**Recitation 9: Hybrid Games**
**15-424/15-624/15-824 Logical Foundations of Cyber-Physical Systems**

**Notes by: Brandon Bohrer**
**Edits by: Yong Kiam Tan (yongkiat@cs.cmu.edu)**

# 1 Announcements

- Theory 5 available soon.
- Lab 3 Veribot graded. Please let us know if you find bugs on the assignment handouts!

# 2 Lab 3 Veribot

In recitation we discussed common mistakes on the assignments, but we will not give out solutions in the recitation notes. If you have questions, come talk to us.

# 3 Motivation and Learning Objectives

This recitation focuses on the semantics and axiomatics of hybrid games. We will first recap the semantics by looking at the definitions of winning regions for Angel and Demon. Then, we will move on to look at hybrid game models and proofs.

# 4 Hybrid Game Semantics

The semantics of a formula $[\![P]\!]$ is (as usual) the set of states in which that formula is true. The key difference when working with hybrid games is in the semantics of the modal connectives. They now make use of the winning regions $\varsigma_\alpha, \delta_\alpha$:

$$[\![\langle\alpha\rangle P]\!] = \varsigma_\alpha([\![P]\!])$$
$$[\![[\alpha]P]\!] = \delta_\alpha([\![P]\!])$$

**Exercise 1:**
For revision purposes, it could help to fill in the following table which compares the transition semantics $[\![\alpha]\!]$ against the winning region semantics. Since there are many entries to fill, informal definitions will suffice, but make sure you know how to formally write down each of the definitions.

| $\alpha$ | $\llbracket\alpha\rrbracket$ | $\varsigma_\alpha(X)$ | $\delta_\alpha(X)$ |
|---|---|---|---|
| $x := e$ | | | |
| $?Q$ | | | |
| $\{x' = f(x) \,\&\, Q\}$ | | | |
| $\alpha \cup \beta$ | | | |
| $\alpha; \beta$ | | | |
| $\alpha^*$ | | | |
| $\alpha^d$ | | | |

Answer: The transition semantics should be clear by now, so we will focus on the winning regions, and especially the winning regions for Demon. The main intuition to keep in mind that these winning regions are defined from the point of view of Angel playing the game.

Recall that $\varsigma_\alpha(X), \delta_\alpha(X)$ are the sets of states for which Angel and Demon can win into $X$ by playing game $\alpha$ respectively. The target region is the set $X$ in all of the following answers.

- ($x := e$) Angel wins if from initial state $\omega$ the assignment leads to a winning state, i.e., $\omega_x^{\omega\llbracket e\rrbracket} \in X$. Conversely, Angel loses, and thus Demon wins if $\omega_x^{\omega\llbracket e\rrbracket} \notin X$.

  **That is incorrect!** Remember that both Angel and Demon are trying to win into $X$, and the assignment game has no choices for either of them to make. Thus, Demon actually wins into $X$ when $\omega_x^{\omega\llbracket e\rrbracket} \in X$ as well. Formally:

  $$\varsigma_{x:=e}(X) = \delta_{x:=e}(X) = \{\omega \mid \omega_x^{\omega\llbracket e\rrbracket} \in X\}$$

- ($?Q$) Angel wins when both $Q$ and $X$ are true in the initial state because Angel must pass the test. Conversely, Demon wins when either $Q$ is false, or $X$ is true in the initial state. Formally:

  $$\varsigma_{?Q}(X) = \llbracket Q\rrbracket \cap X$$
  $$\delta_{?Q}(X) = \llbracket Q\rrbracket^\complement \cup X$$

- ($\{x' = f(x) \,\&\, Q\ \}$) Angel wins if there is **some** solution to the ODE that stays in the domain constraint $Q$ for its entire duration, reaching the target region $X$ at its endpoint. Conversely, Demon wins if **all** such solutions satisfy $X$ at their endpoints. (Formal version omitted)

- ($\alpha \cup \beta$) Recall that Angel gets to make the choices, so Angel wins if she can win into $X$ by choosing either to play the $\alpha$ or $\beta$ game. Conversely, Demon needs to win into $X$ regardless of which game Angel chooses to play.

  $$\varsigma_{\alpha\cup\beta}(X) = \varsigma_\alpha(X) \cup \varsigma_\beta(X)$$
  $$\delta_{\alpha\cup\beta}(X) = \delta_\alpha(X) \cap \delta_\beta(X)$$

- $(\alpha;\beta)$ Like assignments, neither player has much choice in the sequential game. Thus, the definitions are straightforward compositions of winning regions.

  $$\varsigma_{\alpha;\beta}(X) = \varsigma_\alpha(\varsigma_\beta(X))$$
  $$\delta_{\alpha;\beta}(X) = \delta_\alpha(\delta_\beta(X))$$

- $(\alpha^*)$ Loops are easily the most complicated part of the semantics of hybrid games. If you have never seen least or greatest fixpoints before, it is perhaps easiest to remember them via their defining equations.

  For Angel, her winning region is characterized by the **least** set of states containing $X$ and closed under taking "one more iteration" of the loop.

  $$\varsigma_{\alpha^*}(X) = \bigcap_Z (X \cup \varsigma_\alpha(Z) \subseteq Z)$$

  Let us break down this definition:

  1. $X \subseteq Z$ requires the target region $X$ to be contained in $Z$, since Angel can always win from those states by running the loop 0 times.
  2. $\varsigma_\alpha(Z) \subseteq Z$ intuitively says $Z$ should also be closed under taking "one more iteration", because if a state in $\omega \in Z$ was a winning state, then Angel could have played one more loop iteration to get there.
  3. Finally, the $\bigcap_Z$ operator ensures that $\varsigma_{\alpha^*}(X)$ is the smallest set $Z$ satisfying the previous two properties.

  Conversely, Demon must be able to win regardless of how many times Angel chooses to run the loop. Thus, the winning region is characterized by a **greatest** set of states where Demon wins even if Angel decides to run the loop for "one more iteration".

  $$\delta_{\alpha^*}(X) = \bigcup_Z (Z \subseteq X \cap \delta_\alpha(Z))$$

  We can similarly break down this definition:

  1. $Z \subseteq X$ requires that $Z$ is in the target region $X$ already, because otherwise Angel can make Demon lose by running the loop 0 times.
  2. $Z \subseteq \delta_\alpha(Z)$ can be read as follows. Suppose Angel runs one more iteration of the loop from $Z$, then consider Demon's winning region $\delta_\alpha(Z)$. It must be the case that $Z$ is already contained in $\delta_\alpha(Z)$ as well, because Angel could otherwise make Demon lose with one more iteration.
  3. Finally, the $\bigcup_Z$ operator ensures that $\delta_{\alpha^*}(X)$ is the largest set $Z$ satisfying the previous two properties.

**Note: I got slightly confused with Point 2 for Demon at recitation. Reading the advanced material notes below and LFCPS Definition 15.5 might help.**

**Note: Advanced material not covered in recitation.** If you are wondering why for Angel we take the least fixpoint whereas for Demon we take the greatest, consider the following scenario for some intuition. Caveat: this is not a full proof.

Suppose that we had a state $\omega$ with the special property that playing the game $\alpha$ one more time always leads us back to $\omega$ (regardless of the moves either player makes).

For Angel, suppose that $\omega \notin X$, so clearly Angel cannot win into $X$ no matter how many iterations she wants to run the loop for. Now, consider a pre-fixpoint set of states $Z$ with $X \cup \varsigma_\alpha(Z) \subseteq Z$ and consider $Y = Z \cup \{\omega\}$, then $Y$ is also a pre-fixpoint but it is clearly not what the winning region for Angel should be because $\omega$ is included in $Y$. The $\bigcap$, or least fixpoint, operation ensures that none of these extra "junk" states are included.

For Demon, suppose that $\omega \in X$, so Demon wins into $X$ no matter how many iteration Angel runs the loop for. Now, consider a post-fixpoint set of states $Z$ with $X \cup \varsigma_\alpha(Z) \subseteq Z$ and consider $Y = Z \setminus \{\omega\}$, then $Y$ is also a post-fixpoint, but it is now missing the state $\omega$ from which Demon certainly wins from. The $\bigcup$, or greatest fixpoint, operation ensures that all of these "consistent" states are included.

- ($\alpha^d$) The crucial ingredient that makes hybrid games work so elegantly is the dual operator. This operator has no hybrid program counterpart so its corresponding transition semantics in the table you filled in above should be empty.

  The idea behind its semantics is illustrated in Geri's Game which we watched in the last recitation. For the dual game $\alpha^d$, Angel flips the board around (taking on the role of Demon) and tries to win the game $\alpha$ into $X^\complement$ instead. If the demonic Angel wins game $\alpha$ into $X^\complement$, then the regular Angel loses that game. Conversely, if the demonic Angel has no way to win the game $\alpha$ into $X^\complement$, then regular Angel wins. Thus:

  $$\varsigma_{\alpha^d}(X) = (\varsigma_\alpha(X^\complement))^\complement$$

  Similarly for Demon (think through the intuition from Geri's Game yourselves!):

  $$\delta_{\alpha^d}(X) = (\delta_\alpha(X^\complement))^\complement$$

The very last case for $\alpha^d$ highlights an important property of the winning region semantics. The "demonic Angel" is really just Demon so we should just think of the Angel changing into the Demon directly.

Formally, we start by showing that hybrid games are consistent and determined:

$$(\varsigma_\alpha(X^\complement))^\complement = \delta_\alpha(X)$$

Intuitively, this says that the set of states where Angel does not have a strategy to win into the set $X^\complement$ by playing game $\alpha$ is exactly those where Demon has a strategy to win into $X$.

This leads us on to the axiomatics where this is rendered as the determinacy axiom of dGL:

$$([\cdot])\quad [\alpha]P \leftrightarrow \neg\langle\alpha\rangle\neg P$$

Taken together with the duality axiom:

$$(\langle^{d}\rangle)\quad \langle\alpha^{d}\rangle P \leftrightarrow \neg\langle\alpha\rangle\neg P$$

We obtain the following very useful axiom that allows us to switch from proving diamond properties to box properties (and vice-versa) when we encounter the dual operator:

$$\langle\alpha^{d}\rangle P \leftrightarrow [\alpha]P$$

# 5 Axiomatics and Proving Hybrid Games

Notice that the $[\cdot]$ determinacy axiom is actually true in dL as well, when $\alpha$ is a hybrid program. In fact, as we have already seen in class, many of the axioms and proof rules of dGL are identical to those of dL, just with a different underlying semantics. In the lectures next week, we will see axioms where this is **not** the case, i.e., there are axioms of dL that would be unsound for hybrid games. However, if the hybrid game $\alpha$ does not mention the duality operator then it is indeed the case that all of the axioms of dL apply.

For now though, let us work through some dGL proofs using the axioms that we are already familiar with. (We will secretly avoid unsound uses of axioms.)

## 5.1 Verified Filibustering

Our first example is a simple game:

$$x = 0 \rightarrow \langle\big((x := 1 \cup v := 1); \{x' = v\}\big)^{\times}\rangle x = 0$$

**Exercise 2:**
Is this formula valid? If so, what is Angel's winning strategy?
Answer: It is valid because Angel can always force the value of $x$ to stay at 0 as long as it starts at 0. In other words, Angel can filibuster Demon (who controls the loop). Since Demon must stop running the loop eventually, Demon loses the game.

Now, let us try to verify this formula using the axioms that we already know.

$$x = 0 \vdash \langle\big((x := 1 \cup v := 1); \{x' = v\}\big)^{\times}\rangle x = 0$$

**Exercise 3:**
What is the first step?

Answer: Remember that the demonic loop operator gives Demon control over the loop iterations. Thus, the first step we need to use the axioms $[\cdot]$,$\langle^d\rangle$ to remove the outermost duality operator.

$$\scriptstyle [\cdot],\langle^d\rangle\ \displaystyle\frac{x=0 \vdash [\big((x:=1 \cup v:=1);\{x'=v\}\big)^*]x=0}{x=0 \vdash \langle\big((x:=1 \cup v:=1);\{x'=v\}\big)^\times\rangle x=0}$$

**Note: Hopefully you should have noticed that I have deliberately made a mistake in the proof above by unfolding the demonic loop incorrectly. However, let us see where the proof takes us.**

Now that we are left with a loop, all we need to do is to apply loop induction rule, or more formally the ind rule for hybrid games:

$$(\text{ind})\quad \frac{P \to [\alpha]P}{P \to [\alpha^*]P}$$

**Exercise 4:**

What loop invariant should we use?

Answer: Let us perhaps try the invariant $x=0$. After all, we do not know much more than that in the beginning. Continuing the proof as we are used to from dL, we can now unfold the game operators:

$$\begin{array}{r} \scriptstyle [;],[\cup],[:=],\wedge R \\ \scriptstyle \text{ind} \end{array}\ \cfrac{\cfrac{x=1 \vdash [\{x'=v\}]x=0 \qquad x=0 \vdash [\{x'=1\}]x=0}{x=0 \vdash [(x:=1 \cup v:=1);\{x'=v\}]x=0}}{x=0 \vdash [\big((x:=1 \cup v:=1);\{x'=v\}\big)^*]x=0}$$

**Exercise 5:**

Those premises do not look provable (or even true at all). What went wrong?

Answer: The problem lies with how we unfolded the demonic loop operator. Recall that:

$$\alpha^\times \overset{\text{def}}{\equiv} ((\alpha^d)^*)^d$$

We forgot to include the duality operator around $\alpha$ when unfolding the demonic loop! Always remember to unfold the demonic operators correctly. When in doubt, just remember that the demonic operators are syntactic abbreviations so you could also simply remove all of them before you start your proof.

Here is the corrected unfolding:

$$\scriptstyle [\cdot],\langle^d\rangle\ \displaystyle\frac{x=0 \vdash [\Big(\big((x:=1 \cup v:=1);\{x'=v\}\big)^d\Big)^*]x=0}{x=0 \vdash \langle\big((x:=1 \cup v:=1);\{x'=v\}\big)^\times\rangle x=0}$$

**Exercise 6:**

What is the loop invariant to use?

Answer: As before, $x=0$ looks like a plausible option. After applying ind we now flip back into a diamond question because of the nested duality operator.

$$\text{ind}\;\dfrac{[\cdot],\langle^d\rangle\;\dfrac{x = 0 \vdash \langle (x := 1 \cup v := 1); \{x' = v\}\rangle x = 0}{x = 0 \vdash [\big((x := 1 \cup v := 1); \{x' = v\}\big)^d] x = 0}}{x = 0 \vdash [\Big(\big((x := 1 \cup v := 1); \{x' = v\}\big)^d\Big)^*] x = 0}$$

Now, we can apply the usual axioms you know from dL in diamond form. Since we have not had much experience with the diamond version of these rules, let us do the proof a little slower:[1]

$$\langle ; \rangle\;\dfrac{\langle \cup \rangle, \vee\text{R}\;\dfrac{x = 0 \vdash \langle x := 1\rangle\langle \{x' = v\}\rangle x = 0, \langle v := 1\rangle\langle\{x' = v\}\rangle x = 0}{x = 0 \vdash \langle (x := 1 \cup v := 1)\rangle\langle\{x' = v\}\rangle x = 0}}{x = 0 \vdash \langle (x := 1 \cup v := 1); \{x' = v\}\rangle x = 0}$$

**Exercise 7:**
What do we do next?
Answer: The key here is to look back at Angel's strategy. If she chooses the left choice, there is not much hope of guaranteeing that $x = 0$ at the end of her run of the ODE unless $v$ is negative (but we do not know that). However, if she chooses the right branch, then since $x = 0$ initially, she can simply evolve the ODE for no time. Thus, we can safely drop the first succedent on the right and complete the proof from the right disjunct using the ODE solution axiom:

$$\langle := \rangle\;\dfrac{\langle ' \rangle\;\dfrac{\mathbb{R}\;\dfrac{*}{x = 0 \vdash \exists t \geq 0\, x + t = 0}}{x = 0 \vdash \langle \{x' = 1\}\rangle x = 0}}{x = 0 \vdash \langle v := 1\rangle\langle\{x' = v\}\rangle x = 0}$$

We used two insights in this proof. First, the duality operators allowed us to flip back and forth between the box and diamond modalities. Second, the proof actually follows Angel's strategy quite closely. Thus, one very good way of figuring out a games proof is to first figure out the Angel (or Demon's) winning strategy.

## 5.2 Verified Planar Avoidance

Finally, let us turn to modeling situation using hybrid games. The scenario we will be considering is as follows:

The Demon is a mosquito flying around in straight lines and you the human (a.k.a., the Angel) are trying to avoid getting bitten. We want the system to be interactive, so the mosquito could choose to change directions whenever it likes, but whenever it does so, you can also react by changing your direction.
**Note: For now, we will skip any bounds on the velocities and position, etc., but you should feel free to extend this model.**

**Exercise 8:**
How would we go about modeling this scenario?

[1] Have you seen $\langle ; \rangle$ somewhere before?

Answer: We could start by deciding on the coordinate system. Let us suppose that the coordinates of the mosquito are $(x, y)$ while your coordinates are $(a, b)$, both in the Euclidean plane.

Let us further suppose that both players can instantaneously change their heading direction and velocities, which we will prescribe using $v_x, v_y$ and $v_a, v_b$ respectively.

**Exercise 9:**
How would we describe the game?
Answer: First, we need to write down controllers for each player. This is relatively simple, since both players simply make a choice of heading.

$$\alpha_m \equiv v_x := *; v_y := *$$

$$\alpha_h \equiv v_a := *; v_b := *$$

Next, the ODEs describing the motion of the mosquito and the human:

$$\beta \equiv \{x' = v_x, y' = v_y, a' = v_a, b' = v_b\}$$

**Exercise 10:**
How should we put these three parts of the program together?
Answer: We need to be careful to put the things we want under appropriate player controls. As we said earlier, this mosquito can change its heading anytime it likes, so perhaps $\alpha_m, \beta$ should both be under its control.

However, we can really only react to the mosquito if we have access to where it is currently heading. So we certainly want $\alpha_h$ to come after $\alpha_m$.

Finally, we want to avoid getting stung no matter how many times the mosquito changes its heading, so the loop should also be under Demonic control. Thus, our overall program is:

$$\gamma \equiv (\alpha_m^d; \alpha_h; \beta)^\times$$

**Exercise 11:**
Finally, we are ready to write down (and prove) a formula that means we never get bitten. What should it be?
Answer: There are many possible ways of writing this down. For example, let us say that the human and mosquito have to always be separated by some distance $d$. Then the dGL formula modeling our scenario could be:

$$d > 0 \land (x - a)^2 + (y - b)^2 > d \to \langle\gamma\rangle(x - a)^2 + (y - b)^2 > d$$

**Exercise 12:**
Would this formula be valid? If so, what is Angel's strategy?

Answer: There are multiple possibilities for Angel since she has full access over the mosquito's movements. For example, she can simply mirror what the mosquito is doing. In 2-dimensions, she can even do more interesting maneuvers, such as moving perpendicularly away from the mosquito.

**Exercise 13:**
Add more restrictions to Angel, e.g., bounding her velocity so that simply mirroring the mosquito would not be a viable strategy. Next, prove your resulting model (possibly in KeYmaera X).
**Note: The accompanying archive has the filibuster and planar game models as rec9fili and rec9planar respectively.**