Chapter 17
Game Proofs & Separations

Synopsis The primary purpose of this chapter is to compare the proof principles of hybrid games versus those of hybrid systems. Having established reasoning principles for hybrid games in the previous chapter, our attention shifts to contrasting and identifying what the actual difference really is. Despite being rooted in a different semantics, hybrid game axioms are surprisingly close to those for hybrid systems. But there are also some major soundness-critical discrepancies to notice. These findings are important for correctly reasoning about hybrid games, but also shine a complementary light on reasoning principles for hybrid systems by highlighting which ones crucially depend on the absence of adversarial dynamics.

17.1 Introduction

This chapter continues the study of hybrid games and their logic, differential game logic [4]. After Chap. 14 introduced hybrid games and Chap. 15 developed their winning-region semantics, Chap. 16 achieved major breakthroughs in their understanding by studying the axioms of hybrid games. The resulting simple axioms made it surprisingly easy to prove correctness properties of hybrid games with dGL in ways that were quite similar to how we have already successfully proved properties of hybrid systems with dL in this book.

Of course, it should make us wonder why two logics that are based on such different conditions (hybrid systems versus hybrid games) end up being so surprisingly close in their axioms. And, indeed, upon closer inspection, we will find notable differences that we definitely need to respect when analyzing hybrid games. The chapter starts out with a comparison of the axioms of hybrid systems versus hybrid games and inspects what we have missed so far when considering hybrid game axioms. We will find a surprising logical robustness that even two semantically quite different logics end up having, for the most part, quite similar axioms.

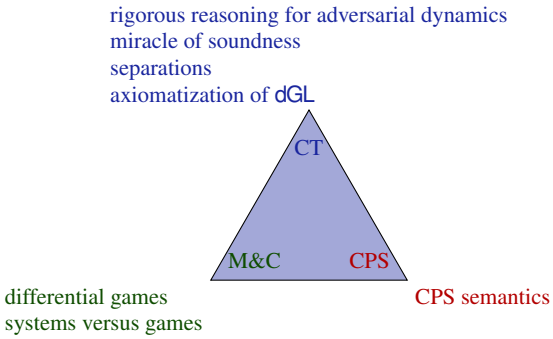
This chapter is based on prior work [4], where more information can be found on logic and hybrid games. The most important learning goals of this chapter are:

A. Platzer, *Logical Foundations of Cyber-Physical Systems*,
https://doi.org/10.1007/978-3-319-63588-0_17

Modeling and Control: While the primary learning objectives in this chapter come from computational thinking, modeling and control observations still find out in passing that continuous and adversarial dynamics also mix in the form of differential games to which differential game logic generalizes [5]. A coverage of those findings is beyond the scope of this textbook, though.

Computational Thinking: This chapter solidifies our understanding of rigorous reasoning techniques for CPS models involving adversarial dynamics. Its primary purpose is to identify which hybrid systems reasoning principles are still sound for hybrid games and which ones crucially depend on the absence of adversariality. This delineation is critical to ensure that no incorrect arguments enter our proofs for CPSs with adversarial interactions. This refined understanding of what is sound and what is not also leads to a new appreciation for the robustness of logic. Finally, these findings shine a complementary light on what is specific to hybrid systems and what is more general.

CPS Skills: We will develop a complementary understanding of CPS models and how they are impacted by the presence or absence of adversariality. Being rooted in a syntactic characterization of the difference of hybrid systems and hybrid games, this understanding will make it easier to pinpoint what the exact nuances in different CPS operations and arguments are.



17.2 Recap: Hybrid Games

Recall a result from Chap. 16 and, in Fig. 17.1, the axiomatization of differential game logic [4] that Chap. 16 discussed.

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

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

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

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

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

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

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

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

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

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

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

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

Fig. 17.1 Differential game logic axiomatization (repeated)

17.3 Separating Axioms

Parts I and II of this textbook identified a number of useful axioms for hybrid systems. Chapter 16 did the same for hybrid games, albeit at a faster pace, because the earlier parts of this book already prepared us well for the typical challenges when developing and using axioms. When we compare the axioms of differential game logic dGL (Fig. 17.1) to those of differential dynamic logic dL, we notice that they share significant similarities. But the dGL axioms already had more involved soundness justifications, most notably in axiom $[\cdot]$, which is a simple observation for hybrid systems (all runs satisfy P iff it is not the case that there is a run satisfying $\neg P$) but already needs the full determinacy theorem Theorem 16.1 as justification for hybrid games.

Without any doubt, the axioms of differential game logic in Fig. 17.1 are sound for hybrid systems as well, because every hybrid system is a (single-player) hybrid game. In fact, except of course the duality axiom $\langle^d\rangle$, they all look surprisingly close to the axioms for hybrid systems from Chaps. 5 and 7. Many look almost identical when comparing dL axioms in Fig. 5.4 on p. 160 to the box modality formulation of the dGL axioms in Fig. 16.4 on p. 505. If they look so close, couldn't we have arrived at the dGL axioms more quickly by inferring them from dL axioms?

Well not quite, because all axioms for hybrid games are sound for hybrid systems, since all hybrid systems are hybrid games, but not the other way around! We need to pay more attention and conduct more refined proofs to justify that axioms are *even*

sound for hybrid games, not just hybrid systems, because hybrid games can exhibit more behaviors. Of course, we could still have used hybrid systems axioms as an inspiration for possible hybrid games axioms, precisely because of the fact that an axiom can only work for hybrid games if it is, at least, sound for hybrid systems. But once we list hybrid system axioms, we need to scrutinize them very carefully to ensure they continue to be sound for hybrid games, still. In fact, the best preparation for this chapter is to do exactly that by first solving Exercise 16.9.

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

In order to understand the fundamental difference between hybrid systems and hybrid games, it is instructive to 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. 17.2.

~~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~~	$\langle\alpha\rangle\exists xP\to\exists x\langle\alpha\rangle P\quad(x\notin\alpha)$	$\overleftarrow{\mathrm{B}}$	$\exists x\langle\alpha\rangle P\to\langle\alpha\rangle\exists xP$
~~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~~	$\langle\alpha^*\rangle P\to P\vee\langle\alpha^*\rangle(\neg P\wedge\langle\alpha\rangle P)$		
~~$\overleftarrow{[*]}$~~	$[\alpha^*]P\leftrightarrow P\wedge[\alpha^*][\alpha]P$	[*]	$[\alpha^*]P\leftrightarrow P\wedge[\alpha][\alpha^*]P$

Fig. 17.2 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 showing that the axioms on the left of Fig. 17.2 are unsound for hybrid games are reported in previous work [4], but let us investigate the intuition for the difference causing their unsoundness in hybrid games. Kripke's modal modus ponens K from Lemma 5.9 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 even pass the ball) and Demon can also play robot soccer so that his robots always pass the ball (somewhere in some random direction), that does not mean Demon has a strategy to always score goals in robot soccer, because that is significantly more difficult to achieve. The problem with axiom K for hybrid games is that Demon's strategies in its two assumptions can be incompatible, which is something that cannot happen in hybrid systems where both box modalities refer to all runs of HP α.

A concrete counterexample illustrating why K is unsound for hybrid games is

$$[x:=0\cap(x:=1\cup x:=-1)](x\neq 0\to x>0)\to$$
$$\big([x:=0\cap(x:=1\cup x:=-1)]x\neq 0\to[x:=0\cap(x:=1\cup x:=-1)]x>0\big)$$

The first assumption is *true*, because Demon can play left ($x:=0$), which trivially satisfies the postcondition $x\neq 0\to x>0$. The second assumption is *true*, because Demon can play right ($x:=1\cup x:=-1$), which satisfies $x\neq 0$ whichever way Angel decides. But there is no winning strategy that enables Demon to achieve $x>0$, because playing left makes x zero and playing right enables Angel to play right ($x:=-1$), too.

As Chap. 16 showed, the closely related monotonicity rule M[·] is sound also for hybrid games. The difference of monotonicity rule M[·] to the unsound Kripke 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 axiom K requires. The converse monotonicity axiom $\overleftarrow{\text{M}}$, however, is also unsound for hybrid games: just because Angel EVE has a strategy to be close to WALL·E or far away does not mean EVE either has a strategy to always end up close to WALL·E or a strategy to always be far away. It is a mere triviality to be either close or far, because if EVE isn't close to WALL·E then she's far away. Period. 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 $P\vee Q$, because P implies $P\vee Q$.

The induction axiom I from Lemma 7.1 is unsound for hybrid games: just because Demon has a strategy for his 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 (one control cycle does not need a lot of battery), that does not mean he has a strategy to keep his robots' batteries nonempty all the time, because that would require quite a revolution in battery designs. The problem is that one more round may be possible for Demon with the appropriate control 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 $P\to[\alpha]P$ be valid so true in all states, not just true for one particular winning strategy of Demon in the hybrid game α^*.

The Barcan axiom B, which provides a way of commuting modalities with like-minded quantifiers [1], 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 is possible to predict this winner x before the game α. By contrast, the converse Barcan axiom $\overleftarrow{\text{B}}$ [1] is sound for hybrid games since, if x is known before the game α, selecting the winner for x can still be postponed until after the game, because that is much 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 is 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 ($[\alpha]true$) implying that Demon has a winning strategy to reach any final state at all (in which *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 following counterexample is an instance of Gödel's rule G with a valid premise but a conclusion that is equivalent to *false*:

$$\frac{true}{[?false^{\mathrm{d}}]true}$$

The monotonicity rule M[·] is again similar to Gödel's G but 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 soccer robots have a strategy to focus all robots on strong defense and another strategy to, instead, focus them all on strong offense that does not mean he has 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, because they won't know which way to go. 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, which, by the premise, implies Q.

The first-arrival axiom FA, which is the dual of the induction axiom I, 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 either starts with capture or has 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 expected to catch him. Having a better battery, Angel will still ultimately win even if Demon speeds ahead, but not in the round she thought she would be able to predict.

Another way of understanding why several hybrid systems axioms summarized in Fig. 17.2 are not sound for hybrid games is that hybrid games can turn box modalities into diamond modalities by duality and vice versa. After all, the duality axiom $\langle^d\rangle$ together with the determinacy axiom [·] derive

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

Consequently, if an axiom such as K were sound for hybrid games, then it would also be sound for the hybrid game α^{d} instead of α, which, by axioms $\langle^d\rangle$,$[\cdot]$, turns its box modalities into diamond modalities, but the resulting pure diamond formulation of K is not even sound for hybrid systems:

$$\langle\alpha\rangle(P \to Q) \to (\langle\alpha\rangle P \to \langle\alpha\rangle Q)$$

Note 79 (One game's boxes are another game's diamonds) If a hybrid systems axiom is not also sound when replacing box modalities with diamond modalities and vice versa, then it cannot possibly be sound for hybrid games.

This principle does not explain all cases listed in Fig. 17.2, though! Not even the backwards iteration axiom $\overleftarrow{[*]}$ from Lemma 7.5 on p. 239 is sound for hybrid games, however innocently similar the backwards iteration axiom $\overleftarrow{[*]}$ may be to the (sound) forward iteration axiom $[^*]$. The only difference between the unsound $\overleftarrow{[*]}$ and the sound axiom $[^*]$ is whether α or the repetition 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 will always keep on moving when its power is off. The following easier instance of hybrid systems axiom $\overleftarrow{[*]}$ is not valid, so the axiom is 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 [;], the two formulas from axioms $[^*]$ 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! 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. Unrolling loops in the beginning is acceptable in hybrid games, but unrolling them in the end may change their semantics! Unrolling loops

at the end as in $[^*]$ is not sound for hybrid games, because it requires predicting the end of the game prematurely.

17.4 Repetitive Diamonds – Convergence Versus Iteration

More fundamental differences between hybrid systems and hybrid games also exist in terms of convergence rules, even if these have not played a prominent rôle in this textbook. These differences are discussed in detail elsewhere [4]. In a nutshell, Harel's convergence rule [2] is not separating, because it is sound for dGL, just unnecessary, and, furthermore, not even particularly useful for hybrid games [4]. The hybrid version of Harel's convergence rule [3] for dL makes it possible to prove diamond properties of loops. It reads as follows (where v does not occur in α):

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

The convergence rule con uses a *variant* $p(v)$, which is the diamond counterpart of an invariant of the induction rule loop for box modalities of repetitions. Just as an invariant expresses what never changes as a loop executes (Chap. 7), a variant expresses what does change and make progress toward a goal when a loop executes. The dL proof rule con expresses that the variant $p(v)$ holds for some nonpositive real number $v\leq 0$ after repeating α sufficiently often if $p(v)$ holds for any 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. The variant $p(v)$ is an abstract progress measure that can decrease by at least 1 unless already at the goal and will, thus, eventually reach the goal (for a nonpositive distance $v\leq 0$).

Just as the induction rule ind is often used with a separate premise for the initial and postcondition check (loop from Chap. 7), rule con is often used in the following derived form that we simply also call con since it will be easy enough for us now to disambiguate which of the two versions of the rule we are referring to:

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

The following sequent proof shows how convergence rule con with $x<n+1$ for $p(n)$ can be used to prove a simple dL liveness property of a discrete HP:

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

Let's compare how dGL proves diamond properties of repetitions based on the iteration axiom $\langle^*\rangle$. In addition to the iteration axiom $\langle^*\rangle$, the following proofs for diamond repetitions employ a clever use of the uniform substitution proof rule US, which concludes that any substitution instance of a provable formula is provable, too. That is, if ϕ has a proof, then the instance $\sigma(\phi)$ that is obtained by performing any (admissible) uniform substitution σ on ϕ is valid, too:

$$\text{US}\ \frac{\phi}{\sigma(\phi)}$$

Uniform substitutions replace function symbols with suitable terms and predicate symbols by logical formulas. For example, a uniform substitution σ may substitute an abstract predicate symbol p such that $p(x)$ is replaced with the dL formula $\langle(x:=x-1)^*\rangle(0\leq x<1)$ of the (same) free variable x. Uniform substitution will be explored in Chap. 18 of Part IV, but its intuition can already be easily understood, which is all we need right now. For the time being, all that is important to know about it is that rule US substitutes formulas for predicate symbols and has appropriate implementations that check and ensure soundness. Using it from the conclusion to its premise, rule US can be used to abstract formulas by predicate symbols. And all we need to know about predicate symbols is that they are indeed symbolic in the sense that unlike for a concrete logical formula such as $0\leq x<1$ we do not know a priori when exactly $p(x)$ is *true*.

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

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

above is provable without con, as shown in Fig. 17.3, where $\langle\alpha^*\rangle 0\leq x<1$ is short for $\langle(x:=x-1)^*\rangle(0\leq x<1)$. Note that, as in the subsequent proofs, the extra assumption for cut near the bottom of the proof in Fig. 17.3 is provable by $\langle^*\rangle$,$\forall$R:

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

The rôle of the predicate symbol in Fig. 17.3 is to have $p(x)$ serve as an abstract formula standing for $\langle(x:=x-1)^*\rangle(0\leq x<1)$. Since the premise of rule US can be proved for the abstract predicate $p(x)$, its conclusion for the concrete formula $\langle(x:=x-1)^*\rangle(0\leq x<1)$ in place of $p(x)$ is valid by rule US as well.

Example 17.2 (Choice game). The dGL formula

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

is provable as shown in Fig. 17.4, where $\beta\cap\gamma$ is short for $x:=a;a:=0\cap x:=0$ and $\langle(\beta\cap\gamma)^*\rangle x\neq 1$ is short for $\langle(x:=a;a:=0\cap x:=0)^*\rangle x\neq 1$.

Example 17.3 (2-Nim-type game). The dGL formula

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x(0\le x<1\vee p(x-1)\to p(x))\to(x\ge 0\to p(x))}\,\mathbb{R}}{\forall x(0\le x<1\vee\langle x:=x-1\rangle p(x)\to p(x))\to(x\ge 0\to p(x))}\,\langle:=\rangle}{\forall x(0\le x<1\vee\langle x:=x-1\rangle\langle\alpha^*\rangle 0\le x<1\to\langle\alpha^*\rangle 0\le x<1)\to(x\ge 0\to\langle\alpha^*\rangle 0\le x<1)}\,\mathrm{US}}{x\ge 0\to\langle\alpha^*\rangle 0\le x<1}\,\langle^*\rangle,\forall\mathrm{R},\mathrm{cut}$$

Fig. 17.3 dGL Angel proof for non-game system Example 17.1 $x\ge 0\to\langle(x:=x-1)^*\rangle 0\le x<1$

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

Fig. 17.4 dGL Angel proof for demonic choice game Example 17.2
$x=1\wedge a=1\to\langle(x:=a;a:=0\cap x:=0)^*\rangle x\neq 1$

$$x\ge 0\to\langle(x:=x-1\cap x:=x-2)^*\rangle 0\le x<2$$

is provable as shown in Fig. 17.5, where $\beta\cap\gamma$ is short for $x:=x-1\cap x:=x-2$ and $\langle(\beta\cap\gamma)^*\rangle 0\le x<2$ is short for $\langle(x:=x-1\cap x:=x-2)^*\rangle 0\le x<2$.

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

Fig. 17.5 dGL Angel proof for 2-Nim-type game Example 17.3
$x\ge 0\to\langle(x:=x-1\cap x:=x-2)^*\rangle 0\le x<2$

Example 17.4 (Hybrid game). The dGL formula

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

is provable as shown in Fig. 17.6, where the notation $\langle(\beta\cup\gamma)^*\rangle 0\le x<1$ is short for $\langle(x:=1;x'=1^{\mathrm{d}}\cup x:=x-1)^*\rangle(0\le x<1)$: The proof steps for β use in $\langle'\rangle$ that $t\mapsto x+t$ 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.

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

Fig. 17.6 dGL Angel proof for hybrid game Example 17.4
$\langle (x := 1; x' = 1^{\mathrm{d}} \cup x := x - 1)^* \rangle 0 \le x < 1$

A downside of the approach of using uniform substitution rule US with the iteration axiom $\langle^*\rangle$ to prove diamond properties of loops is that the resulting arithmetic (marked $\mathbb{R}$) mixes real arithmetic with predicate symbols, which is quite challenging. This is a reason to still take note of the convergence rule con despite its limitations.

17.5 Summary

This chapter solidified our understanding of rigorous reasoning principles for hybrid games by developing an appreciation for the axiomatic differences of hybrid systems versus hybrid games. While the previous chapter emphasized the aspects of surprising similarities of hybrid systems and hybrid games reasoning, this chapter now carefully emphasized the differences. We have explored intuitive reasons, which make it easier to remember which axioms can carry over from hybrid systems to hybrid games. But it is, of course, crucial for soundness in our arguments to understand precisely which hybrid systems axioms continue to be sound for hybrid games.

The sophisticated differential equation reasoning principles from Part II that prove properties of differential equations without the need for explicit closed-form solutions carry over to hybrid games, because they do not involve any game aspects. More importantly, though, differential invariants generalize to differential games that directly combine continuous and adversarial dynamics by allowing both players to provide continuous-time input on which the differential equation depends [5]. The idea is to give both players the ability to provide input controls during the continuous system while following a differential game.

17.6 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 the soundness result of Theorem 16.2? Most dGL axioms look rather familiar 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 to the (admittedly rather minor) trouble of proving Theorem 16.2?

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 just to confuse everybody. 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 can we deduce the soundness of the dGL axioms in Fig. 17.1 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 coincide with the more general dGL semantics in case there are no games involved. How can that be done? Maybe by proving the 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 abbreviations $\cap, ^{\times}$).

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 can 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) would become well-defined but is only stating a mere triviality. Everything is equivalent to itself, which is not a gigantic insight to write home about.

Instead, a proper approach would be to rephrase the well-intended but ill-fated (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 3.15 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. 17.1 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 can still occur within α or β, which can only be made sense of with a game semantics.

Consequently, we are much better off proving soundness for the dGL axioms according to their actual semantics, like in Theorem 16.2, as opposed to trying half-witted ways out that only make soundness matters worse.

Exercises

17.1 (Good and bad axioms). Prove each of the axioms on the left of Fig. 17.2 to be unsound for hybrid games. For each of the axioms, provide a concrete dGL formula that is an instance of that axiom but not a valid formula. For the unsound proof rules on the left of Fig. 17.2 give an instance where the premise is valid but the conclusion is not. Then go on to show a way of using each of the reasoning principles on the right of Fig. 17.2 for a hybrid game.

17.2. Prove the following dGL formula with the iteration and uniform substitution technique as in Example 17.2

$$\langle (x:=x^2 \cup (x:=x+1 \cap x'=2))^* \rangle x>0$$

17.3 (***). The following formula was proved using dGL's hybrid games proof rules in Fig. 17.3

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

Try to see whether you can prove it using the convergence rule con instead.

References

[1] Ruth C. Barcan. The deduction theorem in a functional calculus of first order based on strict implication. *J. Symb. Log.* **11**(4) (1946), 115–118.

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

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

[4] André Platzer. Differential game logic. *ACM Trans. Comput. Log.* **17**(1) (2015), 1:1–1:51. DOI: 10.1145/2817824.

[5] André Platzer. Differential hybrid games. *ACM Trans. Comput. Log.* **18**(3) (2017), 19:1–19:44. DOI: 10.1145/3091123.