Assignment 5: Hybrid Games and Uniform Substitutions
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 (November 3rd, 2:00PM): Question 5c: added braces around the ODEs for clarity.
Revision (November 12th, 12:00PM): Question 5e: typo in question. If you have already answered it for the original question, there is no need to change your answer (as long as it makes sense for the original question).
Due Date: Thursday, November 15th, 11:59PM (no late days), worth 60 points
Early Submission Due Date: Tuesday, November 13th, 11:59AM
Important Note: This assignment is due on the day of the final exams so you will not have a chance to receive feedback for it before the exams. If you submit it by the early submission due date, we will try to give you feedback on as many questions as we can.

1. **Games, proof edition.** For the hybrid games in the previous assignment, you had to figure out a winning strategy, but did not need to figure out a proof. For this question, let's do the latter!

   Your task is to prove the following formula using the axioms and proof rules of dGL:

   $$x = 0 \land i = 0 \rightarrow \langle (i := i + 1; (x' = 1 \cap x' = 2))^{\times} \rangle (x \geq 2 \cdot i \land x \leq 4 \cdot i)$$

   In this game, Demon controls how long the loop runs and Angel wants to make sure x is high enough (increases by at least 2 each time the loop runs). Each time the loop runs, Demon tells Angel which ODE to execute, but both ODEs increase x and Angel controls the duration. Thus Angel can always increase x by 2 so long as she sets the duration high enough. We confess this is not the most fun game but sadly the alternative of having a really fun game would result in a really not-fun experience doing your first-ever games proof.

   Hint:

   - All the Demon operators like $\alpha^{\times}$ and $\alpha \cap \beta$ can be defined using the dual operator α^d. We strongly recommend you rewrite the above formula using the dual operator to avoid silly mistakes.
   - Make sure to double-check that you have the right player making the choices at each point in the game.
   - Most proof rules that we had for hybrid programs also work for hybrid games. The exceptions are given in LFCPS Chapter 17.
   - "Most proof rules" includes the induction rule for loops.

2. **Games, (in)variants edition.** In this problem, we are not going to make you do any more proofs (unless you choose to do so). Instead we will give you hybrid games and ask you for an invariant (or variant) from which the desired property follows.

(a) For this problem, define:

$$\begin{aligned}\alpha_1 &\equiv \{x' = v, v' = a, t' = 1 \,\&\, t \le T\}\\ \alpha_2 &\equiv \{x' = v, v' = -B, t' = 1 \,\&\, v \ge 0\}\\ \alpha &\equiv t := 0; a := *; ?(0 \le a \wedge a \le A); T := *^d; ?(T > 0)^d; (\alpha_1 \cup \alpha_2)\end{aligned}$$

The rules of the game can be read as follows:

i. Angel picks an acceleration: $a := *; ?(0 \le a \wedge a \le A)$

ii. Demon picks a positive timestep: $T := *^d; ?(T > 0)^d$

iii. Angel then gets to either accelerate with acceleration a, or apply the brakes at $-B$ indefinitely until a stop.

Demon has a strategy to make the following formula valid, i.e. to win the game by preventing Angel from reaching the station, even though Angel is in control of the loop (α^*):

$$A > 0 \wedge B > 0 \wedge v = 0 \wedge x < \mathit{station} \rightarrow [\alpha^*] x < \mathit{station}$$

What is Demon's invariant? Briefly explain why the invariant works.

(b) For this problem, define:

$$\begin{aligned}\alpha_1 &\equiv (T := \frac{T}{2} \cap v := -v); (T := 2T \cup v := -v); t := 0\\ \alpha_2 &\equiv \{x' = v, t' = 1 \,\&\, t \le T\}\\ \alpha &\equiv \alpha_1; \alpha_2\end{aligned}$$

The rules of this game can be read as follows:

i. There is a time limit T on how long the ODE can run.

ii. Demon can either halve the time limit or flip the direction of movement $T := \frac{T}{2} \cap v := -v$

iii. Angel can either double the time limit or flip the direction of movement $T := 2T \cup v := -v$

iv. Angel then gets to follow the ODE for at most T time units.

Angel has an easy winning strategy: just undo what Demon does at each loop iteration. In other words, the following formula is valid:

$$T > 0 \wedge v > 0 \rightarrow \langle \alpha^* \rangle x \ge \mathit{station}$$

To prove this formula, we can use the *loop convergence* rule:

$$\text{(con)} \quad \frac{\Gamma \vdash \exists \tau\, p(\tau), \Delta \qquad \vdash \forall \tau{>}0\, (p(\tau) \rightarrow \langle \alpha \rangle p(\tau - 1)) \qquad \exists \tau{\le}0\, p(\tau) \vdash Q}{\Gamma \vdash \langle \alpha^* \rangle Q, \Delta} \quad (\tau \notin \alpha)$$

If you were to do a full proof for Angel, you would start by applying the convergence rule con with a choice of the loop variant $p(v)$. State a *loop variant* $p(v)$ that can be used to prove the formula, and briefly explain why all 3 resulting premises of the rule are valid.

Hint: Convergence properties have been covered in less detail in the lectures. You may wish to read LFCPS Chapter 17.4 for a more in depth discussion. Since you have less exposure to this material, it may be best to save this part of the question for last if you get stuck.

(c) **Bonus.** This question is optional. Its main purpose is for groups working on projects related to hybrid games to gain some practice with proving them in KeYmaera X. Your task is to prove the formulas from the previous parts in KeYmaera X. For your convenience, we have written the formulas in KeYmaera X syntax below. `^@` is KeYmaera X syntax for the dual operator:

i.

```
A > 0 & B > 0 & v = 0 & x < station
->
[{
  t:=0; a:=*; ?(0 <= a & a <= A);
  {T:=*; ?(T > 0);}^@
  {{x'=v,v'=a,t'=1 & t<=T} ++ {x'=v,v'=-B,t'=1 & v >= 0}}
}*]
x < station
```

ii.

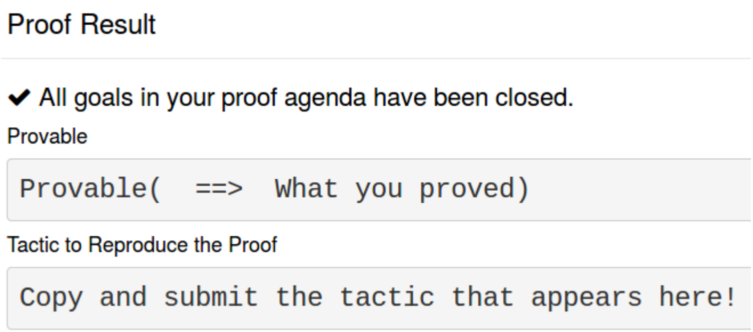
```
T > 0 & v > 0
->
<{
  {T := T/2; ++ v:=-v;}^@
  {T := 2*T; ++ v:=-v;}
  {t:=0;}
  {x'=v,t'= 1 & t <= T}
}*>
x >= station
```

Copy and submit the text of your tactic for both questions (see Figure 1).

3. **Taylor series, KeYmaera X edition.** For this problem, we will again explore upper and lower bounds for e^t, whose Taylor series is given by:

$$e^t = 1 + t + \frac{t^2}{2!} + \frac{t^3}{3!} + \dots$$

Recall that you proved a lower bound on e^t in the last assignment. As we start using more terms in the Taylor series expansion, it becomes much more convenient to use



Proof Result

✔ All goals in your proof agenda have been closed.

Provable

```
Provable(  ==>  What you proved)
```

Tactic to Reproduce the Proof

```
Copy and submit the tactic that appears here!
```

Figure 1: Submit tactic text for KeYmaera X proofs.

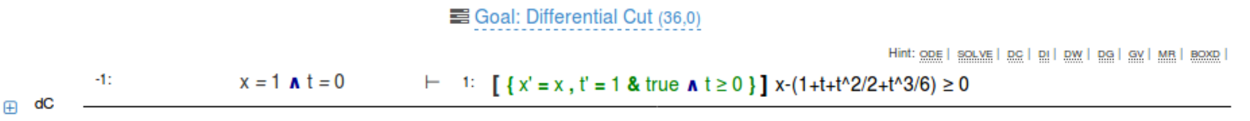
KeYmaera X to automate your proof. We will use this opportunity to learn about an advanced tactic that you might need for your course projects.

(a) Prove the following formula in KeYmaera X:

```
x=1&t=0->[{x'=x,t'=1}]x-(1+t+t^2/2+t^3/6)>=0
```

Here is a step-by-step guide to the proof:

i. First, use a differential cut to add $t \geq 0$ to the domain constraint. Your goal should look like this after the cut:



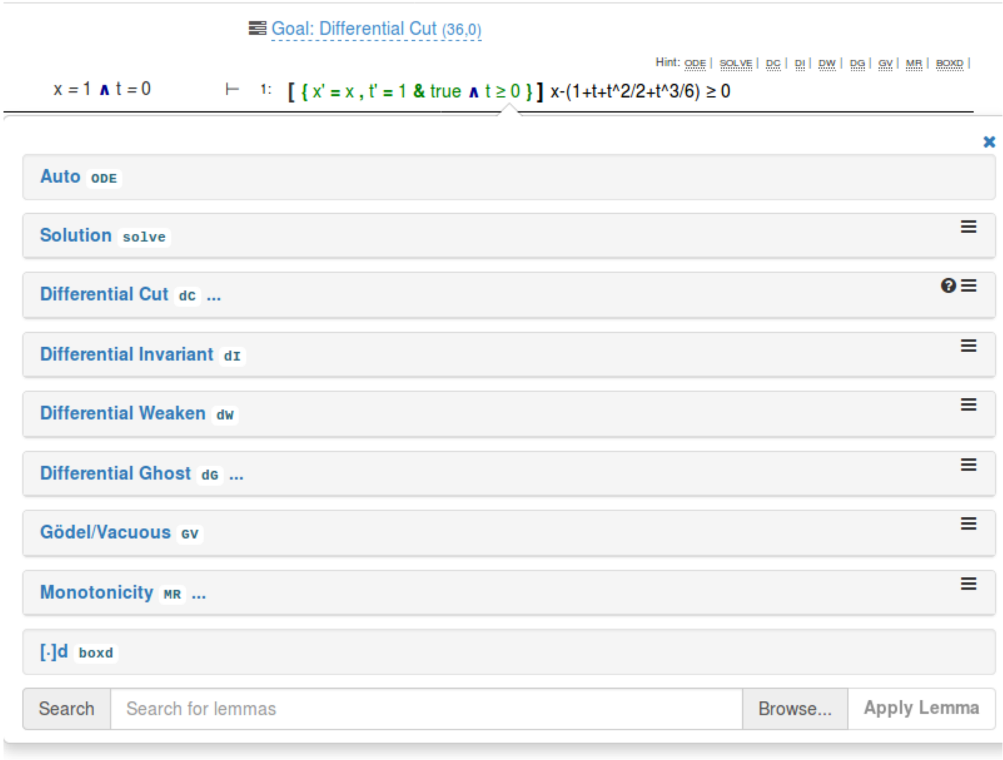
Goal: Differential Cut (36,0)

Hint: ODE | SOLVE | DC | DI | DW | DG | GV | MR | BOXD |

```
-1:   x = 1 ∧ t = 0   ⊢   1:  [ { x' = x , t' = 1 & true ∧ t ≥ 0 } ] x-(1+t+t^2/2+t^3/6) ≥ 0
```

⊞ dC

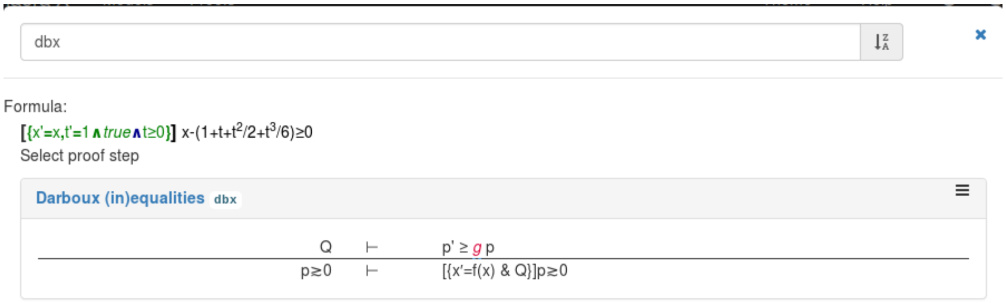
ii. Now, right-click on the ODE in the succedent, and select `Browse...`



Goal: Differential Cut (36,0)

x = 1 ∧ t = 0 ⊢ 1: [{ x' = x , t' = 1 & true ∧ t ≥ 0 }] x-(1+t+t^2/2+t^3/6) ≥ 0

iii. In the search box, type `dbx` and you should see a proof rule called "Darboux (in)equalities". This is a tactic that automatically uses differential ghosts to prove advanced properties of differential equations. Expand the rule information for `dbx` by clicking on ☰:



dbx

Formula:
[{x'=x,t'=1 ∧ *true* ∧ t≥0}] x-(1+t+t^2/2+t^3/6)≥0

Select proof step

Darboux (in)equalities dbx

$$\frac{Q \vdash p' \geq g\, p}{p \geq 0 \vdash [\{x'=f(x)\ \&\ Q\}]p \geq 0}$$

The following discussion is advanced material. You are not required to know this, but it is here for completeness in case you would like to understand how the proof works in more detail or if you need to use this in your projects.
This rule says that in order to prove $p \geq 0$ (or $p > 0$) invariant, it suffices to prove that $[x' := f(x)](p)' \geq gp$ for some cofactor polynomial g.[1] Notice that

[1] Recall that dI would require you to prove $(p)' \geq 0$ in the postcondition instead.

the cofactor polynomial g has to be supplied to the tactic as an argument. In this case, we can do a rough calculation (assuming $x' = x, t' = 1$ and using the domain constraint $t \geq 0$ for the last inequality):

$$\overbrace{(x - (1 + t + \frac{t^2}{2} + \frac{t^3}{6}))'}^{p'} = x - (1 + t + \frac{t^2}{2}) \geq \overbrace{1}^{g} \cdot \overbrace{(x - (1 + t + \frac{t^2}{2} + \frac{t^3}{6}))}^{p}$$

So we can apply the rule by choosing g to be 1.

iv. Click on g, type `1`, press "Enter", and run the tactic. The proof should be completed.

v. Copy and submit the text of your tactic (see Figure 1).

(b) Since e^t grows faster than any polynomial function as $t \to \infty$, it is impossible to prove a polynomial upper bound on it for all $t \geq 0$. It is possible, however, if we restrict ourselves to a bounded time interval like $t \leq 1$.

Prove the following formula in KeYmaera X:

```
x=1&t=0->[{x'=x,t'=1&t<=1}]x<=1+t+t^2/2+t^3/4
```

Submit the final proof tactic like you did for the previous part of this question. **Hint:** A very similar proof should work for this question, but you have to normalize the postcondition to have 0 on one side of the inequality first in order to use `dbx` in your proof. (How?)

Together with the previous part of this question, this proves the following approximation to e^t on the interval $0 \leq t \leq 1$:

$$1 + t + \frac{t^2}{2} + \frac{t^3}{6} \leq e^t \leq 1 + t + \frac{t^2}{2} + \frac{t^3}{4}$$

This bound can be used, for example, to show $1 \leq e^t \leq 2.75$ for $0 \leq t \leq 1$.

(c) **Bonus (very difficult).** In fact, we can make the lower bound on e^t arbitrarily tight by truncating its Taylor series at the t^k term for higher values of k:

$$\sum_{i=0}^{k} \frac{t^i}{i!} \leq e^t$$

Similarly, give an expression involving powers of t up to t^k that is an **upper bound** on e^t on $0 \leq t \leq 1$ and that can be made arbitrarily tight by increasing k. The expression should also be invariant for the ODE, i.e., the following formula should be valid for your expansion for any $k \geq 2$, where $\theta(k)$ is your expression involving the first k powers of t:

$$x \leq \theta(k) \to [\{x' = x, t' = 1 \,\&\, 0 \leq t \leq 1\}]x \leq \theta(k)$$

Hint: There are multiple possible answers. You may wish to check your answer (for some values of k) in KeYmaera X using the `dbx` tactic shown earlier.

4. **Sound axioms v.s. sound proof rules** You should have lots of experience proving *axioms* sound by now: an axiom is sound iff all of its instances are valid.

   In contrast, we say that a *proof rule*:

$$\frac{\Gamma_1 \vdash \Delta_1 \qquad \dots \qquad \Gamma_n \vdash \Delta_n}{\Gamma \vdash \Delta}$$

   is sound iff for all instances of the rule, validity of all of the premises $\Gamma_i \vdash \Delta_i$ (for $i = 1, \dots, n$) implies validity of its conclusion $\Gamma \vdash \Delta$.

   The two notions look similar and can be easily confused. For each of the following pairs of similar-looking axioms (on the left) and proof rules (on the right), state whether the axiom and/or proof rule is sound and briefly explain your answer.

   (a) Gödel Generalization.

$$P \to [\alpha]P \qquad\qquad \frac{\vdash P}{\Gamma \vdash [\alpha]P, \Delta}$$

   (b) Hoare Sequencing.

$$[\alpha]E \land (E \to [\beta]B) \to [\alpha;\beta]B \qquad\qquad \frac{\Gamma \vdash [\alpha]E \qquad E \vdash [\beta]B}{\Gamma \vdash [\alpha;\beta]B, \Delta}$$

   (c) Differential Weakening.

$$(\forall x\,(Q \to P)) \to [\{x' = f(x)\,\&\,Q\}]P \qquad\qquad \frac{\Gamma, Q \vdash P, \Delta}{\Gamma \vdash [\{x' = f(x)\,\&\,Q\}]P, \Delta}$$

5. **Uniform substitution.** For each of the following formulas, identify a corresponding dL axiom from LFCPS Figure 18.2 that matches the shape of the formula. If possible, also give a uniform substitution σ that can be used to prove the formula. If no such substitution exists, briefly explain why a clash would occur for your chosen dL axiom.

   (a) $[x := y^2][y := y^2]x + y \geq 0 \leftrightarrow [y := y^2]y^2 + y \geq 0$

   (b) $[x := z^2][y := x + y]x + y \geq 0 \leftrightarrow [y := z^2 + y]z^2 + y \geq 0$

   (c) $[x := 1][\{x' = x\}]x > 0 \leftrightarrow [\{x' = 1\}]x > 0$

   (d) $x + y > 5 \to [?x = y]x + y > 5$

   (e) $[x := zy; y := zx]x = y + z \leftrightarrow [x := zy][y := zx]x = y + z$