:

$$\gamma \equiv \{x' = v_x, b' = v_b, v_b' = a_b, t' = 1\}$$

We can now put these three programs together in a loop and start our timer off at $t = 0$:

$$\delta \equiv t := 0; (\alpha; \beta; \gamma)^*$$

Exercise 12:
How could we express the property that Brandon has a strategy to get to school within T minutes in dL?
Answer: This is a trick question, because we will not be able express this cleanly. However, we shall try to do it anyway.

Recall from Lab 1 that we represented the efficiency property for the controller with a formula of the form $[\alpha](v = 0 \rightarrow \cdots)$. We can do something similar here. For example, we could say that if the timer has reached time $t = T$, then Brandon's position must be $x \geq d$.

$$[\delta](t = T \rightarrow x \geq d)$$

There are two flaws with this formula. First, the box modality quantifies over *all runs* of the program. This is not quite what we want, because there is a run where Brandon simply stays and waits for the bus forever! This formula would actually unsatisfiable assuming appropriate initial assumptions on the constants.

Secondly, the postcondition intuitively says **if** $t = T$ then $x \geq d$. This is somewhat unsatisfying (like some students pointed out for Lab 1), because we do not actually know that $t = T$ is eventually reached. Admittedly, this is rather obvious for this model because if the loop (and ODE) is executed for sufficiently many iterations we should be able to reach $t = T$. This would not be the case for more complicated models, though.

To resolve both of these issues, we could try to instead ask a diamond modality formula:

$$\langle \delta \rangle (t = T \land x \geq d)$$

Exercise 13:
What is wrong with this formula?
Answer: Just like the box modality quantifies over *all runs*, the diamond modality only quantifies over *some* run of δ. In particular, we have lost the adversarial dynamics of the demonic bus! We could instead try to break the hybrid program and write it down with alternating modalities:

$$\langle \alpha \rangle [\beta] \langle \gamma \rangle (t = T \land x \geq d)$$

These alternations correctly capture what we want: there is *some* run of Brandon's controller, such that *for all* runs of the bus controller, there is *some* run of the physics so that $t = T \land x \geq d$. But we have dropped the program loop! Now all we can do is run the controllers and ODEs once, which is not very interesting. Intuitively, we want them to alternate as many times as required until the timer expires.

To correctly express our intended meaning for the model, we will therefore need to use a hybrid game rather than just a simple hybrid program. In particular, let us think about the formula:

$$\langle t := 0; (\alpha; \beta^d; \gamma)^* \rangle (t = T \land x \geq d)$$

This says that the Angel player (in this case, Brandon) has a strategy to win into postcondition $t = T \land x \geq d$ in the hybrid game $(\alpha; \beta^d; \gamma)^*$.

Let us peel apart the game layer by layer and read it intuitively in the context of what we are trying to model.

First, the outermost loop operator gives Brandon a choice of repeating the loop as many times as possible. This seems natural, because after all, it is Brandon who is heading to school.

Next, in the body of the loop, Brandon first gets to run his controller α. Control is then ceded over to the bus controller by use of the dual operator. Brandon has no control over what the demonic bus does, so in order for Brandon to win, he must be able to cope with whatever strategy the bus decides to play. After the bus controller has made its choice, control is returned to Brandon who runs the physics.

Exercise 14:
That latter step where Brandon controlled physics seems rather fishy. Why? Should we add the dual operator on γ as well?
Answer: Adding a dual operator here would not quite work because then the demonic bus can always decide to run the ODEs for no time, causing Brandon to lose the game. As we saw in class, this is a filibuster strategy by the Demon that prevents Brandon from ever achieving his objecting. In this case, our model is simply saying that Brandon can make his choice of whether to stop or walk at any time he sees fit.