15-424/15-624 Recitation 4
Manual proofs and KeYmaera proofs

1 Quick notes on assignment 1

These were some fairly common mistakes that are worth pointing out:

1. Don't forget how terms are defined! We are allowed to write the term x^n, where $n \in \mathbb{N}$ is a fixed natural number. That's because we can always represent it through multiplication: $x \cdot x \cdot ... \cdot x$, n times. Thus, *for a fixed* n, we can rewrite the term into multiplication, which is in the grammar.

   When we try to do x^y, where both x and y are variables over the $\mathbb{R}$, then we don't have a way to rewrite it through multiplication.

2. The functions cos or sin are also not in the syntax. That's because it's hard to reason about them symbolically, like we do in differential dynamic logic. That doesn't mean they can't be represented! As you know, the differential equation $x' = -y, y' = x$ gives us those functions. And we know how to reason symbolically about ODEs!

   The critical realization is that while we are talking about cos and sin, we understand them through their definition according to the differential equation. Thus, when reasoning symbolically about cos and sin, we can only use the fact that $x' = -y, y' = x$, nothing else.

2 Manual proofs

2.1 The ODE solve rule

The ODE solve rule, which deconstructs the program $[x' = f(x) \& H]\phi$ is fairly complicated. Luckily, it's usually used in a really straightforward way. In fact, you often need to make a single choice, and that choice is usually clear. Let's start:

$$\text{ODE solve}\;\dfrac{\forall_R\;\dfrac{\to_R\;\dfrac{\to_R\;\dfrac{\forall_L\;\dfrac{?}{t_0 \geq 0, \forall s.\, (0 \leq s \land s \leq t_0 \to \langle x := \varphi(s) \rangle H) \vdash \langle x := \varphi(t_0) \rangle \phi}}{t_0 \geq 0 \vdash \forall s.\, (0 \leq s \land s \leq t_0 \to \langle x := \varphi(s) \rangle H) \to \langle x := \varphi(t_0) \rangle \phi}}{\vdash t_0 \geq 0 \to \forall s.\, (0 \leq s \land s \leq t_0 \to \langle x := \varphi(s) \rangle H) \to \langle x := \varphi(t_0) \rangle \phi}}{\vdash \forall .t\, (t \geq 0 \to \forall s.\, (0 \leq s \land s \leq t \to \langle x := \varphi(s) \rangle H) \to \langle x := \varphi(t) \rangle \phi)}}{\vdash [x' = f(x) \& H]\phi}$$

But when we assume that something is true for all s, then we can choose what we want s to be. A smart choice will help us prove our property. A bad one will not.

In order to get some intuition, think back on lab 1, where your robot had to stop before the charging station. If you chose your acceleration just right, the robot would stop right at the charging station.

Because of non-determinism, we allowed the continuous evolution to stop at any point (as long as the velocity was non-negative). But really, if the robot was moving forwards, what would be the duration that would make the robot most likely to go past the station?

The longest duration possible! In the proof, this is represented by the free variable t_0. In fact, it's at time t_0 that ϕ needs to hold. So let's try to substitute that in.

$$\forall_L, s := t_0\ \cfrac{\to_L\ \cfrac{\text{ax}\ \cfrac{*}{t_0 \geq 0 \vdash 0 \leq t_0 \wedge t_0 \leq t_0} \qquad \cfrac{\text{rest of proof}}{t_0 \geq 0, \langle x := \varphi(t_0)\rangle H \vdash \langle x := \varphi(t_0)\rangle \phi}}{t_0 \geq 0, 0 \leq t_0 \wedge t_0 \leq t_0 \to \langle x := \varphi(t_0)\rangle H \vdash \langle x := \varphi(t_0)\rangle \phi}}{t_0 \geq 0, \forall s.\, (0 \leq s \wedge s \leq t_0 \to \langle x := \varphi(s)\rangle H) \vdash \langle x := \varphi(t_0)\rangle \phi}$$

Given that choice, the rest becomes pretty easy! One of the branches proves trivially. The other, $t_0 \geq 0, \langle x := \varphi(t_0)\rangle H \vdash \langle x := \varphi(t_0)\rangle \phi$, essentially means $H \to \phi$, since the assumption and the desired conclusion are talking about the same state!

2.2 Cut - bring your knife! haha so fun

It is a truth universally acknowledged that computers are in want of intelligence! Sometimes, they need guidance when we tell them to find proofs for a given formula. They get easily confused by formulas that say what we mean in strange ways.

To illustrate, let's start working with the following:

$$\big((x-y)^2 \leq 0 \wedge \phi(x)\big) \to \phi(y)$$

The proof starts easily enough...

$$\to_R\ \cfrac{\wedge_L\ \cfrac{\cfrac{?}{(x-y)^2 \leq 0, \phi(x) \vdash \phi(y)}}{(x-y)^2 \leq 0 \wedge \phi(x) \vdash \phi(y)}}{\vdash ((x-y)^2 \leq 0 \wedge \phi(x)) \to \phi(y)}$$

But now what? well, if ϕ is a FOL formula and it's small and simple enough, it might be possible to get KeYmaera and its QE procedure to do the work for us.

Unfortunately, that's often not the case. Formulas are long, complicated, and involve lots of variables, and so KeYmaera is going to really struggle.

What can we do? Looking at the assumption $(x-y)^2 \leq 0$, we can draw some conclusions. We know that $(x-y)^2$ as to be non-negative, which with our assumption gives us $(x-y)^2 = 0$. in turn, this tells us that $x = y$. But wait! If they are equal, then the formulas $\phi(x)$ and $\phi(y)$ are equivalent, making them trivial to prove!

That is a lot easier for KeYmaera to realise, so we are going to cut in the fact that $x = y$. Furthermore, we will also use the weakening or hiding rules to make sure KeYmaera focuses on the right subproblems of our proof, instead of worrying with extraneous stuff.

$$
\to_R \dfrac{\wedge_L \dfrac{\text{cut} \dfrac{W_L \dfrac{W_R \dfrac{\text{QE} \dfrac{*}{(x-y)^2 \leq 0 \vdash x = y}}{(x-y)^2 \leq 0 \vdash x = y, \phi(y)}}{(x-y)^2 \leq 0, \phi(x) \vdash x = y, \phi(y)} \qquad W_L \dfrac{\dfrac{*}{x = y, \phi(x) \vdash \phi(y)}}{(x-y)^2 \leq 0, x = y, \phi(x) \vdash \phi(y)}}{(x-y)^2 \leq 0, \phi(x) \vdash \phi(y)}}{(x-y)^2 \leq 0 \wedge \phi(x) \vdash \phi(y)}}{\vdash ((x-y)^2 \leq 0 \wedge \phi(x)) \to \phi(y)}
$$

This practice of weakening/hiding and then applying QE is extremely helpful to save time in your proof attempts!