LFCPS Exercise Class 2
Verifying cyber-physical systems

Exercise 1 (Semantics Review)**.** *For each of the following* dℒ *formulas, determine whether they are valid, satisfiable,* and/or *unsatisfiable:*

1. $[?\text{true}]\text{true}$.
2. $[?\text{true}]\text{false}$.
3. $[?\text{false}]\text{true}$.
4. $[?\text{false}]\text{false}$.
5. $[x' = 1 \,\&\, \text{true}]\text{true}$.
6. $[x' = 1 \,\&\, \text{true}]\text{false}$.
7. $[x' = 1 \,\&\, \text{false}]\text{true}$.
8. $[x' = 1 \,\&\, \text{false}]\text{false}$.
9. $[(x' = 1 \,\&\, \text{true})^*]\text{true}$.
10. $[(x' = 1 \,\&\, \text{true})^*]\text{false}$.
11. $[(x' = 1 \,\&\, \text{false})^*]\text{true}$.
12. $[(x' = 1 \,\&\, \text{false})^*]\text{false}$.
13. $[(x := x + 1; x' = -1)^*; ?x > 0; x' = 2]$ $x > 0$

Exercise 2. *Replace α with a concrete HP that makes the following* dℒ *formulas valid or explain why such an HP does not exist. For an extra challenge do not use assignments in α.*

1. $[\alpha]\text{false}$
2. $[\alpha^*]\text{false}$
3. $[\alpha]x > 0 \leftrightarrow \langle\alpha\rangle x > 0$
4. $[\alpha]x > 0 \leftrightarrow [\alpha]x > 1$
5. $[\alpha]x > 0 \leftrightarrow \neg[\alpha \cup \alpha]x > 0$
6. $[\alpha]x = 1 \wedge [\alpha]x = 2$

Exercise 3. *Consider the bouncing ball model from the lecture. Identify all requirements that imply the following formula, in which the bouncing ball might deflate and lie flat.*

$$\big[\big(\{x' = v, v' = -g \,\&\, x \geq 0\}; \texttt{if}(x = 0)\,(v := -cv \cup v := 0)\big)^*\big](0 \leq x \leq H)$$

Differential Dynamic Logic for Verification

Exercise 4. *The axioms of dynamic logic are also useful to prove the correctness of discrete programs. Find a way of proving the following formula which expresses that a triple of clever assignments swaps the values of two variables in place:*

$$x = a \wedge y = b \rightarrow [x := x + y;\ y := x - y;\ x := x - y](x = b \wedge y = a)$$

Exercise 5 (Proof practice)**.** *Give* dℒ *sequent calculus proofs for the following formulas:*

1. $x > 0 \wedge v \geq 0 \rightarrow [x := x + 1 \cup x' = v]x > 0$
2. $x^2 \geq 100 \rightarrow [(?x > 0; x' = 2) \cup (?x < 0; x' = -2)]x^2 \geq 100$

Exercise 6. *Let $y(t)$ be the solution at time t of the differential equation $x' = f(x)$ with initial value $y(0) = x$. The following sequent proof rule, which checks the evolution domain $q(x)$ at the end, is sound:*

$$\frac{\Gamma \vdash \forall t{\geq}0\,\big([x := y(t)](q(x) \rightarrow p(x))\big), \Delta}{\Gamma \vdash [x' = f(x) \,\&\, q(x)]p(x), \Delta}$$

Would the following also be a sound axiom? Prove or disprove.

$$[x' = f(x) \,\&\, \psi]\varphi \leftrightarrow \forall t{\geq}0\,\big([x := y(t)](\psi \rightarrow \varphi)\big)$$

Test in Modeling CPSs

Exercise 7. *Correctness arguments for cyber-physical system models can only be as good as the logic that is used to justify them, which is why it is so essential that differential dynamic logic is sound. The proofs are also only as good as the implementation of the verification tool in which the correctness proof was conducted, which is why it is so important that KeYmaera X has a small and trustworthy prover microkernel. However, the cyber-physical systems themselves are also only as safe as the model used for their verified conjectures was accurate, which is why it is so important to exercise caution and good judgment in modeling. While modeling real systems is never easy, some modeling pitfalls are especially important to guard against.*

One source of modeling pitfalls are tests, which, after all, are assumptions on the execution of the system. Tests are harmless when they are merely used to control which branch of execution through the model is taken under what circumstance. Tests are significant restrictive assumptions, however, if there is no other branch to execute if they fail, because they, thus, assume their condition to hold and discard all runs that violate them. An example of a fine use of tests is the following:

$$(?v \geq 5; a := a + 1 \cup ?v \leq 5; a := -5); \{x' = v, v' = a \,\&\, v \geq 0\}$$

The left branch in the controller assumes that $v \geq 5$ holds, which at first sounds like a significant assumption. But its sibling, the right branch of the controller assumes that $v \leq 5$ holds. Obviously, every state will pass one of the two tests, so no run will ever be discarded by the controller. And states that satisfy both assumptions $v \geq 5$ and $v \leq 5$ because $v = 5$ even pass both tests and may, thus, run either branch. There is still another assumption in the model, though, that discards runs. Can you spot it?

An example of a restrictive test is the following:

$$(?v \leq 10; a := a + 1 \cup ?v \leq 5; a := -5); \{x' = v, v' = a \,\&\, v \geq 0\}$$

While this HP branches equally fine, the branches jointly still simply assume that the velocity v is at most 10, and thus discard all runs of the HP from very fast initial velocities. The same problem arises in a loop even if the initial velocity is assumed to be slow:

$$((?v \leq 10; a := a + 1 \cup ?v \leq 5; a := -5); \{x' = v, v' = a \,\&\, v \geq 0\})^*$$

These restrictive tests silently assume slow velocities, and, thus, repetition is entirely impossible after following the differential equation with a positive velocity for a long time.

A general rule of thumb is that tests that have a sibling that supposes the opposite, or at least whose disjunction of tests is valid, are harmless, because they merely control which branch is chosen when. But tests without such a sibling may be restrictive.

Which assumptions in the following HP are harmless or restrictive, respectively?

$$(?v \geq 5; a := a + 1; \{x' = v, v' = a \,\&\, v < 5\} \cup ?v \leq 5; a := -5; \{x' = v, v' = a \,\&\, v \geq 5\})^*$$