Assignment 5: Play Around with Hybrid Games
15-424/15-624 Foundations of Cyber-Physical Systems
Course TA: Brandon Bohrer (bbohrer@cs)
Revision 2: Q3 edits, second round of Q3a edits

Due: 11:59pm, Thursday, 4/6/2017
Total Points: 70

1. **Games, games, games** Consider the following formulas: a) For which starting states does Angel have a winning strategy? b) Briefly describe her winning strategy. c) (Only applies to games where Angel has a winning strategy in at least some states). Say we let demon pick one hybrid program operator and flip it between being an Angel or Demon operator, e.g. replacing $\alpha \cup \beta$ with $\alpha \cap \beta$ or vice-versa. If he does this, can he make it so that Angel never has a winning strategy, not in any stat?ef

   A warm-up: $\langle (x := 0 \cap x := 1)^\times \rangle x \geq 0$

   Ups and Downs: $\langle ((x := x + 1 \cup (x' = v)^d); (y := y - 1 \cup (y' = w)^d))^* \rangle |x - y| \leq 1$

   A chase: $\langle (w := w \cap w := -w); (v := v \cup v := -v); (x' = v)^d; y' = w \rangle x < y$

2. **Games, proof edition:** For the above problems, we just made you figure out a winning strategy, but didn't make you figure out a proof. For this one, let's do both! 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 they both 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.

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

   Some hints/suggestions:

   - 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. As discussed in recitation, having the wrong player in control can drastically alter the outcome.
   - Most proof rules that we had in hybrid systems also work in games (the exceptions are given in the lecture notes[1]).

[1] `http://symbolaris.com/course/fcps17/19-axiomaticgames.pdf`

- "Most proof rules" includes the induction rule for loops.

3. **Games, Invariants Edition**. In this problem, we're not going to make you do any more proofs, instead we'll give you games and ask you for an invariant (or variant) from which safety should follow.

   - This was just revised a second time. Please read carefully as revision 1 was also wrong. Yay! For this problem, define:

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

     Demon has a strategy to make the following condition true:

$$\text{Pre} \rightarrow [\alpha^*]x \leq \mathit{station}$$

     The rules of this game say that Angel picks an acceleration and Demon picks a timestep. Then Angel gets to either acceleratie for up to that timestep or brake indefinitely. What is Demon's invariant to win the game?

     Note: Since there is more than one strategy, there might be more than one invariant. If so, look for the most general one, meaning the one that captures the most different strategies (or equivalently, allows even the worst of Demon's possibly-many winning strategies).

   - **IMPORTANT:** This problem is significantly broken and the fix might not be so simple, so it is hereby removed from the assignment. I am leaving it in the PDF because some of you will need convergence on your final projects. If you are using convergence on your projects, consider looking at this game and what does/doesn't work, what the fixes to the problemmight be. That debugging process is similar to what you will need while designing and proving your models, and this example is likely simpler.

     For this problem, define

$$\begin{aligned}\alpha_1 &\equiv (T := T/2 \ \cap \ ?\mathit{true}); T_1 := T; (B := B \cdot 4 \ \cup \ ?\mathit{true})\\ \alpha_2 &\equiv \{x' = v, v' = -B, t' = 1 \ \& \ T \geq T_1 - 1 \wedge T \geq 0\}\\ \alpha &\equiv \alpha_1; \alpha_2\end{aligned}$$

     In this game, Angel is racing to reach the station within T seconds (here T is the *time remaining*; the ODE domain constraint says we must not run over time and also must not run more than 1 time unit per iteration). Demon has the option to

reduce the remaining time, but Angel has the option to increase her acceleration. Then Angel has a strategy to make the following formula ψ true:

$$\psi \equiv (x + v \cdot T + B/2 \cdot T^2 = station \wedge T > 0 \rightarrow \langle \alpha^* \rangle x \geq station)$$

Recall the convergence rule from Recitation 9:

$$\text{con}' \frac{\Gamma \vdash \exists v.\varphi(v) \qquad \vdash \forall v \geq 0.\varphi(v) \rightarrow \langle \alpha \rangle \varphi(v-1) \qquad \exists v \leq 0.\varphi(v) \vdash \phi}{\Gamma \vdash \langle \alpha^* \rangle \phi, \Delta}$$

If you were to do the proof of ψ,, it would start by applying the convergence rule. We won't make you do the whole proof, though. Instead, state a *convergence property* $\varphi(v)$ which Angel could use to prove ψ. Briefly explain why the $(\exists v < 0.\varphi(v)) \rightarrow x \leq 0 \vee y \leq 0$ branch of the convergence proof will be valid. Note that convergence properties have not been covered in any real detail in lecture, only in recitation, so please refer to the relevant recitation notes: `http://symbolaris.com/course/fcps17/recitation09.pdf`. Since you have less exposure to this material, it may be best to save this question for last if you get stuck.

4. **Taylorism.** When we can't solve an ODE exactly, a useful technique is to use a *taylor series approximation* to get an upper or lower bound on the value of function. For a tutorial on taylor bound proofs in KeYmaera X, see `https://github.com/LS-Lab/KeYmaeraX-release/wiki/Taylor-Series-Approximations`. For this problem you're going to get some practice by proving a specific Taylor bound.

   Prove (using the axioms and proof rules of $\mathsf{d}\mathcal{L}$) that

   $$x = 1 \wedge t = 0 \rightarrow [\{x' = x, t' = 1 \& x \geq 1\}] x \geq 1 + t + \frac{t^2}{2} + \frac{t^3}{6} + \frac{t^4}{24}$$

   Submit *either* a hand-written proof or a KeYmaera X tactic that proves this.

5. **Chord length vs. arc length.** Because you've already done Lab 3, we know you know how fun circular dynamics are! So in this exercise and the following, we are going to prove yet *another* interesting property of circular dynamics! Let's dive right in!

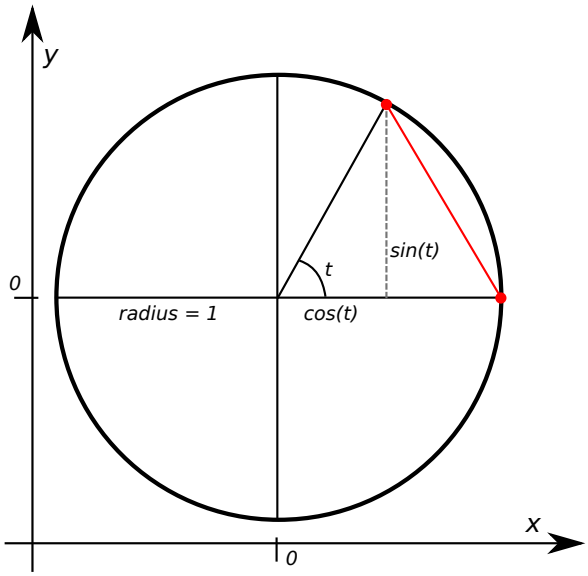

Figure 1: A beautiful picture, meticulously & lovingly hand-crafted by the Spring 2016 TA's

The following formula states that chord length (in red) is always smaller than arc length in a circle of radius 1.

$$x = 1 \land y = 0 \land t = 0 \rightarrow [x' = -y, y' = x, t' = 1]\ 2(1 - x) \leq t^2$$

It will be your job to figure out why that's the case! Fortunately, Figure 1 can help you figure out why the heck $2(1 - x) \leq t^2$ means "the chord length is less than the arc length".

Despite its misleading name, t is not time (sneaky, sneaky t!). As you can see above, it's the angle. Moreover, we know that $t = \frac{\text{arc length}}{r}$, i.e. arc length $= tr$. One famous version of this formula is the arc of 360° degrees, i.e. $c = 2\pi r$. Because we are assuming the unit radius $r = 1$, then the arc is simply t!

Using the quantities in the figure and the initial values of $x = 1, y = 0$, explain how $2(1 - x) \leq t^2$ means that the chord length is smaller than the arc length.

6. **Chord length vs. arc length (proof edition)!** We know you like circular motion. But we're on to your dark secret! More than circular motion, we know you love *proving things*! What can we do but oblige?

   Please prove the above formula in $\mathsf{d}\mathcal{L}$.

   Hint: use DC and DI, a dash of DW, and a sprinkle of circular motion properties. One very useful insight is that applying DI will generally yield formulas that you need in

order to prove the original property. So try to find a way to include those formulas in the proof!