André Platzer

Lecture Notes on Foundations of Cyber-Physical Systems

15-424/624/824 Foundations of Cyber-Physical Systems

Chapter 17
Game Proofs & Separations

17.1 Introduction

This chapter continues the study of hybrid games and their logic, differential game logic [3]. Chap. 14 introduced hybrid games, Chap. 15 studied the winning region semantics, and Chap. 16 identified the winning region semantics for loops in hybrid games as well as a study of the axioms of hybrid games.

This textbook are based on [3], where more information can be found on logic and hybrid games.

17.2 Recap: Semantics of Hybrid Games

Recall the semantics of hybrid games and two results from Chap. 16.

Definition 15.4 (Semantics of hybrid games). The *semantics of a hybrid game* α is a function $\varsigma_\alpha(\cdot)$ that, for each set of Angel's winning states $X \subseteq \mathscr{S}$, 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:

1. $\varsigma_{x:=e}(X) = \{\omega \in \mathscr{S} : \omega_x^{\omega[\![e]\!]} \in X\}$
   That is, an assignment $x:=e$ wins a game into X from any state whose modification $\omega_x^{\omega[\![e]\!]}$ that changes the value of x to that of $\omega[\![e]\!]$ is in X.
2. $\varsigma_{x'=f(x)\,\&\,Q}(X) = \{\varphi(0) \in \mathscr{S} : \varphi(r) \in X$ for some solution $\varphi : [0,r] \to \mathscr{S}$ of any duration $r \in \mathbb{R}$ satisfying $\varphi \models x' = f(x) \wedge Q\}$
   That is, Angel wins the differential equation $x' = f(x)\,\&\,Q$ into X from any state $\varphi(0)$ from which there is a solution φ of $x' = f(x)$ of any duration r that remains in Q all the time and leads to a final state $\varphi(r) \in X$.

3. $\varsigma_{?Q}(X) = [\![Q]\!] \cap X$
   That is, Angel wins into X for a challenge $?Q$ from the states which satisfy Q to pass the challenge and are already in X, because challenges $?Q$ do not change the state.
4. $\varsigma_{\alpha\cup\beta}(X) = \varsigma_\alpha(X) \cup \varsigma_\beta(X)$
   That is, Angel wins a game of choice $\alpha\cup\beta$ into X whenever she wins α into X or wins β into X (by choosing a subgame she has a winning strategy for).
5. $\varsigma_{\alpha;\beta}(X) = \varsigma_\alpha(\varsigma_\beta(X))$
   That is, Angel wins a sequential game $\alpha;\beta$ into X whenever she has a winning strategy in game α to achieve $\varsigma_\beta(X)$, i.e. to make it to one of the states from which she has a winning strategy in game β to achieve X.
6. $\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathscr{S} : X \cup \varsigma_\alpha(Z) \subseteq Z\}$
   That is, Angel wins a game of repetition α^* into X from the smallest set of states Z that includes both X and the set of states $\varsigma_\alpha(Z)$ from which Angel can achieve Z in one more round of game α.
7. $\varsigma_{\alpha^d}(X) = (\varsigma_\alpha(X^\complement))^\complement$
   That is, Angel wins α^d to achieve X in exactly the states in which she does not have a winning strategy in game α to achieve the opposite $X^\complement$.

Lemma 15.1 (Monotonicity). *The* dGL *semantics is* monotone*, that is, both* $\varsigma_\alpha(X) \subseteq \varsigma_\alpha(Y)$ *and* $\delta_\alpha(X) \subseteq \delta_\alpha(Y)$ *for all* $X \subseteq Y$.

Theorem 16.1 (Consistency & determinacy). *Hybrid games are consistent and determined, i.e.* $\vDash \neg\langle\alpha\rangle\neg P \leftrightarrow [\alpha]P$.

17.3 Hybrid Game Proofs

An axiomatization for differential game logic has been found in previous work [3], where we refer to for more details.

Note 77 (Differential game logic axiomatization [3])

$$[\cdot]\ [\alpha]P \leftrightarrow \neg\langle\alpha\rangle\neg P$$

$$\langle:=\rangle\ \langle x:=e\rangle p(x) \leftrightarrow p(e)$$

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

$$\langle?\rangle\ \langle ?Q\rangle P \leftrightarrow Q\wedge P$$

$$\langle\cup\rangle\ \langle\alpha\cup\beta\rangle P \leftrightarrow \langle\alpha\rangle P \vee \langle\beta\rangle P$$

$$\langle;\rangle\ \langle\alpha;\beta\rangle P \leftrightarrow \langle\alpha\rangle\langle\beta\rangle P$$

$$\langle^*\rangle\ \langle\alpha^*\rangle P \leftrightarrow P \vee \langle\alpha\rangle\langle\alpha^*\rangle P$$

$$\langle^d\rangle\ \langle\alpha^{\mathrm{d}}\rangle P \leftrightarrow \neg\langle\alpha\rangle\neg P$$

$$\mathrm{M}\ \frac{P\to Q}{\langle\alpha\rangle P\to\langle\alpha\rangle Q}$$

$$\mathrm{FP}\ \frac{P\vee\langle\alpha\rangle Q\to Q}{\langle\alpha^*\rangle P\to Q}$$

$$\mathrm{ind}\ \frac{P\to[\alpha]P}{P\to[\alpha^*]P}$$

17.4 Soundness

The dGL proof calculus is sound [3] (and can even be shown to be a sound and complete axiomatization of dGL relative to any differentially expressive logic).

Theorem 17.2 (Soundness of dGL). *The* dGL *proof calculus in Fig. 77 is sound, i.e. all provable formulas are valid.*

Proof. The full proof can be found in [3]. 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 $P\leftrightarrow Q$, show $[\![P]\!]=[\![Q]\!]$ for all interpretations I with any set of states $\mathscr{S}$.

$\langle\cup\rangle$ $[\![\langle\alpha\cup\beta\rangle P]\!]=\varsigma_{\alpha\cup\beta}([\![P]\!])=\varsigma_\alpha([\![P]\!])\cup\varsigma_\beta([\![P]\!])=[\![\langle\alpha\rangle P]\!]\cup[\![\langle\beta\rangle P]\!]=[\![\langle\alpha\rangle P\vee\langle\beta\rangle P]\!]$

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

$\langle?\rangle$ $[\![\langle?Q\rangle P]\!]=\varsigma_{?Q}([\![P]\!])=[\![Q]\!]\cap[\![P]\!]=[\![Q\wedge P]\!]$

$[\cdot]$ is sound by Theorem 16.1.

M Assume the premise $P\to Q$ is valid in interpretation I, i.e. $[\![P]\!]\subseteq[\![Q]\!]$. Then the conclusion $\langle\alpha\rangle P\to\langle\alpha\rangle Q$ is valid in I, i.e. $[\![\langle\alpha\rangle P]\!]=\varsigma_\alpha([\![P]\!])\subseteq\varsigma_\alpha([\![Q]\!])=[\![\langle\alpha\rangle Q]\!]$ by monotonicity (Lemma 15.1). □

17.5 Separating Axioms

The axioms of differential game logic in Fig. 77 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 Chap. 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 axioms that are sound for hybrid systems but not for hybrid games are summarized in Fig. 17.1.

~~K~~	$[\alpha](P\to Q)\to([\alpha]P\to[\alpha]Q)$	$\mathrm{M}_{[\cdot]}$	$\dfrac{P\to Q}{[\alpha]P\to[\alpha]Q}$
~~$\overleftarrow{\mathrm{M}}$~~	$\langle\alpha\rangle(P\vee Q)\to\langle\alpha\rangle P\vee\langle\alpha\rangle Q$	M	$\langle\alpha\rangle P\vee\langle\alpha\rangle Q\to\langle\alpha\rangle(P\vee Q)$
~~I~~	$[\alpha^*]P\leftrightarrow P\wedge[\alpha^*](P\to[\alpha]P)$	ind	$\dfrac{P\to[\alpha]P}{P\to[\alpha^*]P}$
~~B~~	$\langle\alpha\rangle\exists x\,P\to\exists x\langle\alpha\rangle P$ $\quad(x\notin\alpha)$	$\overleftarrow{\mathrm{B}}$	$\exists x\langle\alpha\rangle P\to\langle\alpha\rangle\exists x P$
~~V~~	$p\to[\alpha]p$ $\quad(\mathrm{FV}(p)\cap\mathrm{BV}(\alpha)=\emptyset)$	VK	$p\to([\alpha]\mathit{true}\to[\alpha]p)$
~~G~~	$\dfrac{P}{[\alpha]P}$	$\mathrm{M}_{[\cdot]}$	$\dfrac{P\to Q}{[\alpha]P\to[\alpha]Q}$
~~R~~	$\dfrac{P_1\wedge P_2\to Q}{[\alpha]P_1\wedge[\alpha]P_2\to[\alpha]Q}$	$\mathrm{M}_{[\cdot]}$	$\dfrac{P_1\wedge P_2\to Q}{[\alpha](P_1\wedge P_2)\to[\alpha]Q}$
~~FA~~	$\langle\alpha^*\rangle P\to P\vee\langle\alpha^*\rangle(\neg P\wedge\langle\alpha\rangle P)$		
~~$\overleftarrow{[*]}$~~	$[\alpha^*]P\leftrightarrow P\wedge[\alpha^*][\alpha]P$		

Fig. 17.1 Separating axioms: The axioms and rules on the left are sound for hybrid systems but not for hybrid games. The related axioms or rules on the right are sound for hybrid games.

Detailed counterexamples why the axioms on the left of Fig. 17.1 are unsound for hybrid games are reported in previous work [3], but let us investigate the intuition for the difference causing unsoundness in hybrid games. Kripke's modal modus ponens K from Lemma **??** is unsound for hybrid games: even if Demon can play robot soccer so that his robots score a goal every time they pass the ball (they just never try to pass the ball) and Demon can also play robot soccer so that his robots always pass the ball (somewhere into some random direction), that does not mean Demon would have a strategy to always score goals in robot soccer, because that is significantly more difficult. The problem with axiom K for hybrid games is that Demon's strategies in both assumptions could be incompatible. As Chap. 16 showed, the monotonicity rule M[·] is sound also for hybrid games. The difference to the unsound axiom K is that it requires the implication $P\to Q$ in the premise to be valid, so true in all states, not just in the states that some of Demon's winning strategies reaches as K would. The converse monotonicity axiom $\overleftarrow{\mathrm{M}}$ is unsound for hybrid games: just because Angel WALL·E has a strategy to be close to EVE or far away does not mean WALL·E would either have a strategy to always end up close

to E or a strategy that is always far away. It is a mere triviality to be either close or far, because if WALL·E isn't close to EVE then he's far away. But consistently staying close may be about as challenging as consistently always staying far away. The other direction of the monotonicity axiom M is still sound, because if there is a winning strategy for Angel to achieve P in hybrid game α then she also has a winning strategy to achieve the easier $P \vee Q$.

The induction axiom I from Lemma 7.2 is unsound for hybrid games: just because Demon has a strategy for his robot soccer robots (e.g. power down) that, no matter how often α^* repeats, Demon still has a strategy such that his robots do not run out of battery for just one more control cycle, that does not mean he has a strategy to keep his robots' batteries nonempty all the time. The problem is that one more round may be possible for Demon with the appropriate choices even if the winning condition cannot be sustained forever. The loop induction rule ind (Corollary 16.1) is sound for hybrid games, because its premise requires that $P \rightarrow [\alpha]P$ be valid, not just true for one particular winning strategy of Demon in the hybrid game α^*.

The Barcan axiom B is unsound for hybrid games: just because the winner of a robot soccer tournament who satisfies P can be chosen for x after the robot game α does not mean it would be possible to predict this winner x before the game α. By contrast, the converse Barcan axiom $\overleftarrow{\text{B}}$ is sound for hybrid games since, if known before the game α, selecting the winner for x can still be postponed until after the game x, because that is easier. The reason why both Barcan axioms are sound for hybrid systems is that all choices are nondeterministic in hybrid systems, so there is no opponent that will take an unexpected turn, which is why predicting x ahead of time is possible.

The vacuous axiom V from Lemma 5.11, in which no free variable of p is bound by α, is unsound for hybrid games: even if p does not change its truth-value during α does not mean it would be possible for Demon to reach any final state at all without being tricked into violating the rules of the game along the way by Angel. With an additional assumption ($[\alpha]\mathit{true}$) implying that Demon has a winning strategy to reach any final state at all (in which *true*, i.e. true, holds which imposes no condition), the possible vacuous axiom VK is still sound for hybrid games. Similarly, Gödel's rule G from Lemma 5.12 is unsound for hybrid games: even if P holds in all states, Demon may still fail to win $[\alpha]P$ if he loses prematurely since Angel tricks Demon into violating the rules during the hybrid game α. The monotonicity rule M[·] is similar and sound for hybrid games, because its assumption at least implies that Demon has a winning strategy to get to P at all, which then implies by the premise that he also has a winning strategy to get to the easier Q. Likewise, the regularity rule R is unsound for hybrid games: just because Demon's robot soccer robots have a strategy to focus the robots on strong defense and another strategy to, instead, focus them on strong offense that does not mean he would have a strategy to win robot soccer even if simultaneously strong defense and strong offense together might imply victory (premise), because offensive and defensive strategies are in conflict. Demon cannot possibly send all his robots both into offense and into defense at the same time. They have to choose. A special instance of the monotonicity rule

M[·] is the closest rule that is still sound, because its assumption requires Demon to achieve both P_1 and P_2 at the same time with the same strategy.

The first arrival axiom FA is unsound for hybrid games: just because Angel's robot has a strategy to ultimately capture Demon's faster robot with less battery does not mean she would either start with capture or would have a strategy to repeat her control cycle so that she exactly captures Demon's robot during the next control cycle, as Demon might save up his energy and speed up just when Angel predicted to catch him. Having a better battery, Angel will still ultimately win even if Demon sped ahead, but not in the round she thought she would be able to predict.

Not even the backwards iteration axiom $[\overleftarrow{*}]$ from Lemma 7.10 on p. 225 is sound for hybrid games. However innocently similar the backwards iteration axiom $[\overleftarrow{*}]$ may be to the (sound) forward iteration axiom $[^*]$

$$[^*]\quad [\alpha^*]P \leftrightarrow P \wedge [\alpha][\alpha^*]P$$

The only difference between the unsound $[\overleftarrow{*}]$ and the sound $[^*]$ is whether α^* or α comes first. But that makes a significant difference for hybrid games, because in $[\alpha^*][\alpha]P$ Demon will observe when Angel stopped the repetition α^* but the winning condition P is only checked after one final round of α. Consequently, the right-hand side of the unsound $[\overleftarrow{*}]$ gives Demon one round of early notice about when Angel is going to stop the game, which she will not do in the left-hand side of $[\overleftarrow{*}]$. For example, because of inertia, Demon's robot can easily make sure that it is still moving for one round even though he turned its power off. But that does not mean that the Robot would always keep on moving when its power is off. The following easier instance of $[\overleftarrow{*}]$ is not valid, so the axiom unsound for hybrid games:

$$[(x:=a;a:=0\cap x:=0)^*]x=1 \leftrightarrow \\ x=1\wedge[(x:=a;a:=0\cap x:=0)^*][x:=a;a:=0\cap x:=0]x=1$$

If $a=1$ initially, then the right-hand side is true by Demon's winning strategy of always playing $x:=0$ in the repetition but playing $x:=a;a:=0$ afterwards. The left-hand side is not true, because all that Angel needs to do is repeat sufficiently often at which point Demon will have caused x to be 0, because he cannot predict when Angel will stop. By the sequential composition axiom [;], $[^*]$ and $[\overleftarrow{*}]$ are equivalent to the following two formulas, respectively:

$$[\alpha^*]P \leftrightarrow P \wedge [\alpha;\alpha^*]P \qquad \text{from } [^*] \text{ by } [;]$$
$$[\alpha^*]P \leftrightarrow P \wedge [\alpha^*;\alpha]P \qquad \text{from } [\overleftarrow{*}] \text{ by } [;]$$

From a hybrid systems perspective, the HP $\alpha;\alpha^*$ is equivalent to the HP $\alpha^*;\alpha$, but that does not extend to hybrid games, because hybrid game $\alpha^*;\alpha$ corresponds to Angel announcing the end of the game one round before the game is over, which makes it easier for Demon to win.

Unlike Hare's convergence axiom, Harel's convergence rule [1] is not separating, because it is sound for dGL, just unnecessary. In light of the transfinite iterations explored in Chap. 15, it is questionable whether the convergence rule would be sufficiently complete for hybrid games, because it is based on the existence of bounds on the repetition count. The hybrid version of Harel's convergence rule [2] reads as follows (it assumes that v does not occur in α):

$$\text{con}\ \frac{p(v+1) \land v+1 > 0 \to \langle\alpha\rangle p(v)}{\exists v\, p(v) \to \langle\alpha^*\rangle \exists v{\leq}0\, p(v)}$$

The premise of the convergence rule makes the bound induced by $p(v)$ progress by 1 in each iteration. The postcondition in the conclusion makes it terminate for $v \leq 0$. And the conclusion's antecedent requires a real number for the initial bound. Thus, the convergence rule only permits bounds below ω, not the required transfinite ordinal $\omega \cdot 2$.

17.6 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 rôle in this textbook so far. These differences are discussed in detail elsewhere [3]. In a nutshell, Harel's convergence rule [1] is not a separating axiom, because it is sound for dGL, just unnecessary, and, furthermore, not even particularly useful for hybrid games [3]. The hybrid version of Harel's convergence rule [2] for dL reads as follows (it assumes that v does not occur in α):

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

The dL proof rule con expresses that the variant $p(v)$ holds for some real number $v \leq 0$ after repeating α sufficiently often if $p(v)$ holds for some real number at all in the beginning (antecedent) and, by premise, $p(v)$ 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 $p(v)$ by executing α. Just like the induction rule ind is often used with a separate premiss for the initial and postcondition check (loop from Chap. 7), rule con is often used in the following derived form that we simply call con:

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

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

$$\dfrac{\dfrac{\mathbb{R}\dfrac{*}{x\geq 0\vdash \exists n\, x<n+1}\quad \langle:=\rangle\dfrac{\mathbb{R}\dfrac{*}{x<n+2\land n+1>0\vdash x-1<n+1}}{x<n+2\land n+1>0\vdash \langle x:=x-1\rangle x<n+1}}{\text{con}\dfrac{x\geq 0\vdash \langle x:=x-1\rangle x<n+1}{\to\mathrm{R}\dfrac{}{\vdash x\geq 0\to\langle x:=x-1\rangle x<n+1}}}\quad \mathbb{R}\dfrac{*}{\exists n{\leq}0\, x<n+1\vdash x<1}}{x\geq 0\vdash \langle x:=x-1\rangle x<n+1}$$

Let's compare how dGL proves diamond properties of repetitions based on the iteration axiom $\langle^*\rangle$.

Example 17.1 (Non-game system). The same simple non-game dGL formula

$$x\geq 0\to\langle x:=x-1\rangle^*0\leq x<1$$

as above is provable without con, as shown in Fig. 17.2, where $\langle\alpha^*\rangle 0\leq x<1$ is short for $\langle x:=x-1\rangle^*(0\leq x<1)$. Note that, as in many subsequent proofs, the

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{\forall x(0\leq x<1\vee p(x-1)\to p(x))\to(x\geq 0\to p(x))}\,\mathbb{R}}{\forall x(0\leq x<1\vee\langle x:=x-1\rangle p(x)\to p(x))\to(x\geq 0\to p(x))}\,\langle:=\rangle}{\forall x(0\leq x<1\vee\langle x:=x-1\rangle\langle\alpha^*\rangle 0\leq x<1\to\langle\alpha^*\rangle 0\leq x<1)\to(x\geq 0\to\langle\alpha^*\rangle 0\leq x<1)}\,??}{x\geq 0\to\langle\alpha^*\rangle 0\leq x<1}\,\langle^*\rangle,??,??$$

Fig. 17.2 dGL Angel proof for non-game system Example 17.1 $x\geq 0\to\langle x:=x-1\rangle^*0\leq x<1$

extra assumption for **??** near the bottom of the proof in Fig. 17.2 is provable easily using $\langle^*\rangle$,**??**:

$$\dfrac{\dfrac{*}{\vdash 0\leq x<1\vee\langle x:=x-1\rangle\langle\alpha^*\rangle 0\leq x<1\to\langle\alpha^*\rangle 0\leq x<1}\,\langle^*\rangle}{\vdash\forall x(0\leq x<1\vee\langle x:=x-1\rangle\langle\alpha^*\rangle 0\leq x<1\to\langle\alpha^*\rangle 0\leq x<1)}\,\forall\mathrm{R}$$

Example 17.2 (Choice game). The dGL formula

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

is provable as shown in Fig. 17.3, 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 17.3 (2-Nim-type game). The dGL formula

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

is provable as shown in Fig. 17.3, 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 17.4 (Hybrid game). The dGL formula

$$\langle x:=1;x'=1^{\mathrm{d}}\cup x:=x-1\rangle^*0\leq x<1$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x(x\neq 1\vee p(a,0)\wedge p(0,a)\to p(x,a))\to(true\to p(x,a))}\,\mathbb{R}}{\forall x(x\neq 1\vee\langle\beta\rangle p(x,a)\wedge\langle\gamma\rangle p(x,a)\to p(x,a))\to(true\to p(x,a))}\,\langle;\rangle,\langle:=\rangle}{\forall x(x\neq 1\vee\langle\beta\cap\gamma\rangle p(x,a)\to p(x,a))\to(true\to p(x,a))}\,\langle\cup\rangle,\langle^d\rangle}{\forall x(x\neq 1\vee\langle\beta\cap\gamma\rangle\langle(\beta\cap\gamma)^*\rangle x\neq 1\to\langle(\beta\cap\gamma)^*\rangle x\neq 1)\to(true\to\langle(\beta\cap\gamma)^*\rangle x\neq 1)}\,??}{true\to\langle(\beta\cap\gamma)^*\rangle x\neq 1}\,\langle^*\rangle,??,??}{x=1\wedge a=1\to\langle(\beta\cap\gamma)^*\rangle x\neq 1}\,\mathbb{R}\,{}^*$$

Fig. 17.3 dGL Angel proof for choice game Example 17.2
$x=1\wedge a=1\to\langle(x:=a;a:=0\cap x:=0)^*\rangle x\neq 1$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x(0\leq x<2\vee p(x-1)\wedge p(x-2)\to p(x))\to(true\to p(x))}\,\mathbb{R}}{\forall x(0\leq x<2\vee\langle\beta\rangle p(x)\wedge\langle\gamma\rangle p(x)\to p(x))\to(true\to p(x))}\,\langle:=\rangle}{\forall x(0\leq x<2\vee\langle\beta\cap\gamma\rangle p(x)\to p(x))\to(true\to p(x))}\,\langle\cup\rangle,\langle^d\rangle}{\forall x(0\leq x<2\vee\langle\beta\cap\gamma\rangle\langle(\beta\cap\gamma)^*\rangle 0\leq x<2\to\langle(\beta\cap\gamma)^*\rangle 0\leq x<2)\to(true\to\langle(\beta\cap\gamma)^*\rangle 0\leq x<2)}\,??}{true\to\langle(\beta\cap\gamma)^*\rangle 0\leq x<2}\,\langle^*\rangle,??,??}{x\geq 0\to\langle(\beta\cap\gamma)^*\rangle 0\leq x<2}\,\mathbb{R}\,{}^*$$

Fig. 17.4 dGL Angel proof for 2-Nim-type game Example 17.3
$x\geq 0\to\langle(x:=x-1\cap x:=x-2)^*\rangle 0\leq x<2$

is provable as shown in Fig. 17.5, where the notation $\langle(\beta\cup\gamma)^*\rangle 0\leq x<1$ is short for $\langle(x:=1;x'=1^{\mathrm{d}}\cup x:=x-1)^*\rangle(0\leq x<1)$: The proof steps for β use in $\langle'\rangle$ that

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x(0\leq x<1\vee\forall t\geq 0\,p(1+t)\vee p(x-1)\to p(x))\to(true\to p(x))}\,\mathbb{R}}{\forall x(0\leq x<1\vee\langle x:=1\rangle\neg\exists t\geq 0\langle x:=x+t\rangle\neg p(x)\vee p(x-1)\to p(x))\to(true\to p(x))}\,\langle:=\rangle}{\forall x(0\leq x<1\vee\langle x:=1\rangle\neg\langle x'=1\rangle\neg p(x)\vee p(x-1)\to p(x))\to(true\to p(x))}\,\langle'\rangle}{\forall x(0\leq x<1\vee\langle\beta\rangle p(x)\vee\langle\gamma\rangle p(x)\to p(x))\to(true\to p(x))}\,\langle;\rangle,\langle^d\rangle}{\forall x(0\leq x<1\vee\langle\beta\cup\gamma\rangle p(x)\to p(x))\to(true\to p(x))}\,\langle\cup\rangle}{\forall x(0\leq x<1\vee\langle\beta\cup\gamma\rangle\langle(\beta\cup\gamma)^*\rangle 0\leq x<1\to\langle(\beta\cup\gamma)^*\rangle 0\leq x<1)\to(true\to\langle(\beta\cup\gamma)^*\rangle 0\leq x<1)}\,??}{true\to\langle(\beta\cup\gamma)^*\rangle 0\leq x<1}\,\langle^*\rangle,??,??\,{}^*$$

Fig. 17.5 dGL Angel proof for hybrid game Example 17.4
$\langle(x:=1;x'=1^{\mathrm{d}}\cup x:=x-1)^*\rangle 0\leq x<1$

$t\mapsto x+t$ is the solution of the differential equation, so the subsequent use of $\langle:=\rangle$ substitutes 1 in for x to obtain $t\mapsto 1+t$. Recall from Chap. 16 that the winning regions for this formula need $>\omega$ iterations to converge. It is still provable easily.

17.7 Appendix: Relating Differential Game Logic and Differential Dynamic Logic

Now that we have come to appreciate the value of soundness, couldn't we have known about that, for the most part, before Theorem 17.2? Most dGL axioms look rather familiar, except for $\langle\cdot\rangle$ versus $[\cdot]$ dualities, when we compare them to the dL axioms from Chap. 5. Does that not mean that these same axioms are already trivially sound? Why did we go through the (rather minor) trouble of proving Theorem 17.2?

Before you read on, see if you can find the answer for yourself.

It is not quite so easy. After all, we could have given the same syntactical operator $\cup$ an entirely different meaning for hybrid games than before for hybrid systems. Maybe we could have been silly and flipped the meaning of ; and $\cup$ around The fact of the matter is, of course, that we did not. The operator $\cup$ still means choice, just for hybrid games rather than hybrid systems. So could we deduce the soundness of the dGL axioms in Fig. 77 from the soundness of the corresponding dL axioms from Chap. 5 and focus on the new axioms, only?

Before we do anything of the kind, we first need to convince ourselves that the dL semantics really coincides with the more general dGL semantics in case there are no games involved. How could that be done? Maybe by proving validity of all formulas of the following form

$$\underbrace{\langle\alpha\rangle P}_{\text{in dL}} \leftrightarrow \underbrace{\langle\alpha\rangle P}_{\text{in dGL}} \tag{17.1}$$

for dual-free hybrid games α, i.e. those that do not mention ^{d} (not even indirectly hidden in the abbreviation $\cap,^{\times}$).

Before you read on, see if you can find the answer for yourself.

The problem with (17.1) is that it is not directly a formula in any logic, because the $\leftrightarrow$ operator could hardly be applied meaningfully to two formulas from different logics. Well, of course, every dL formula is a dGL formula, so the left-hand side of (17.1) could be embedded into dGL, but then (17.1) becomes well-defined but is only stating a mere triviality.

Instead, a proper approach would be to rephrase the well-intended (17.1) semantically:

$$\underbrace{\omega \in [\![\langle\alpha\rangle P]\!]}_{\text{in dL}} \text{ iff } \underbrace{\omega \in [\![\langle\alpha\rangle P]\!]}_{\text{in dGL}} \tag{17.2}$$

which is equivalent to

$$\Big(\underbrace{\nu \in [\![P]\!] \text{ for some } \nu \text{ with } (\omega,\nu) \in [\![\alpha]\!]}_{\text{statement about reachability in dL}}\Big) \text{ iff } \underbrace{\omega \in \varsigma_\alpha([\![P]\!])}_{\text{winning in dGL}}$$

Equivalence (17.2) can be shown. In fact, Exercise 3.9 in Chap. 3 already developed an understanding of the dL semantics based on sets of states, preparing for(17.2).

The trouble is that, besides requiring a proof itself, the equivalence (17.2) will still not quite justify soundness of the dGL axioms in Fig. 77 that look innocuously like dL axioms. Equivalence (17.2) is for dual-free hybrid games α. But even if the top-level operator in axiom $\langle\cup\rangle$ is not ^{d}, that dual operator could still occur within α or α, which requires a game semantics to make sense of.

Consequently, we are better off proving soundness for the dGL axioms according to their actual semantics, like in Theorem 17.2, as opposed to trying half-witted ways out that only make soundness matters worse.

Exercises

17.1 (***). The following formula was proved using dGL's hybrid games proof rules in Fig. 17.2

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

Try to prove it using the convergence rule con instead.

References

1. Harel, D., Meyer, A. R. & Pratt, V. R. *Computability and Completeness in Logics of Programs (Preliminary Report)* in *STOC* (ACM, 1977), 261–268.
2. Platzer, A. Differential Dynamic Logic for Hybrid Systems. *J. Autom. Reas.* **41,** 143–189 (2008).
3. Platzer, A. Differential Game Logic. *ACM Trans. Comput. Log.* **17,** 1:1–1:51 (2015).