Assignment 2: Loops and Proofs
15-424/15-624/15-824 Logical Foundations of Cyber-Physical Systems

TAs: Irene Li (mengzeli@andrew.cmu.edu)
Yong Kiam Tan (yongkiat@cs.cmu.edu)

Revision (September 26th, 4:30PM): Question 3, removed colons next to axiom names.
Revision (September 17th, 5:30PM): Question 6, added $t' = 1$ to ODEs in the last part.
Due Date: Thursday, September 27th, 11:59PM (no late days), worth 60 points

1. **Searching for validation!** For each of the following formulas replace α with a concrete hybrid program, or ODE with a concrete ODE that makes the resulting formula valid.

   If such a program/ODE cannot exist, briefly explain (in 1-2 sentences) why. Oh, and it looks like your ':=' key is broken, so your programs must not use assignments (e.g., $x := 5$)

   (a) $[\alpha]\mathit{false}$

   (b) $[\alpha^*]\mathit{false}$

   (c) $x = 5 \rightarrow [\{ODE \,\&\, x \leq 5\}]\mathit{false}$

   (d) $\langle\{ODE \,\&\, x \geq 10\}\rangle x \geq 10 \leftrightarrow \langle\{x' = v, v' = 1\}; ?x \geq 10\rangle x \geq 10$

   (e) $[\alpha]x > 1 \leftrightarrow [\alpha]x > 2$

   (f) $[t := 50; \{t' = 1 \,\&\, t \leq 10\}; \alpha]t = 10$

2. **Semantics: What does it actually mean?** In the previous assignment, you defined the if-then-else and switch statements. Now, let us extend the syntax of hybrid programs with three new operators:

$$\alpha, \beta ::= \cdots \mid \alpha^+ \mid \alpha^\# \mid \textbf{try } \alpha \textbf{ otherwise } \beta$$

   As we have emphasized when defining the syntax and semantics of terms, formulas and programs, these new syntactic operators have no inherent meaning. We must also define their semantics, which is given as follows:

$$[\![\alpha^+]\!] = \{(\omega, \nu) \mid (\omega, \nu) \in \textstyle\bigcup_{n\in\mathbb{N}} [\![\alpha^{n+1}]\!]\}$$
$$[\![\alpha^\#]\!] = \{(\omega, \nu) \mid (\omega, \nu) \in \textstyle\bigcup_{n\in\mathbb{N}} [\![\alpha^{2n+1}]\!]\}$$
$$[\![\textbf{try } \alpha \textbf{ otherwise } \beta]\!] = \{(\omega, \nu) \mid (\omega, \nu) \in [\![\alpha]\!] \text{ or } \big((\omega, \nu) \notin [\![\alpha]\!] \text{ and } (\omega, \nu) \in [\![\beta]\!]\big)\}$$

   where $\alpha^0 \overset{\text{def}}{\equiv} ?\mathit{true}, \alpha^{i+1} \overset{\text{def}}{\equiv} \alpha^i; \alpha$

   Fortunately, these new operators are already definable in the usual language of hybrid programs. For example, α^+ is the "loop-once-or-more" operator, and it can be defined as $\alpha^+ \overset{\text{def}}{\equiv} \alpha; \alpha^*$. This can be justified using the fact that $[\![\alpha^+]\!] = [\![\alpha; \alpha^*]\!]$.

   For the remaining two operators, similarly define them with hybrid programs that do not use the new operators. Briefly justify your answer (in 1-2 sentences).

3. **Semantic soundness proofs.** Give a proof of soundness for the following axioms *using the semantics* of formulas and hybrid programs.

   (a) ([?]) $[?H]\phi \leftrightarrow (H \rightarrow \phi)$

   (b) ($\langle\vee\rangle$) $\langle\alpha\rangle(\phi \vee \psi) \leftrightarrow \langle\alpha\rangle\phi \vee \langle\alpha\rangle\psi$

   (c) ([$*$;]) $[(\alpha)^*]\phi \leftrightarrow \phi \wedge [\alpha;(\alpha)^*]\phi$

   (d) **Bonus.** ($\langle**\rangle$) $\langle\alpha^*;\alpha^*\rangle\phi \leftrightarrow \langle\alpha^*\rangle\phi$

   Hint: Follow the process used in class: consider an axiom of the form $\phi_1 \leftrightarrow \phi_2$. To prove the axiom sound, let ω be an arbitrary state. It suffices to show that $\omega \in [\![\phi_1]\!]$ iff $\omega \in [\![\phi_2]\!]$. Now, unfold $\omega \in [\![\phi_1]\!]$ using the various definitions of the semantics until you have gotten rid of the syntax. Then, work backwards, again using the semantics to add back syntax until you get to $\omega \in [\![\phi_2]\!]$. Most of the time, you should be reasoning with if-and-only-if steps, which means you are already done! If not, repeat the process in the other direction, i.e., starting from $\omega \in [\![\phi_2]\!]$ and ending with $\omega \in [\![\phi_1]\!]$ instead.

4. **ODE soundness proofs.** For this question, assume that $y(t)$ is the unique *global* solution to the ODE $x' = f(x)$, i.e., a solution which exists for all $t \in [0,\infty)$ and obeys $y'(t) = f(y)$.

   (a) Prove that this axiom is sound using the semantics of differential equations:[1]

   $$[\{x' = f(x) \,\&\, Q\}]\phi \leftarrow \forall t\,[x := y(t)]\phi$$

   (b) The following candidate axioms are different versions of the ODE solve axiom [′]. Which, if any, are sound? Explain your answer (intuitively – a proof is not required!).

   $$[\{x' = f(x) \,\&\, Q\}]P \leftrightarrow \forall t{\geq}0 \left(([x := y(0)]Q \wedge [x := y(t)]Q) \rightarrow [x := y(t)]P\right)$$

   $$[\{x' = f(x) \,\&\, Q\}]P \leftrightarrow \forall t{\geq}0 \left((\forall 0{\leq}s{\leq}t\,[x := y(s)]Q) \rightarrow [x := y(t)]P\right)$$

5. **Inevitability of invariants.** Remember Lab 1? Wasn't that fun? Let's add stars to make it even *more* fun! In real cyber-physical systems, control isn't executing all the time. CPS controllers typically poll sensors and decide on what to do at regular intervals. As a step in this direction, in this exercise, we allow continuous evolution to happen for at most time T.

   $vel > 0 \wedge pos < station \wedge T > 0 \wedge acc = \_\_\_\_\_\_ \rightarrow$
   $[(t := 0; \{pos' = vel, vel' = acc, t' = 1 \,\&\, vel \geq 0 \wedge t \leq T\})^*](vel = 0 \rightarrow pos = station)$

[1] Note the backward implication symbol: $P \leftarrow Q \overset{\text{def}}{\equiv} Q \rightarrow P$, which we will occasionally use in this course.

(a) Find an initial condition for acc for which the robot will stop at exactly the station. If your robot was efficient, you already solved this in Lab 1!

(b) There is no guarantee that the robot will stop within one execution of the loop, because the domain constraint $t \leq T$ allows continuous evolution to happen for *at most* time T but not *definitely* time T.

Multiple loops of the program might be required before the car does actually stop. But we have no clue how many! What do we do? *Invariants to the rescue!* Recall that an invariant of α^* is true no matter how many iterations of α execute. If it holds before α executes, it holds after α executes. Invariants will generally relate the different state variables in a way that isn't altered by the dynamics.

Find an invariant for this system that lets you prove the postcondition.

Hint: The invariant is tied to the physical dynamics.

(c) To simplify, let

- $Pre \equiv vel > 0 \land pos < station \land T > 0 \land acc = \underline{\hspace{3em}}$
- $\alpha \equiv t := 0; \{pos' = vel, vel' = acc, t' = 1 \,\&\, vel \geq 0 \land t \leq T\}$

Rewriting the above formula, we obtain $Pre \to [\alpha^*](vel = 0 \to pos = station)$, which we will try to prove.

$$\to_R \dfrac{?\;\dfrac{?}{Pre \vdash [\alpha^*](vel = 0 \to pos = station)}}{\vdash Pre \to [\alpha^*](vel = 0 \to pos = station)}$$

Which rule would you apply next? Give a brief explanation of why each resulting branch is valid (you do not need to show us the proof).

Hint: Recall that rules can only be applied to the main formula (i.e., the outermost operator in the formula), not to smaller sub-formulas.

6. **Practice makes for perfect proofs.**

In each of the following sub-problems, you are given a valid sequent in the conclusion. We want you to finish the first step of a proof for that sequent using the proof rules of dL. You should use proof rules available in KeYmaera X:

`http://keymaerax.org/KeYmaeraX-sheet.pdf`

Hint: For this question and the next, feel free to use KeYmaera X to check your answers. This will give you some additional practice with doing manual proofs in KeYmaera X.

In some cases we will tell you which rule to use, but the rule takes an argument (e.g., an invariant). In these cases make sure to specify what the argument is. In other cases we will not say which rule to use, so make sure to include the name of the rule. In each case, make sure that your instantiation is not only syntactically correct, but that the instantiation you chose makes it possible to prove the property.

$$\text{(PART A)}\ \frac{(PARTB) \qquad x^2y \geq 0 \land x \geq 0 \land z \geq x \vdash [x := 2x][y := 2y]xy \geq 0, y \geq 0}{x^2y \geq 0 \land x \geq 0 \land z \geq x \vdash [x := 2x][y := 2y]xy \geq 0}$$

$$\texttt{hide left (a.k.a. WL)}\ \frac{(PARTC)}{x^2y \geq 0, x \geq 0, z \geq x \vdash [x := 2x][y := 2y]xy \geq 0}$$

$$\text{(PART D)}\ \frac{(PARTE) \vdash v = 0}{\forall x\, x^2 = y^2 + 2v \vdash v = 0}$$

$$\texttt{loop}\ \frac{(PARTF) \qquad (PARTG) \qquad (PARTH)}{x = 0 \vdash [(x := x + 1)^*]x \neq -1}$$

$$\texttt{loop}\ \frac{(PARTI) \qquad (PARTJ) \qquad (PARTK)}{B > 0, T > 0, t > 0, (PARTL) \vdash [(a := B \cup a := 0; \{x' = v, v' = a, t' = 1 \,\&\, t \leq T\})^*]v \geq 0}$$

7. **Loopholes in loop invariants.** After getting through the first few questions on this homework, you decided that you love loop invariants so much, you will teach them to your friend. When teaching them to your friend, assume you are using the basic `loop` rule given in lecture (i.e. you do not have any extra magic that might be provided by KeYmaera X):

$$\texttt{loop}\ \frac{\Gamma \vdash J, \Delta \qquad J \vdash [\alpha]J \qquad J \vdash P}{\Gamma \vdash [\alpha^*]P, \Delta}$$

You start with a simple system:

$$x \geq 0 \vdash [(x := 5 \cup x := 3)^*]x > 0$$

Your friend exclaims, the invariant is just $x > 0$!

(a) After applying the `loop` rule with this invariant, one of the resulting premises will not be provable. Which premise breaks down, why, and what do you have to do to fix it?

You decide to challenge your friend with a more complicated system:

$$x > 0 \land a > 0 \land A > 0 \land v \geq 0 \vdash [((a := 0 \cup a := A); \{x' = v, v' = a\})^*]x \geq 0$$

Your friend, ever so quick to jump to conclusions, suggests the invariant $x \geq 0$.

(b) After applying the loop rule with this invariant, the proof will eventually break down. Which part breaks down and what do you have to do to fix it?

(c) To show off your skills, you decide to prove the whole formula:

$$\texttt{loop}\ \frac{YourProofGoesHere}{x \geq 0 \land a > 0 \land A > 0 \land v \geq 0 \vdash [((a := 0 \cup a := A); \{x' = v, v' = a\})^*]x \geq 0}$$

8. **The one where robots go back and forth.** In the previous lab, our robot moved to the charging station and stopped. What if instead we had a robot that moves back and forth between two walls (say one is at 0 and one is at W)? How would we model this system?

First, let us consider what we want to prove about this model:

(a) What safety and efficiency conditions would you use?

(b) What continuous dynamics will you use? (How do you model the motion?)

(c) What controls would the robot use? (Should it be able to accelerate or brake?)

(d) Using the first three parts of the question, write a complete dL formula to model this situation.

Note: This question is designed to be a little open-ended: you might think of it as practice for what you will eventually need to do in the course project! Thus, feel free to make design decisions that you deem appropriate. At the same time, accurate models are a crucial part of CPS verification, so make sure that your formula sets out to prove meaningful properties.