15-424/15-624/15-824 Recitation 
Circular Dynamics and Spooky Ghosts Jumping Out Of Planes
15-424/15-624/15-824 Foundations of Cyber-Physical Systems

1 Circular Dynamics

Important Supplementary Material: `https://www.youtube.com/watch?v=PGNiXGX2nLU`

In recitation, we talked about the circular motion dynamics for Lab 3. Details aren't available in the online notes since they are closely related to BetaBot 3 solutions, but feel free to ask in office hours or class if you need a reminder.

Important ideas:

- We can and should prove some basic theorems to make sure we've got a good model of circular motion before proving complicated safety conditions. Example theorems are "we always stay on the circle" which can be expressed with x, y and "we always have the right velocity" which can be written with x', y'. These theorems can get a bit harder when you get to a model that has acceleration, so make sure they still work on such a model!

- When safety problems get more complicated, proving an exact solution can be very difficult or even impossible. For example, a perfectly tight safety argument for Lab 3 would be based on arc length, which is difficult to deal with. Easier, but still good, solutions can be made based on other common distance metrics such as L_2 norm (Euclidean distance), L_1 norm (x-distance + y-distance), or L_∞ norm (max of x-distance, y-distance). Note $L_\infty \leq L_2 \leq$ arcdistance $\leq L_1$, but you can bound the difference between these different notions of "distance" by a constant factor, which allows you to get upper bounds out of lower bounds and vice versa.

- Understanding how to make the robot stay on the circle with correct velocity gets tricky when we split off a separate vector dx, dy to represent the direction of motion as a unit vector, but this will help us in Lab 4 when we need to support multiple circles.

2 Spooky Ghosts Are A Drag

Important Supplementary Material 2:`https://www.youtube.com/watch?v=eqavulPAfRA`
Important Supplementary Material 3:`https://www.youtube.com/watch?v=Fe93CLbHjxQ`

Spooky differential ghosts are an advanced proof technique that allow us to use differential invariants in cases where differential invariants otherwise wouldn't work. In general, ghosts are useful any time we want to prove an invariant that gets "less true" over time, but never so much "less true" that it ever actually becomes false. More concretely, we sometimes want to show that an inequality $\theta_1 < \theta_2$ is an invariant when the difference $\theta_2 - \theta_1$ gets smaller over time. If this difference gets smaller, then $\theta_1 < \theta_2$ isn't inductive and a DI proof would fail. We need something stronger.

As an example, let's model 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:

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

[1] Does this sound like a more exciting/fun case study than robots driving in one dimension? One reason for giving you a fun case study this week is to remind you that we've now passed the midterm and also part of the course where we learned all the core logical features we need for course projects! We'll try not to work you too hard over spring break, but that might be a good time to start thinking about the fun side of final projects: coming up with a cool topic to model+verify! (Don't start working on it too hard, though, please do get some rest.)

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. Yay!

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

$$v' = 0 \to c() \cdot v^2 - g = 0 \to v = +- \sqrt{g}c$$

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

$$v < -\sqrt{g}c \to [\alpha]v = -\sqrt{g}c$$

Remember that $-\sqrt{g}c$ is just a constant, so DI will ask us to prove $v' \leq 0$. DI wants us to say the inequality gets *more true* over time. But wait! It *doesn't* get more true! It gets more false! It just *less more* false, and so it never gets all the way to being actually false!

To put that less cryptically, remember how we had to worry about Zeno's paradox when we're writing down a model, so we know it's possible for a model to keep evolving for all time t? Well, Zeno's paradox can work in our favor, too. So v keeps stepping closer and closer to $-\sqrt{g}c$ 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 $-\sqrt{g}c$ 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 $v < -\sqrt{g}c$ 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. Let's come up with a rule that allows us to add a variable then. We'll call that rule differential auxilliaries, which is the most commonly-used form of differential ghosts:

$$\text{dA}\ \frac{P \leftrightarrow \exists y.J \qquad \Gamma, J \vdash [x' = f(x), y' = g(y,x)\&Q]F, \Delta}{\Gamma, P \vdash [x' = f(x)\&Q]P, \Delta}$$

In general, this rule is scary and confusing the first N times that you see it. The important ideas are

- 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. Recall from a previous recitation that rewriting our invariants into the right form can make DI proofs easier. This is even more true when we can rewrite them to use new variables. And why is the new variable under an $\exists$? At the start of the ODE we already know P and want to change it around, and we want the freedom to construct a convenient starting value for y. Then we don't know how long the ODE will run so the final value of y might be lots of different things, so we want to be able to get back P from J no matter what y we ended up with.

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

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

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! Recall again that even if two formulas are semantically equivalent, dI 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 just like we did with dI, we can identify special cases of the DA rule that work well for simple formulas. Specifically, here's a formula of dA that works for formulas of the form $e < 0$:

$$DA_{<}\ \frac{(e < 0) \leftrightarrow \exists y.y^2 \cdot e = -1 \qquad \Gamma, J \vdash [x' = f(x), y' = g(y,x)\&Q](y^2 \cdot e = -1), \Delta}{\Gamma, P \vdash [x' = f(x)\&Q](e < 0), \Delta}$$

There's a cute trick here: The branch $(e < 0) \leftrightarrow \exists y.y^2 \cdot e = -1$ is always valid, no matter what e is: 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 it's always true we actually don't have to list it as a branch when we write down the proof rule. Also, we're always going to second branch by DI, so we can simplify the rule further to get:

$$DA_{<}\ \frac{\Gamma, J \vdash [x' = f(x), y' = g(y,x) \& Q](y^2 \cdot (e)' + e \cdot 2 \cdot y \cdot g(y,x) = 0), \Delta}{\Gamma, P \vdash [x' = f(x) \& Q](e < 0), \Delta}$$

In order to apply this rule successfully, "all" we need to do is find a definition of $g(y,x)$ such that $y^2 \cdot (e)' + e \cdot 2 \cdot y \cdot g(y,x) = 0$ 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 links the variables v and L, 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 $g(y,x)$:

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

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:

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

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 I 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 $\mathsf{d}\mathcal{L}$. If we did it wrong, then when we applied the DA rule 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 DA.

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

$$DA_{<}\,\dfrac{\mathrm{dI}\,\dfrac{\mathrm{derive}\,\dfrac{\mathbb{R}\,\dfrac{\mathbb{R}\,\dfrac{\mathbb{R}\,\dfrac{\mathbb{R}\,\dfrac{*}{((c\cdot v^2-g)=(v^2-\frac{g}{c})\cdot c)}}{((c\cdot v^2-g)=(v+\sqrt{\frac{g}{c}})\cdot\left[c\cdot\left(v-\sqrt{\frac{g}{c}}\right)\right])}}{(y^2\cdot(c\cdot v^2-g)=(v+\sqrt{\frac{g}{c}})\cdot y^2\cdot\left[c\cdot\left(v-\sqrt{\frac{g}{c}}\right)\right])}}{(y^2\cdot(c\cdot v^2-g)+(v+\sqrt{\frac{g}{c}})\cdot 2\cdot y\cdot y\cdot\left[-\frac{1}{2}\cdot c\cdot\left(v-\sqrt{\frac{g}{c}}\right)\right]=0)}}{(y^2\cdot v'+(v+\sqrt{\frac{g}{c}}<0)\cdot 2\cdot y\cdot y\cdot\left[-\frac{1}{2}\cdot c\cdot\left(v-\sqrt{\frac{g}{c}}\right)\right]=0)}}{(y^2\cdot(v+\sqrt{\frac{g}{c}})'+(v+\sqrt{\frac{g}{c}}<0)\cdot 2\cdot y\cdot y\cdot\left[-\frac{1}{2}\cdot c\cdot\left(v-\sqrt{\frac{g}{c}}\right)\right]=0)}}{J\vdash[v'=c\cdot v^2-g,y'=y\cdot\left[-\frac{1}{2}\cdot c\cdot\left(v+\sqrt{\frac{g}{c}}\right)\right]\&Q](y^2\cdot(v-\sqrt{\frac{g}{c}})'+e\cdot 2\cdot y\cdot y'=0)}}{(v+\sqrt{\frac{g}{c}}<0)\vdash[v'=c\cdot v^2-g\&Q](v+\sqrt{\frac{g}{c}}<0)}$$

Other notes on ODEs:

- dA is not sound for all choices of $g(x,y)$, because adding dimensions to an ODE is only sound if we know that the extra dimension will not change how long the ODE evolves. I don't mean this in terms of how long the domain constraint will be true — that stays the same no matter what. What I mean is that if the new dimension y has an asymptote at infinity in finite time, then the duration of the ODE would change and that would be bad. The easiest way to get out of this is to restrict $g(x,y)$ to be linear in y (but arbitrarily complex in x): there's a nice theorem about ODEs that says any linear ODE has a solution for all time t. And if you're linear in yourself but not other variables, you have a solution as long as they do.

- You can get KeYmaera X to try and do a dI proof for you some of the time, though it might not work all of the time. The way to do this is to use the `ODE` tactic in your proofs instead of the `solve` tactic: `ODE` will try invariants, ghosts, solving, anything that it thinks might help. But it's new so it also might not work all the times that you want it to.