15-424: Foundations of Cyber-Physical Systems

Lecture Notes on Game Proofs & Separations

André Platzer

Carnegie Mellon University

Lecture 23

1 Introduction

This lecture continues the study of hybrid games and their logic, differential game logic [Pla13]. Lecture 20 on Hybrid Systems & Games introduced hybrid games, Lecture 21 on Winning Strategies & Regions studied the winning region semantics, and Lecture 22 on Winning & Proving Hybrid Games identified the winning region semantics for loops in hybrid games as well as a study of the axioms of hybrid games.

These lecture notes are based on [Pla13], where more information can be found on logic and hybrid games.

2 Recall: Semantics of Hybrid Games

Recall the semantics of hybrid games and two results from Lecture 22 on Winning & Proving Hybrid Games.

Definition 1 (Semantics of hybrid games). The *semantics of a hybrid game* α is a function $\varsigma_\alpha(\cdot)$ that, for each interpretation I and each set of Angel's winning states $X \subseteq \mathcal{S}$, gives the *winning region*, i.e. the set of states $\varsigma_\alpha(X)$ from which Angel has a winning strategy to achieve X (whatever strategy Demon chooses). It is defined inductively as follows[a]

1. $\varsigma_{x:=\theta}(X) = \{\nu \in \mathcal{S} : \nu_x^{[\![\theta]\!]_\nu} \in X\}$
2. $\varsigma_{x'=\theta\,\&\,H}(X) = \{\varphi(0) \in \mathcal{S} : \varphi(r) \in X$ for some $r \in \mathbb{R}_{\geq 0}$ and (differentiable) $\varphi : [0,r] \to \mathcal{S}$ such that $\varphi(\zeta) \in [\![H]\!]^I$ and $\frac{\mathrm{d}\,\varphi(t)(x)}{\mathrm{d}t}(\zeta) = [\![\theta]\!]_{\varphi(\zeta)}$ for all $0 \leq \zeta \leq r\}$
3. $\varsigma_{?H}(X) = [\![H]\!]^I \cap X$
4. $\varsigma_{\alpha\cup\beta}(X) = \varsigma_\alpha(X) \cup \varsigma_\beta(X)$
5. $\varsigma_{\alpha;\beta}(X) = \varsigma_\alpha(\varsigma_\beta(X))$
6. $\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathcal{S} : X \cup \varsigma_\alpha(Z) \subseteq Z\}$
7. $\varsigma_{\alpha^d}(X) = (\varsigma_\alpha(X^\complement))^\complement$

The *winning region* of Demon, i.e. the set of states $\delta_\alpha(X)$ from which Demon has a winning strategy to achieve X (whatever strategy Angel chooses) is defined inductively as follows

1. $\delta_{x:=\theta}(X) = \{\nu \in \mathcal{S} : \nu_x^{[\![\theta]\!]_\nu} \in X\}$
2. $\delta_{x'=\theta\,\&\,H}(X) = \{\varphi(0) \in \mathcal{S} : \varphi(r) \in X$ for all $r \in \mathbb{R}_{\geq 0}$ and (differentiable) $\varphi : [0,r] \to \mathcal{S}$ such that $\varphi(\zeta) \in [\![H]\!]^I$ and $\frac{\mathrm{d}\,\varphi(t)(x)}{\mathrm{d}t}(\zeta) = [\![\theta]\!]_{\varphi(\zeta)}$ for all $0 \leq \zeta \leq r\}$
3. $\delta_{?H}(X) = ([\![H]\!]^I)^\complement \cup X$
4. $\delta_{\alpha\cup\beta}(X) = \delta_\alpha(X) \cap \delta_\beta(X)$
5. $\delta_{\alpha;\beta}(X) = \delta_\alpha(\delta_\beta(X))$
6. $\delta_{\alpha^*}(X) = \bigcup\{Z \subseteq \mathcal{S} : Z \subseteq X \cap \delta_\alpha(Z)\}$
7. $\delta_{\alpha^d}(X) = (\delta_\alpha(X^\complement))^\complement$

[a] The semantics of a hybrid game is not merely a reachability relation between states as for hybrid systems [Pla12], because the adversarial dynamic interactions and nested choices of the players have to be taken into account.

Lemma 2 (Monotonicity [Pla13]). *The semantics is* monotone, *i.e.* $\varsigma_\alpha(X) \subseteq \varsigma_\alpha(Y)$ *and* $\delta_\alpha(X) \subseteq \delta_\alpha(Y)$ *for all* $X \subseteq Y$.

Theorem 3 (Consistency & determinacy [Pla13]). *Hybrid games are consistent and determined, i.e.* $\vDash \neg\langle\alpha\rangle\neg\phi \leftrightarrow [\alpha]\phi$.

3 Hybrid Game Proofs

An axiomatization for differential game logic has been found in previous work [Pla13], where we refer to for more details.

Note 4 (Differential game logic axiomatization [Pla13]).

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

$$(\langle{:=}\rangle)\ \langle x := \theta\rangle\phi(x) \leftrightarrow \phi(\theta)$$

$$(\langle{}'\rangle)\ \langle x' = \theta\rangle\phi \leftrightarrow \exists t{\geq}0\, \langle x := y(t)\rangle\phi \qquad (y'(t) = \theta)$$

$$(\langle?\rangle)\ \langle ?H\rangle\phi \leftrightarrow (H \land \phi)$$

$$(\langle\cup\rangle)\ \langle\alpha \cup \beta\rangle\phi \leftrightarrow \langle\alpha\rangle\phi \lor \langle\beta\rangle\phi$$

$$(\langle;\rangle)\ \langle\alpha;\beta\rangle\phi \leftrightarrow \langle\alpha\rangle\langle\beta\rangle\phi$$

$$(\langle{}^*\rangle)\ \phi \lor \langle\alpha\rangle\langle\alpha^*\rangle\phi \rightarrow \langle\alpha^*\rangle\phi$$

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

$$(\text{M})\ \frac{\phi \rightarrow \psi}{\langle\alpha\rangle\phi \rightarrow \langle\alpha\rangle\psi}$$

$$(\text{FP})\ \frac{\phi \lor \langle\alpha\rangle\psi \rightarrow \psi}{\langle\alpha^*\rangle\phi \rightarrow \psi}$$

$$(\text{ind})\ \frac{\phi \rightarrow [\alpha]\phi}{\phi \rightarrow [\alpha^*]\phi}$$

The proof rules FP and ind are equivalent in the sense that one can be derived from the other in the dGL calculus [Pla13].

Example 4. The dual filibuster game formula from Lecture 20 proves easily in the dGL calculus by going back and forth between players [Pla13]:

$$
\begin{array}{rl}
 & * \\ \hline
\mathbb{R} & x=0 \rightarrow 0=0 \lor 1=0 \\ \hline
\langle:=\rangle & x=0 \rightarrow \langle x:=0\rangle x=0 \lor \langle x:=1\rangle x=0 \\ \hline
\langle\cup\rangle & x=0 \rightarrow \langle x:=0 \cup x:=1\rangle x=0 \\ \hline
\langle^{d}\rangle & x=0 \rightarrow \neg\langle x:=0 \cap x:=1\rangle \neg x=0 \\ \hline
[\cdot] & x=0 \rightarrow [x:=0 \cap x:=1]x=0 \\ \hline
\text{ind} & x=0 \rightarrow [(x:=0 \cap x:=1)^{*}]x=0 \\ \hline
\langle^{d}\rangle & x=0 \rightarrow \langle (x:=0 \cup x:=1)^{\times}\rangle x=0
\end{array}
$$

4 Soundness

Theorem 5 (Soundness [Pla13])**.** *The* dGL *proof calculus in Fig. 4 is sound, i.e. all provable formulas are valid.*

Proof. The full proof can be found in [Pla13]. We just consider a few cases to exemplify the fundamentally more general semantics of hybrid games arguments compared to hybrid systems arguments. To prove soundness of an equivalence axiom $\phi \leftrightarrow \psi$, show $[\![\phi]\!]^I = [\![\psi]\!]^I$ for all interpretations I with any set of states $\mathcal{S}$.

$\langle\cup\rangle$ $[\![\langle\alpha\cup\beta\rangle\phi]\!]^I = \varsigma_{\alpha\cup\beta}([\![\phi]\!]^I) = \varsigma_\alpha([\![\phi]\!]^I) \cup \varsigma_\beta([\![\phi]\!]^I) = [\![\langle\alpha\rangle\phi]\!]^I \cup [\![\langle\beta\rangle\phi]\!]^I = [\![\langle\alpha\rangle\phi \lor \langle\beta\rangle\phi]\!]^I$

$\langle;\rangle$ $[\![\langle\alpha;\beta\rangle\phi]\!]^I = \varsigma_{\alpha;\beta}([\![\phi]\!]^I) = \varsigma_\alpha(\varsigma_\beta([\![\phi]\!]^I)) = \varsigma_\alpha([\![\langle\beta\rangle\phi]\!]^I) = [\![\langle\alpha\rangle\langle\beta\rangle\phi]\!]^I$.

$\langle?\rangle$ $[\![\langle ?H\rangle\phi]\!]^I = \varsigma_{?H}([\![\phi]\!]^I) = [\![H]\!]^I \cap [\![\phi]\!]^I = [\![H \land \phi]\!]^I$

$[\cdot]$ is sound by Theorem 3.

M Assume the premise $\phi \rightarrow \psi$ is valid in interpretation I, i.e. $[\![\phi]\!]^I \subseteq [\![\psi]\!]^I$. Then the conclusion $\langle\alpha\rangle\phi \rightarrow \langle\alpha\rangle\psi$ is valid in I, i.e. $[\![\langle\alpha\rangle\phi]\!]^I = \varsigma_\alpha([\![\phi]\!]^I) \subseteq \varsigma_\alpha([\![\psi]\!]^I) = [\![\langle\alpha\rangle\psi]\!]^I$ by monotonicity (Lemma 2). □

5 Separating Axioms

The axioms of differential game logic in Fig. 4 are sound for hybrid systems as well, because every hybrid system is a (single player) hybrid game. With a few exceptions, they look surprisingly close to the axioms for hybrid systems from Lecture 5. In order to understand the fundamental difference between hybrid systems and hybrid games, it is instructive to also investigate separating axioms, i.e. axioms of hybrid systems that are not sound for hybrid games. Some of these are summarized in Fig. 1, referring to [Pla13] for details.

$$\cancel{\mathrm{K}}\quad [\alpha](\phi \to \psi) \to ([\alpha]\phi \to [\alpha]\psi) \qquad\qquad \mathrm{M}\quad \langle\alpha\rangle\phi \lor \langle\alpha\rangle\psi \to \langle\alpha\rangle(\phi \lor \psi)$$

$$\cancel{\mathrm{G}}\quad \frac{\phi}{[\alpha]\phi} \qquad\qquad \mathrm{M}_{[\cdot]}\ \frac{\phi \to \psi}{[\beta]\phi \to [\beta]\psi}$$

$$\cancel{\mathrm{R}}\quad \frac{\phi_1 \land \phi_2 \to \psi}{[\alpha]\phi_1 \land [\alpha]\phi_2 \to [\alpha]\psi}$$

$$\cancel{\mathrm{B}}\quad \langle\alpha\rangle\exists x\, \phi \to \exists x\, \langle\alpha\rangle\phi \qquad (x \notin \alpha) \qquad\qquad \overleftarrow{\mathrm{B}}\quad \exists x\, \langle\alpha\rangle\phi \to \langle\alpha\rangle\exists x\, \phi \qquad (x \notin \alpha)$$

$$\cancel{\mathrm{I}}\quad [\alpha^*](\phi \to [\alpha]\phi) \to (\phi \to [\alpha^*]\phi)$$

$$\cancel{\mathrm{FA}}\ \langle\alpha^*\rangle\phi \to \phi \lor \langle\alpha^*\rangle(\neg\phi \land \langle\alpha\rangle\phi)$$

Figure 1: Separating axioms: The axioms and rules on the left are sound for hybrid systems but not for hybrid games. The related axioms on the right are sound for hybrid games.

6 Repetitive Diamonds – Convergence vs. Iteration

More fundamental differences between hybrid systems and hybrid games also exist in terms of convergence rules, even if these have played a less prominent role in this course so far. These differences are discussed in detail elsewhere [Pla13]. In a nutshell, Harel's convergence rule [HMP77] is not a separating axiom, because it is sound for dG$\mathcal{L}$, just unnecessary, and, furthermore, not even particularly useful for hybrid games [Pla13]. The hybrid version of Harel's convergence rule [Pla08] for d$\mathcal{L}$ reads as follows (it assumes that v does not occur in α):

$$(\text{con})\ \frac{\varphi(v+1) \land v+1>0 \vdash \langle\alpha\rangle\varphi(v)}{\Gamma, \exists v\, \varphi(v) \vdash \langle\alpha^*\rangle\exists v{\leq}0\, \varphi(v), \Delta}$$

The d$\mathcal{L}$ proof rule con expresses that the variant $\varphi(v)$ holds for some real number $v \leq 0$ after repeating α sufficiently often if $\varphi(v)$ holds for some real number at all in the beginning (antecedent) and, by premise, $\varphi(v)$ can decrease after some execution of α by 1 (or another positive real constant) if $v > 0$. This rule can be used to show positive progress (by 1) with respect to $\varphi(v)$ by executing α. Just like the induction rule ind is often used with a separate premiss for the initial and postcondition check (*ind′* from Lecture 7 on Loops & Invariants), rule con is often used in the following derived form:

$$(con')\ \frac{\Gamma \vdash \exists v\, \varphi(v), \Delta \quad \forall v{>}0\, (\varphi(v) \to \langle\alpha\rangle\varphi(v-1)) \quad \exists v{\leq}0\, \varphi(v) \vdash \psi}{\Gamma \vdash \langle\alpha^*\rangle\psi, \Delta}$$

The following sequent proof shows how convergence rule *con′* can be used to prove a simple dℒ liveness property of a hybrid program:

$$\text{→r}\,\dfrac{\text{con}'\,\dfrac{\mathbb{R}\,\dfrac{*}{x \geq 0 \vdash \exists n\, x < n+1} \qquad \langle{:=}\rangle\,\dfrac{\mathbb{R}\,\dfrac{*}{x < n+2 \land n+1 > 0 \vdash x-1 < n+1}}{x < n+2 \land n+1 > 0 \vdash \langle x := x-1\rangle x < n+1} \qquad \mathbb{R}\,\dfrac{*}{\exists n{\leq}0\, x < n+1 \vdash x < 1}}{x \geq 0 \vdash \langle (x := x-1)^*\rangle 0 \leq x < 1}}{x \geq 0 \rightarrow \langle (x := x-1)^*\rangle x < 1}$$

Let's compare how dGℒ proves diamond properties of repetitions based on the iteration axiom ⟨*⟩.

Example 6 (Non-game system). The simple non-game dGℒ formula

$$x \geq 0 \rightarrow \langle (x := x-1)^*\rangle 0 \leq x < 1$$

is provable, shown in Fig. 2, where $\langle \alpha^*\rangle 0 \leq x < 1$ is short for $\langle (x := x-1)^*\rangle (0 \leq x < 1)$.

$$\text{MP}\,\dfrac{\langle *\rangle,\forall\,\dfrac{\text{US}\,\dfrac{\langle{:=}\rangle\,\dfrac{\mathbb{R}\,\dfrac{*}{\forall x\,(0 \leq x < 1 \lor p(x-1) \rightarrow p(x)) \rightarrow (x \geq 0 \rightarrow p(x))}}{\forall x\,(0 \leq x < 1 \lor \langle x := x-1\rangle p(x) \rightarrow p(x)) \rightarrow (x \geq 0 \rightarrow p(x))}}{\forall x\,(0 \leq x < 1 \lor \langle x := x-1\rangle\langle \alpha^*\rangle 0 \leq x < 1 \rightarrow \langle \alpha^*\rangle 0 \leq x < 1) \rightarrow (x \geq 0 \rightarrow \langle \alpha^*\rangle 0 \leq x < 1)}}{\forall x\,(0 \leq x < 1 \lor \langle x := x-1\rangle\langle \alpha^*\rangle 0 \leq x < 1 \rightarrow \langle \alpha^*\rangle 0 \leq x < 1)}}{x \geq 0 \rightarrow \langle \alpha^*\rangle 0 \leq x < 1}$$

Figure 2: dGℒ Angel proof for non-game system Example 6
$x \geq 0 \rightarrow \langle (x := x-1)^*\rangle 0 \leq x < 1$

Example 7 (Choice game). The dGℒ formula

$$x = 1 \land a = 1 \rightarrow \langle (x := a; a := 0 \cap x := 0)^*\rangle x \neq 1$$

is provable as shown in Fig. 3, where $\beta \cap \gamma$ is short for $x := a; a := 0 \cap x := 0$ and $\langle (\beta \cap \gamma)^*\rangle x \neq 1$ short for $\langle (x := a; a := 0 \cap x := 0)^*\rangle x \neq 1$:

Example 8 (2-Nim-type game). The dGℒ formula

$$x \geq 0 \rightarrow \langle (x := x-1 \cap x := x-2)^*\rangle 0 \leq x < 2$$

is provable as shown in Fig. 3, where $\beta \cap \gamma$ is short for $x := x-1 \cap x := x-2$ and $\langle (\beta \cap \gamma)^*\rangle 0{\leq}x{<}2$ short for $\langle (x := x-1 \cap x := x-2)^*\rangle 0 \leq x < 2$:

Example 9 (Hybrid game). The dGℒ formula

$$\langle (x := 1; x' = 1^d \cup x := x-1)^*\rangle 0 \leq x < 1$$

is provable as shown in Fig. 5, where the notation $\langle (\beta \cup \gamma)^*\rangle 0 \leq x < 1$ is short for $\langle (x := 1; x' = 1^d \cup x := x-1)^*\rangle (0 \leq x < 1)$: The proof steps for β use in ⟨′⟩ that $t \mapsto x+t$ is the solution of the differential equation, so the subsequent use of ⟨:=⟩ substitutes 1 in for x to obtain $t \mapsto 1+t$. Recall from Lecture 22 that the winning regions for this formula need $>\omega$ iterations to converge. It is still provable easily.

$$\begin{array}{lr}
 & * \\ \hline
\mathbb{R} & \forall x\,(x \neq 1 \lor p(a,0) \land p(0,a) \to p(x,a)) \to (\mathit{true} \to p(x,a)) \\ \hline
\langle ;\rangle,\langle :=\rangle & \forall x\,(x \neq 1 \lor \langle\beta\rangle p(x,a) \land \langle\gamma\rangle p(x,a) \to p(x,a)) \to (\mathit{true} \to p(x,a)) \\ \hline
\langle\cup\rangle,\langle^d\rangle & \forall x\,(x \neq 1 \lor \langle\beta\cap\gamma\rangle p(x,a) \to p(x,a)) \to (\mathit{true} \to p(x,a)) \\ \hline
\mathrm{US} & \forall x\,(x \neq 1 \lor \langle\beta\cap\gamma\rangle\langle(\beta\cap\gamma)^*\rangle x \neq 1 \to \langle(\beta\cap\gamma)^*\rangle x \neq 1) \to (\mathit{true} \to \langle(\beta\cap\gamma)^*\rangle x \neq 1) \\ \hline
\langle^*\rangle,\forall,\mathrm{MP} & \mathit{true} \to \langle(\beta\cap\gamma)^*\rangle x \neq 1 \\ \hline
\mathbb{R} & x = 1 \land a = 1 \to \langle(\beta\cap\gamma)^*\rangle x \neq 1
\end{array}$$

Figure 3: dGL Angel proof for choice game Example 7 $x = 1 \land a = 1 \to \langle(x := a; a := 0 \cap x := 0)^*\rangle x \neq 1$

$$\begin{array}{lr}
 & * \\ \hline
\mathbb{R} & \forall x\,(0{\le}x{<}2 \lor p(x-1) \land p(x-2) \to p(x)) \to (\mathit{true} \to p(x)) \\ \hline
\langle :=\rangle & \forall x\,(0{\le}x{<}2 \lor \langle\beta\rangle p(x) \land \langle\gamma\rangle p(x) \to p(x)) \to (\mathit{true} \to p(x)) \\ \hline
\langle\cup\rangle,\langle^d\rangle & \forall x\,(0{\le}x{<}2 \lor \langle\beta\cap\gamma\rangle p(x) \to p(x)) \to (\mathit{true} \to p(x)) \\ \hline
\mathrm{US} & \forall x\,(0{\le}x{<}2 \lor \langle\beta\cap\gamma\rangle\langle(\beta\cap\gamma)^*\rangle 0{\le}x{<}2 \to \langle(\beta\cap\gamma)^*\rangle 0{\le}x{<}2) \to (\mathit{true} \to \langle(\beta\cap\gamma)^*\rangle 0{\le}x{<}2) \\ \hline
\langle^*\rangle,\forall,\mathrm{MP} & \mathit{true} \to \langle(\beta\cap\gamma)^*\rangle 0{\le}x{<}2 \\ \hline
\mathbb{R} & x \ge 0 \to \langle(\beta\cap\gamma)^*\rangle 0{\le}x{<}2
\end{array}$$

Figure 4: dGL Angel proof for 2-Nim-type game Example 8 $x \ge 0 \to \langle(x := x-1 \cap x := x-2)^*\rangle 0 \le x < 2$

$$\begin{array}{lr}
 & * \\ \hline
\mathbb{R} & \forall x\,(0 \le x < 1 \lor \forall t{\ge}0\, p(1+t) \lor p(x-1) \to p(x)) \to (\mathit{true} \to p(x)) \\ \hline
\langle :=\rangle & \forall x\,(0 \le x < 1 \lor \langle x := 1\rangle\neg\exists t{\ge}0\, \langle x := x+t\rangle\neg p(x) \lor p(x-1) \to p(x)) \to (\mathit{true} \to p(x)) \\ \hline
\langle '\rangle & \forall x\,(0 \le x < 1 \lor \langle x := 1\rangle\neg\langle x' = 1\rangle\neg p(x) \lor p(x-1) \to p(x)) \to (\mathit{true} \to p(x)) \\ \hline
\langle ;\rangle,\langle^d\rangle & \forall x\,(0 \le x < 1 \lor \langle\beta\rangle p(x) \lor \langle\gamma\rangle p(x) \to p(x)) \to (\mathit{true} \to p(x)) \\ \hline
\langle\cup\rangle & \forall x\,(0 \le x < 1 \lor \langle\beta\cup\gamma\rangle p(x) \to p(x)) \to (\mathit{true} \to p(x)) \\ \hline
\mathrm{US} & \forall x\,(0{\le}x{<}1 \lor \langle\beta\cup\gamma\rangle\langle(\beta\cup\gamma)^*\rangle 0 \le x < 1 \to \langle(\beta\cup\gamma)^*\rangle 0 \le x < 1) \to (\mathit{true} \to \langle(\beta\cup\gamma)^*\rangle 0 \le x < 1) \\ \hline
\langle^*\rangle,\forall,\mathrm{MP} & \mathit{true} \to \langle(\beta\cup\gamma)^*\rangle 0 \le x < 1
\end{array}$$

Figure 5: dGL Angel proof for hybrid game Example 9 $\langle(x := 1; x' = 1^d \cup x := x-1)^*\rangle 0 \le x < 1$

7 There and Back Again Game

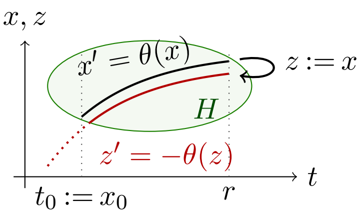
Quite unlike in hybrid systems and (poor test) differential dynamic logic [Pla08, Pla12], every hybrid game containing a differential equation $x' = \theta \,\&\, H$ with evolution domain constraints H can be replaced equivalently by a hybrid game without evolution domain constrains (even using poor tests, i.e. each test $?H$ uses only first-order formulas H). Evolution domains are definable in hybrid games and can, thus, be removed equivalently.

Lemma 10 (Domain reduction [Pla13, Pla12])**.** *Evolution domains of differential equations are definable as hybrid games: For every hybrid game there is an equivalent hybrid game that has no evolution domain constraints, i.e. all continuous evolutions are of the form $x' = \theta$.*

Proof. For notational convenience, assume the (vectorial) differential equation $x' = \theta(x)$ to contain a clock $x_0' = 1$ and that t_0 and z are fresh variables. Then $x' = \theta(x) \,\&\, H(x)$ is equivalent to the hybrid game:

$$t_0 := x_0; x' = \theta(x); (z := x; z' = -\theta(z))^d; ?(z_0 \geq t_0 \rightarrow H(z)) \tag{1}$$

See Fig. 6 for an illustration. Suppose the current player is Angel. The idea behind game equivalence (1) is that the fresh variable t_0 remembers the initial time x_0, and Angel then evolves forward along $x' = \theta(x)$ for any amount of time (Angel's choice). Afterwards, the opponent Demon copies the state x into a fresh variable (vector) z that he can evolve backwards along $(z' = -\theta(z))^d$ for any amount of time (Demon's choice). The original player Angel must then pass the challenge $?(z_0 \geq t_0 \rightarrow H(z))$, i.e. Angel loses immediately if Demon was able to evolve backwards and leave region $H(z)$ while satisfying $z_0 \geq t_0$, which checks that Demon did not evolve backward for longer than Angel evolved forward. Otherwise, when Angel passes the test, the extra variables t_0, z become irrelevant (they are fresh) and the game continues from the current state x that Angel chose in the first place (by selecting a duration for the evolution that Demon could not invalidate). □



Angel plays forward game, reverts flow and time x_0;
Demon checks H in backwards game until initial t_0

Figure 6: "There and back again game": Angel evolves x forwards in time along $x' = \theta(x)$, Demon checks evolution domain backwards in time along $z' = -\theta(z)$ on a copy z of the state vector x

Lemma 10 can eliminate all evolution domain constraints equivalently in hybrid games from now on. While evolution domain constraints are fundamental parts of standard hybrid systems [Hen96, HKPV95, ACHH92, Pla08], they turn out to be mere convenience notation for hybrid games. In that sense, hybrid games are more fundamental than hybrid systems, because they feature elementary operators.

Exercises

Exercise 1 (***). The following formula was proved using dG$\mathcal{L}$'s hybrid games type proof rules in Fig. 2

$$x \geq 0 \rightarrow \langle (x := x - 1)^* \rangle 0 \leq x < 1$$

Try to prove it using the convergence rule *con*′ instead.

References

[ACHH92] Rajeev Alur, Costas Courcoubetis, Thomas A. Henzinger, and Pei-Hsin Ho. Hybrid automata: An algorithmic approach to the specification and verification of hybrid systems. In Robert L. Grossman, Anil Nerode, Anders P. Ravn, and Hans Rischel, editors, *Hybrid Systems*, volume 736 of *LNCS*, pages 209–229. Springer, 1992.

[Hen96] Thomas A. Henzinger. The theory of hybrid automata. In *LICS*, pages 278–292, Los Alamitos, 1996. IEEE Computer Society. doi:10.1109/LICS.1996.561342.

[HKPV95] Thomas A. Henzinger, Peter W. Kopke, Anuj Puri, and Pravin Varaiya. What's decidable about hybrid automata? In Frank Thomson Leighton and Allan Borodin, editors, *STOC*, pages 373–382. ACM, 1995. doi:10.1145/225058.225162.

[HMP77] David Harel, Albert R. Meyer, and Vaughan R. Pratt. Computability and completeness in logics of programs (preliminary report). In *STOC*, pages 261–268. ACM, 1977.

[Pla08] André Platzer. Differential dynamic logic for hybrid systems. *J. Autom. Reas.*, 41(2):143–189, 2008. doi:10.1007/s10817-008-9103-8.

[Pla12] André Platzer. The complete proof theory of hybrid systems. In *LICS*, pages 541–550. IEEE, 2012. doi:10.1109/LICS.2012.64.

[Pla13] André Platzer. A complete axiomatization of differential game logic for hybrid games. Technical Report CMU-CS-13-100R, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, January, Revised and extended in July 2013.