15-424/15-624 Recitation 3: Did you prove what you meant to prove?
15-424/15-624 Foundations of Cyber-Physical Systems
Course TA: Sarah Loos (`sloos+fcps@cs.cmu.edu`)

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 behavior. Additionally, forcing the evolution to stop only after it has evolved for some minimum time is a behavior we can actually build into the 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. (More about this in a much later part of the course...)

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.**

   See notes for lecture 5 on soundness. Section 3 covers soundness of $\cup$, which we reviewed in recitation.

   `http://symbolaris.com/course/fcps13/05-dynax.pdf`

3. **Quiz**

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

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

   For what values of t do you know that your hybrid program ensures the property $\phi(x, v)$?

   Solution: Property ϕ holds for all $t \ge T$. Because the guard $?(t = T)$ only allows runs where the first differential equation evolved for exactly T time, the hybrid program can only terminate at or after $t = T$.