15-424/15-624 Recitation 3
Did you prove what you meant to prove?

Mostly copied over from last year's notes! Thanks Sarah and Joao!

1. **Examples**

What's the difference between the following hybrid programs α, β, and γ?

$$\alpha \equiv \{x' = v, v' = a \ \& \ v \geq 0\}$$

$$\beta \equiv \{x' = v, v' = a \ \& \ v \geq 0\}; ?(v = 0) \quad \text{(Bad idea! See below.)}$$

$$\gamma \equiv t := 0; \{x' = v, v' = a, t' = 1 \ \& \ t \leq T\}; ?(t = T)$$

$\phi(x, v)$:

Now let $\phi(x, v)$ be a property that holds after (or in some cases during) the execution of each of these hybrid programs. In the remainder of these notes, I will use ϕ and $\phi(x, v)$ interchangeably. We write ϕ so that it explicitly depends on state variables x, v because these are the only continuously evolving variables. They describe the physical state of the system. Most often the properties we want to prove are focused on the continuous state variables of the system. That doesn't mean other variables won't also be used, but the state variables are crucial.

$[\alpha]\phi(x, v)$:

Suppose you have found a proof of property $[\alpha]\phi(x, v)$. This means that $\phi(x, v)$ holds at the end of every run of the hybrid program. Since α can stop at all possible times such that the evolution domain $v \geq 0$ still holds, we've actually ensured that property $\phi(x, v)$ holds throughout the nondeterministic evolution. This is great, since we often want to prove properties about the system for the entire time it runs, rather than just when it stops.

$[\beta]\phi(x, v)$:

Now suppose you have found a proof of property $[\beta]\phi(x, v)$. Again, this means that $\phi(x, v)$ holds at the end of every run of β; HOWEVER, some runs of β have been omitted, specifically whenever the velocity does not end with value exactly zero. This means, first, that $\phi(x, v)$ only holds at the end of the run, not necessarily throughout. But it has the bad and unintended effect that if you happen to have set your acceleration to be a positive value, and if velocity starts positive, too, then your system will never brake to a stop, so it is excused from satisfying property $\phi(x, v)$. In general, it is a bad idea to add tests that guard on state variables (like x, v in this example), because those are the variables that we want to prove properties about.

$[\gamma]\phi(x, v)$:

In this case, we still have a guard, but it is on time instead of on the system state. The variable t has simple and well defined dynamics, so we aren't too worried about it exhibiting unexpected behaviour. Additionally, forcing the evolution to stop only after it has evolved for some minimum time is a behaviour we can actually build into the real cyber-physical system. Compare this to trying to build a system that has to force the velocity of a robot to be zero. Now, even though this is a system we can actually implement, we still have to be careful in proving properties about it. Because we have

disallowed runs that evolve for less time than T, the property is no longer guaranteed to hold at those times.

If we removed the test, then we'd be saying that the property had to hold throughout all durations up to T. Typically, these programs are repeated using α^*, which means that at most time T will pass before the program loops again. The idea is that in real systems, the control loop is guaranteed to run every T time units, thus keeping the CPS safe. Without a bound on how often the controller must execute it would be impossible to guarantee any safety properties!

Executive Summary:

Suppose we have found proofs for $[\alpha]\phi$, $[\beta]\phi$, and $[\gamma]\phi$. Then, property ϕ holds *throughout all* executions of α. Property ϕ only holds at the *end of some* (but not all) executions of β. And property ϕ holds at the *end of all* executions of γ.

Generally we want to prove things throughout all executions of a hybrid program, so we design our HPs to look like α. Sometimes we want to prove properties that hold only at the end of a hybrid program, so we design our HPs to look like γ. We NEVER want to prove a property that only holds sometimes, so we avoid including tests on state variables, like in β.

2. **Soundness.**

Why do we want this, to verify that our axioms are true from any state. - Essentially allows us to do proofs, transition from HP syntax to logic, easier to do proofs with
Soundness ensures that axiom will be true for all instances (alphas, beta, gammas, Ps and Qs).

Here goes a quick, direct, formal proof of the $\cup$ axiom.

$$[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \wedge [\beta]\phi$$

The axiom is of the form $\phi_1 \leftrightarrow \phi_2$. The idea is to apply the semantics definitions of the formulas and programs to one side, say ϕ_1 until we reach a clear understanding of what the formula means (in a combination of math and English). Then we shuffle that understanding around a bit to get the meaning of ϕ_2, and then syntactically rebuild ϕ_2 from the semantics.

Let's try it! To prove the axiom is sound, we must show it holds for all states ν. To prove an equivalence, we have to prove implication from both sides. Let's start with $[\alpha \cup \beta]\phi \rightarrow [\alpha]\phi \wedge [\beta]\phi$.

Let ν be an arbitrary state. Assume $\nu \models [\alpha \cup \beta]\phi$.

$\nu \models [\alpha \cup \beta]\phi$	iff
for all ω such that $(\nu, \omega) \in [\![\alpha \cup \beta]\!]$, then $\omega \models \phi$	iff
for all ω such that $(\nu, \omega) \in [\![\alpha]\!] \cup [\![\beta]\!]$, then $\omega \models \phi$	iff
for all ω such that $(\nu, \omega) \in [\![\alpha]\!]$ or $(\nu, \omega) \in [\![\beta]\!]$, then $\omega \models \phi$	iff
for all ω such that $(\nu, \omega) \in [\![\alpha]\!]$ then $\omega \models \phi$ and for all ω such that $(\nu, \omega) \in [\![\beta]\!]$ then $\omega \models \phi$*	iff
$\nu \models [\alpha]\phi$ and $\nu \models [\beta]\phi$	iff
$\nu \models [\alpha]\phi \wedge [\beta]\phi$	

But 'lo and behold, all of the steps are in fact equivalences! So instead of proving a single direction of the equivalence, we actually proved both directions at once. This isn't always the case, so be careful!

And that's how you do a no-bullsh*t axiom proof!

*Note: We can do this because: A or B $\implies$ C iff (A $\implies$ C) and (B $\implies$ C)

Additional example with composition axiom:

$$([;]): \quad [\alpha;\beta]\phi \leftrightarrow [\alpha][\beta]\phi$$

Let ν be a state. Assume $\nu \models [\alpha;\beta]\phi$.

$\nu \models [\alpha;\beta]\phi$ iff
for all ω s.t. $(\nu,\omega) \in [\![\alpha;\beta]\!]$, $\omega \models \phi$ iff
for all ω_0 s.t. $(\nu,\omega_0) \in [\![\alpha]\!]$, then for all ω s.t. $(\omega_0,\omega) \in [\![\beta]\!]$, $\omega \models \phi$ iff
for all ω_0 s.t. $(\nu,\omega_0) \in [\![\alpha]\!]$, then $\omega_0 \models [\beta]\phi$ iff
$\nu \models [\alpha][\beta]\phi$

Since these are all equivalences, then both directions of the axiom hold.

3. **Quiz**

Suppose you have a proof for the following $\mathsf{d}\mathcal{L}$ formula:

$$\begin{array}{l}[t := 0;\\ \ \{x' = v, v' = a, t' = 1 \ \&\ t \leq T\};\\ \ ?(t = T);\\ \ \{x' = v, v' = a, t' = 1\}]\ \phi(x,v)\end{array}$$