André Platzer

Lecture Notes on Foundations of Cyber-Physical Systems

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

Chapter 16
Winning & Proving Hybrid Games

Synposis This chapter begins the development of the logical characterization of the dynamics of hybrid games, which proves from which state which player can win which game. It investigates compositional reasoning principles with dynamic axioms for adversarial dynamical systems, where each axiom captures how the existence of a winning strategy for a more complex hybrid game relates to the existence of corresponding winning strategies for simpler game fragments. These dynamic axioms enable rigorous reasoning for adversarial CPS models and axiomatize differential game logic, which turns the specification logic dGL into a verification logic for CPS. This is the cornerstone for lifting hybrid systems reasoning techniques to hybrid games.

16.1 Introduction

This chapter continues the study of hybrid games and their logic, differential game logic [10], whose syntax was introduced in Chap. 14 and whose semantics was developed in Chap. 15. This chapter furthers the development of differential game logic to the third leg of the logical trinity: its axiomatics. It will focus on the development of rigorous reasoning techniques for hybrid games as models for CPS with adversarial dynamics. Without such analysis and reasoning techniques, a logic that only comes with syntax and semantics can be used as a specification language with a precise meaning, but would not be very helpful for actually analyzing and verifying hybrid games. It is the logical trinity of syntax, semantics, and axiomatics that gives logics the power of serving as well-founded specification and verification languages with a (preferably concise) syntax, an unambiguous semantics, and actionable analytic reasoning principles. Thus, this chapter is the hybrid games analogue of Chap. 5. Indeed, after the logical sophistication we reached throughout the textbook, this chapter will settle for a Hilbert-type calculus as in Chap. 5 as opposed to the more easily automatable sequent calculus from Chap. 6.

Playing hybrid games is fun. Winning hybrid games is even more fun. But the most fun comes from proving that you'll win a hybrid game. Only don't tell your opponent that you have proved that you have a winning strategy, because he might not want to play this game with you any more.

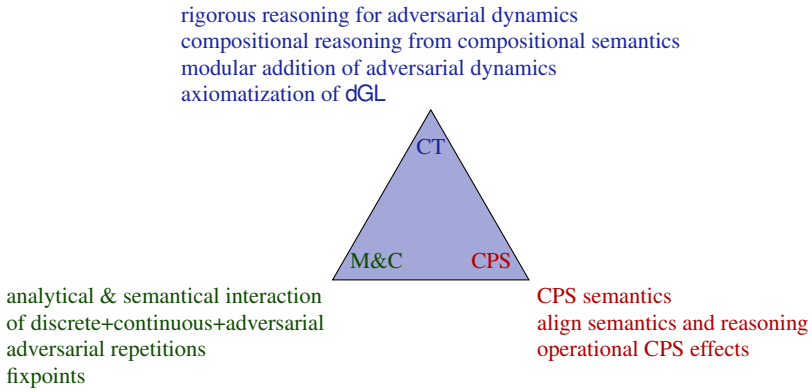
Before submerging completely into the development of rigorous reasoning techniques for hybrid games as models for CPS with adversarial dynamics, however, it will be wise to take a short detour by investigating some simple properties of their semantics.

This chapter is based on [10], where more information can be found on logic and hybrid games. The most important learning goals of this chapter are:

Modeling and Control: We advance our understanding of the core principles behind CPS with hybrid games by understanding analytically and semantically how discrete, continuous, and the adversarial dynamics resulting, e.g., from multiple agents are integrated and interact in CPS. This chapter also uncovers nuances in the semantics of adversarial repetitions that makes them conceptually better behaved than the highly transfinite iterated winning region construction from Chap. 15. A byproduct of this development shows fixpoints in actions, which play a prominent rôle in the understanding of other classes of models as well and provides one important aspect for the subsequent development of reasoning techniques.

Computational Thinking: This chapter is devoted to the development of rigorous reasoning techniques for CPS models involving adversarial dynamics, which is critical to getting CPS with such interactions right. Hybrid games provide even more subtle interactions than hybrid systems did, which make it even more challenging to say for sure whether and why a design is correct without sufficient rigor in their analysis. After Chap. 15 captured the semantics of differential game logic and hybrid games compositionally, this chapter exploits the compositional meaning to develop compositional reasoning principles for hybrid games. This chapter systematically develops one reasoning principle for each of the operators of hybrid programs, resulting in a compositional verification approach. A compositional semantics is de facto a necessary but not a sufficient condition for the existence of compositional reasoning principles. Despite the widely generalized semantics of hybrid games compared to hybrid systems, this chapter will strive to generalize reasoning techniques for hybrid systems to hybrid games as smoothly as possible. This leads to a modular way of integrating adversariality into the realm of hybrid systems models also in terms of their analysis while simultaneously taming their complexity. This chapter provides an *axiomatization* of differential game logic dGL [10] to lift dGL from a specification language to a verification language for CPS with adversarial dynamics.

CPS Skills: We will develop a deep understanding of the semantics of CPS models with adversariality by carefully relating their semantics to their reasoning principles and aligning them in perfect unison. This understanding will also enable us to develop a better intuition for the operational effects involved in CPS. This chapter also shows insightful and influential nuances on the semantics of repetitions in CPS models with adversarial dynamics.



In our quest to develop rigorous reasoning principles for hybrid games, we will strive to identify compositional reasoning principles that align in perfect unison with the compositional semantics of hybrid games developed in Chap. 15. This enterprise will be enlightening and, for the most part, quite successful. And, in fact, the reader is encouraged to start right away with the development of a proof calculus for differential game logic and later compare it with the one that this textbook develop. The part, where this will turn out to be rather difficult is repetition, which is why the textbook take a scenic detour through characterizing their semantics.

16.2 Semantical Considerations

This section discusses simple but important meta-properties of the semantics of hybrid games that we will make use of subsequently, but which are also of independent interest.

16.2.1 Recap: Semantics of Hybrid Games

Before establishing any of their properties, first recall the semantics of hybrid games from Chap. 15.

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. $\varsigma_{x'=f(x)\&Q}(X) = \{\varphi(0) \in \mathscr{S} : \varphi(r) \in X \text{ for some solution } \varphi : [0,r] \to \mathscr{S} \text{ of any duration } r \in \mathbb{R} \text{ satisfying } \varphi \models x' = f(x) \wedge Q\}$
   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 $X^{\complement}$.

Definition 15.5 (Semantics of hybrid games, continued). 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:

1. $\delta_{x:=e}(X) = \{\omega \in \mathscr{S} : \omega_x^{\omega[\![e]\!]} \in X\}$
   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. $\delta_{x'=f(x)\&Q}(X) = \{\varphi(0) \in \mathscr{S} : \varphi(r) \in X \text{ for all durations } r \in \mathbb{R} \text{ and all solutions } \varphi : [0,r] \to \mathscr{S} \text{ satisfying } \varphi \models x' = f(x) \wedge Q\}$
   That is, Demon wins the differential equation $x' = f(x)\&Q$ into X from any state $\varphi(0)$ from which all solutions φ of $x' = f(x)$ of any duration r that remain within Q all the time lead to states $\varphi(r) \in X$ in the end.
3. $\delta_{?Q}(X) = ([\![Q]\!])^{\complement} \cup X$
   That is, Demon wins into X for a challenge $?Q$ from the states which violate Q so that Angel fails her challenge $?Q$ or that are already in X, because challenges $?Q$ do not change the state.

4. $\delta_{\alpha\cup\beta}(X) = \delta_\alpha(X) \cap \delta_\beta(X)$
   That is, Demon wins a game of choice $\alpha\cup\beta$ into X whenever he wins α into X and wins β into X (because Angel might choose either subgame).
5. $\delta_{\alpha;\beta}(X) = \delta_\alpha(\delta_\beta(X))$
   That is, Demon wins a sequential game $\alpha;\beta$ into X whenever he has a winning strategy in game α to achieve $\delta_\beta(X)$, i.e. to make it to one of the states from which he has a winning strategy in game β to achieve X.
6. $\delta_{\alpha^*}(X) = \bigcup\{Z \subseteq \mathscr{S} : Z \subseteq X \cap \delta_\alpha(Z)\}$
   That is, Demon wins a game of repetition α^* into X from the biggest set of states Z that is included both in X and in the set of states $\delta_\alpha(Z)$ from which Demon can achieve Z in one more round of game α.
7. $\delta_{\alpha^d}(X) = (\delta_\alpha(X^\complement))^\complement$
   That is, Demon wins α^d to achieve X in exactly the states in which he does not have a winning strategy in game α to achieve the opposite $X^\complement$.

16.2.2 Monotonicity

As Chap. 15 already conjectured, the semantics is monotone [10], i.e. larger sets of winning states have larger winning regions, as it is easier to win into larger sets of winning states (Fig. 15.3 on p. 417).

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* $X \subseteq Y$.

Proof. The proof is a simple check of Definition 15.4 based on the observation that X only occurs with an even number of negations in the semantics. It easily proves by induction on the structure of the hybrid game α. So when proving Lemma 15.1 for a hybrid game α, we assume that it has already been proved for all subgames of α.

1. $\varsigma_{?Q}(X) = [\![Q]\!] \cap X \subseteq [\![Q]\!] \cap Y = \varsigma_{?Q}(Y)$, because $X \subseteq Y$.
2. The cases of discrete assignments and differential equations are equally simple.
3. $\varsigma_{\alpha\cup\beta}(X) = \varsigma_\alpha(X) \cup \varsigma_\beta(X) \subseteq \varsigma_\alpha(Y) \cup \varsigma_\beta(Y) = \varsigma_{\alpha\cup\beta}(Y)$, because monotonicity is already assumed to hold for the subgames α and β of $\alpha\cup\beta$ by induction hypothesis.
4. $\varsigma_\beta(X) \subseteq \varsigma_\beta(Y)$ by induction hypothesis for the subgame β, because $X \subseteq Y$. Hence, $\varsigma_{\alpha;\beta}(X) = \varsigma_\alpha(\varsigma_\beta(X)) \subseteq \varsigma_\alpha(\varsigma_\beta(Y)) = \varsigma_{\alpha;\beta}(Y)$ by induction hypothesis for the subgame α, because $\varsigma_\beta(X) \subseteq \varsigma_\beta(Y)$.
5. $\varsigma_{\alpha^*}(X) = \bigcap\{Z \subseteq \mathscr{S} : X \cup \varsigma_\alpha(Z) \subseteq Z\} \subseteq \bigcap\{Z \subseteq \mathscr{S} : Y \cup \varsigma_\alpha(Z) \subseteq Z\} = \varsigma_{\alpha^*}(Y)$ if $X \subseteq Y$.
6. $X \subseteq Y$ implies $X^\complement \supseteq Y^\complement$, hence $\varsigma_\alpha(X^\complement) \supseteq \varsigma_\alpha(Y^\complement)$, so $\varsigma_{\alpha^d}(X) = (\varsigma_\alpha(X^\complement))^\complement \subseteq (\varsigma_\alpha(Y^\complement))^\complement = \varsigma_{\alpha^d}(Y)$. ∎

While monotonicity is of independent interest, it also implies that the least fixpoint in $\varsigma_{\alpha^*}(X)$ and the greatest fixpoint in $\delta_{\alpha^*}(X)$ are even well-defined in the first place [3, Lemma 1.7].

16.2.3 Determinacy

Every particular match played in a hybrid game is won by exactly one player, because hybrid games are *zero-sum* (one player's loss is another player's win) and there are no *draws* (the outcome of a particular game play is never inconclusive because every final state is won by one of the players). This is a simple property of each individual match. All we need to do for one particular match is to wait until the players are done playing, which will happen eventually, and check the winning condition in the final state.

Hybrid games satisfy a much stronger property: *determinacy*, i.e. that, from any initial situation, either one of the players always has a winning strategy to force a win, regardless of how the other player chooses to play. Determinacy is quite a strong property indicating that for every state, there is a player who can force a win, so there is a winning strategy that will make that player win every single match in the given hybrid game from that initial state, no matter what the opponent is trying.

If, from the same initial state, both Angel and Demon had a winning strategy for opposing winning conditions, then something would be terribly inconsistent. It cannot possibly happen that Angel has a winning strategy in hybrid game α to get to a state where $\neg P$ and, from the same initial state, Demon supposedly also has a winning strategy in the same hybrid game α to get to a state where P holds. After all, a winning strategy is a strategy that makes that player win no matter what strategy the opponent follows. If both players had such winning strategies for winning conditions $\neg P$ and P, respectively, then their strategies would take the final state simultaneously to $\neg P$ and to P, which is impossible. Hence, for any initial state, at most one player can have a winning strategy for complementary winning conditions. This argues for the validity of $\models \neg([\alpha]P \wedge \langle\alpha\rangle\neg P)$, which can also be proved (Theorem 16.1).

So hybrid games are *consistent*, because it cannot happen that both players have a winning strategy for complementary winning conditions in the same state. But it might still happen that no one has a winning strategy, i.e. both players can let the other player win, but cannot win strategically themselves (recall, e.g., the filibuster example from Chap. 14, which first appeared as if no player has a winning strategy but then turned out to make Demon win, because Angel needs to stop her repetition eventually). For hybrid games at least one (in fact, exactly one) player has a winning strategy for complementary winning conditions from any initial state [10]. Determinacy is important to be able to assign classical truth-values to formulas. If it is not clear which player has a winning strategy then we cannot say whether formulas of the form $\langle\alpha\rangle P$ and $[\alpha]P$ are true.

If Angel has no winning strategy to achieve $\neg P$ in hybrid game α, then Demon has a winning strategy to achieve P in the same hybrid game α, and vice versa.

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

Proof. The proof shows by induction on the structure of α that $\varsigma_\alpha(X^{\complement})^{\complement} = \delta_\alpha(X)$ for all $X \subseteq \mathscr{S}$, which implies the validity of $\neg\langle\alpha\rangle\neg P \leftrightarrow [\alpha]P$ using $X \overset{\text{def}}{=} [\![P]\!]$. For the most part, the proof only expands Definition 15.4 and Definition 15.5 directly.

1. $\varsigma_{x:=e}(X^{\complement})^{\complement} = \{\omega \in \mathscr{S} : \omega_x^{\omega[\![e]\!]} \notin X\}^{\complement} = \varsigma_{x:=e}(X) = \delta_{x:=e}(X)$
2. $\varsigma_{x'=f(x)\&Q}(X^{\complement})^{\complement} = \{\varphi(0) \in \mathscr{S} : \varphi(r) \notin X$ for some $0 \leq r \in \mathbb{R}$ and some (differentiable) $\varphi : [0,r] \to \mathscr{S}$ such that $\frac{\mathrm{d}\varphi(t)(x)}{\mathrm{d}t}(\zeta) = \varphi(\zeta)[\![f(x)]\!]$ and $\varphi(\zeta) \in [\![Q]\!]$ for all $0 \leq \zeta \leq r\}^{\complement} = \delta_{x'=f(x)\&Q}(X)$, because the set of states from which there is no winning strategy for Angel to reach a state in $X^{\complement}$ prior to leaving $[\![Q]\!]$ along $x' = f(x)\&Q$ is exactly the set of states from which $x' = f(x)\&Q$ always stays in X (until leaving $[\![Q]\!]$ in case that ever happens).
3. $\varsigma_{?Q}(X^{\complement})^{\complement} = ([\![Q]\!] \cap X^{\complement})^{\complement} = ([\![Q]\!])^{\complement} \cup (X^{\complement})^{\complement} = \delta_{?Q}(X)$
4. $\varsigma_{\alpha\cup\beta}(X^{\complement})^{\complement} = (\varsigma_\alpha(X^{\complement}) \cup \varsigma_\beta(X^{\complement}))^{\complement} = \varsigma_\alpha(X^{\complement})^{\complement} \cap \varsigma_\beta(X^{\complement})^{\complement} = \delta_\alpha(X) \cap \delta_\beta(X) = \delta_{\alpha\cup\beta}(X)$
5. $\varsigma_{\alpha;\beta}(X^{\complement})^{\complement} = \varsigma_\alpha(\varsigma_\beta(X^{\complement}))^{\complement} = \varsigma_\alpha(\delta_\beta(X)^{\complement})^{\complement} = \delta_\alpha(\delta_\beta(X)) = \delta_{\alpha;\alpha}(X)$
6. $\varsigma_{\alpha^*}(X^{\complement})^{\complement} = \Big(\bigcap\{Z \subseteq \mathscr{S} : X^{\complement} \cup \varsigma_\alpha(Z) \subseteq Z\}\Big)^{\complement} =$
   $\Big(\bigcap\{Z \subseteq \mathscr{S} : (X \cap \varsigma_\alpha(Z)^{\complement})^{\complement} \subseteq Z\}\Big)^{\complement} = \Big(\bigcap\{Z \subseteq \mathscr{S} : (X \cap \delta_\alpha(Z^{\complement}))^{\complement} \subseteq Z\}\Big)^{\complement}$
   $= \bigcup\{Z \subseteq \mathscr{S} : Z \subseteq X \cap \delta_\alpha(Z)\} = \delta_{\alpha^*}(X)$. [1]
7. $\varsigma_{\alpha^{\mathrm{d}}}(X^{\complement})^{\complement} = (\varsigma_\alpha((X^{\complement})^{\complement})^{\complement})^{\complement} = \delta_\alpha(X^{\complement})^{\complement} = \delta_{\alpha^{\mathrm{d}}}(X)$ □

The determinacy direction of Theorem 16.1 is $\vDash \neg\langle\alpha\rangle\neg P \to [\alpha]P$, which is propositionally equivalent to $\vDash \langle\alpha\rangle\neg P \vee [\alpha]P$, implying that from all initial states, either Angel has a winning strategy to achieve $\neg P$ or Demon has a winning strategy to achieve P. The consistency direction of Theorem 16.1 is $\vDash [\alpha]P \to \neg\langle\alpha\rangle\neg P$, i.e. $\vDash \neg([\alpha]P \wedge \langle\alpha\rangle\neg P)$, which implies that there is no state from which both Demon has a winning strategy to achieve P and, simultaneously, Angel has a winning strategy to achieve $\neg P$.

[1] The penultimate equation follows from a μ-calculus [6] equivalence that the greatest fixpoint $\nu Z.\Upsilon(Z)$ of $\Upsilon(Z)$ is the same as the complement $\neg\mu Z.\neg\Upsilon(\neg Z)$ of the least fixpoint $\mu Z.\neg\Upsilon(\neg Z)$ of the dual $\neg\Upsilon(\neg Z)$. Applicability of this equation uses the insights from Chap. 15 that least pre-fixpoints are fixpoints and greatest post-fixpoints are fixpoints for monotone functions.

16.3 Dynamic Axioms for Hybrid Games

This section develops axioms for decomposing hybrid games [10], which will make it possible to reason rigorously about hybrid games. We continue the compositionality principles of logic such that each axiom describes one operator on hybrid games in terms of simpler hybrid games. The major twist compared to the dynamic axioms for dynamical systems described by hybrid programs from Chap. 5 is that the dynamic axioms now need to capture the existence of winning strategies in hybrid games.

What gives us hope to identify reasonable axioms is that the semantics of is well-behaved, because the meaning of each hybrid game is a function of the meaning of its subgames.

16.3.1 Dynamic Axioms for Determinacy

The easiest way to get started with an axiomatization for the operators of differential game logic is to internalize the insights from the semantical theorems in Sect. 16.2 as logical axioms.

Consistency and determinacy (Theorem 16.1) showed that $\models \neg\langle\alpha\rangle\neg P \leftrightarrow [\alpha]P$ is valid. That is, if Angel has no winning strategy to achieve $\neg P$ then Demon has a winning strategy to achieve P in the same hybrid game α, and vice versa. This insight helpfully related box and diamond modalities, but Theorem 16.1 is not yet available in our proofs, because it is about validity or truth, not proof.

All it takes to use Theorem 16.1 in proofs is to internalize it as an axiom.

Lemma 16.2 ([·] determinacy axiom). *The* determinacy axiom *is sound:*

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

Proof. Soundness of axiom [·], i.e. that each of its instances is valid, directly follows from Theorem 16.1. □

After we adopt [·] as an axiom and give a soundness proof for it, we can, from now on, just use the determinacy principle by referring to axiom [·]. We do not need to worry on a case-by-case basis whether it can be used in a proof, because we settled its soundness question once and for all.

Of course, Theorem 16.1 sort of says the same thing as axiom [·] does, but proofs do not come with a mechanism for applying external mathematical theorems, while they very much come with a mechanism of applying axioms.

16.3.2 Monotonicity

Transliterating Theorem 16.1 into the axiomatization of dGL was straightforward, almost copy&paste. What is the axiomatic counterpart of Theorem **??**?

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

Theorem **??** says that $\varsigma_\alpha(X) \subseteq \varsigma_\alpha(Y)$ if $X \subseteq Y$. What is the logical counterpart of $\varsigma_\alpha(X)$ and of $\varsigma_\alpha(Y)$?

Of course the logical counterpart of $\varsigma_\alpha(X)$ cannot possibly be $\langle\alpha\rangle X$, because that is not even a syntactically well-formed formula when $X \subseteq \mathscr{S}$ is a set of states. But for a logical formula P, the dGL formula $\langle\alpha\rangle P$ corresponds to $\varsigma_\alpha([\![P]\!])$, because $[\![\langle\alpha\rangle P]\!] = \varsigma_\alpha([\![P]\!])$ by Definition 15.1. Likewise, when Q is another logical formula, then $\langle\alpha\rangle Q$ corresponds to $\varsigma_\alpha([\![Q]\!])$. What does the inclusion $\varsigma_\alpha([\![P]\!]) \subseteq \varsigma_\alpha([\![Q]\!])$ correspond to?

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

Since $\varsigma_\alpha([\![P]\!]) \subseteq \varsigma_\alpha([\![Q]\!])$ is $[\![\langle\alpha\rangle P]\!] \subseteq [\![\langle\alpha\rangle Q]\!]$, this inclusion is equivalent to the validity of the dGL formula $\langle\alpha\rangle P \to \langle\alpha\rangle Q$. Now Lemma 15.1 does not imply that $\langle\alpha\rangle P \to \langle\alpha\rangle Q$ is valid. Lemma 15.1 only implies $\vDash \langle\alpha\rangle P \to \langle\alpha\rangle Q$ under the assumption that $[\![P]\!] \subseteq [\![Q]\!]$. What is a corresponding rigorous reasoning principle in the dGL proof calculus?

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

The logical internalization of the monotonicity principle from Lemma 15.1 as a proof principle is the following proof rule.

Lemma 16.3 (M monotonicity rule). *The* monotonicity rules *are sound:*

$$\text{M}\ \frac{P \to Q}{\langle\alpha\rangle P \to \langle\alpha\rangle Q} \qquad \text{M}[\cdot]\ \frac{P \to Q}{[\alpha]P \to [\alpha]Q}$$

Proof. This proof rule is sound, i.e. validity of all premises (here just one) implies validity of the conclusion, which directly follows from Lemma 15.1. If the premise $P \to Q$ is valid, then $[\![P]\!] \subseteq [\![Q]\!]$, which implies $[\![\langle\alpha\rangle P]\!] \subseteq [\![\langle\alpha\rangle Q]\!]$ by Lemma 15.1, which says that the conclusion $\langle\alpha\rangle P \to \langle\alpha\rangle Q$ is valid. ∎

This lemma is identical to Lemma 5.13 on p. 149, except that the new lemma applies to arbitrary hybrid games α, not just to hybrid programs as Lemma 5.13 did.

Of course, Lemma 15.1 cannot be internalized as the following formula:

$$(P \to Q) \to (\langle\alpha\rangle P \to \langle\alpha\rangle Q) \tag{16.1}$$

The formula (16.1) only assumes the implication $P \to Q$ to be true in the current state, while rule M assumes the implication $P \to Q$ is valid, so true in all states, including the final states that Angel is trying to achieve to win $\langle\alpha\rangle P$.

The validity from Theorem 16.1 gave rise to an axiom for dGL while the conditional validity from Lemma 15.1 leads to a proof rule with a premise for the assumption and a conclusion.

16.3.3 Dynamic Axioms for Assignments

The semantics of hybrid games is a set-valued semantics, giving the set of states from which Angel has a winning strategy to achieve set $X \subseteq \mathscr{S}$ as the winning region $\varsigma_\alpha(X) \subseteq \mathscr{S}$. But except for the style of definition, assignments $x := e$ still have the same semantics that they had in hybrid systems, because assignments have a deterministic result and involve no choices by any player. Consequently, Angel has a winning strategy in the discrete assignment game $x := e$ to achieve $p(x)$ iff $p(e)$ is true, because the assignment $x := e$ exactly has the effect of changing the value of the variable x to the value of e.

Lemma 16.4 ($\langle:=\rangle$ assignment axiom). *The* assignment axiom *is sound:*

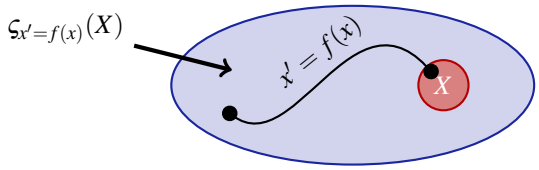
$$\langle:=\rangle \quad \langle x := e\rangle p(x) \leftrightarrow p(e)$$

16.3.4 Dynamic Axioms for Differential Equations

Unlike discrete assignments, differential equations involve a choice, namely Angel's choice of duration. Recall that the winning region semantics of differential equations from Definition 15.4 is the set of all states from which there is a solution of the differential equation to the winning condition:

$$\varsigma_{x'=f(x)}(X) = \{\varphi(0) \in \mathscr{S} : \varphi(r) \in X \text{ for some solution } \varphi : [0,r] \to \mathscr{S} \text{ of any duration } r \in \mathbb{R} \text{ satisfying } \varphi \models x' = f(x)\}$$

Let us schematically illustrate what this region looks like:



If we have a solution $y(\cdot)$ of the initial value problem $y'(t) = f(y), y(0) = x$, then Angel has a winning strategy for $\langle x' = f(x)\rangle p(x)$ iff there is a duration $t \geq 0$ such that $p(x)$ holds after assigning the solution $y(t)$ to x.

Lemma 16.5 ($\langle' \rangle$ solution axiom). *The* solution axiom schema *is sound:*

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

where $y(\cdot)$ solves the symbolic initial value problem $y'(t) = f(y), y(0) = x$.

While differential equations are games that provide a choice for Angel, they, at least, do not give any choices to the other player Demon. That is why there is only one quantifier, the existential quantifier for time, because it is up to Angel to choose her favorite time t to reach $p(x)$. The soundness proof for axiom $\langle' \rangle$ is essentially the same as the correctness argument for the solution axiom $[']$ for hybrid programs from Lemma 5.3, just based on the assumption that $y(\cdot)$ is a solution of the differential equation.

The solution axiom schema $\langle' \rangle$ inherits the same shortcomings that solution axiom schema $[']$ for hybrid systems already had. It only works for simple differential equations that Angel happens to have a solution for. More complicated differential equations need the induction techniques for differential equations from Part II, which continue to work in hybrid games.

As stated, the axiom schema $\langle' \rangle$ also does not support differential equations with evolution domain constraints. While a corresponding generalization is quite straightforward, hybrid games ultimately turn out to provide a more elegant approach for evolution domains (Sect. 16.6). For convenience, we state the evolution domain constraint version of axiom $\langle' \rangle$ regardless:

Lemma 16.6 ($\langle' \rangle$ solution with domains axiom). *This axiom is sound:*

$$\langle' \rangle \quad \langle x' = f(x)\,\&\,q(x)\rangle p(x) \leftrightarrow \exists t{\geq}0\, \big((\forall 0{\leq}s{\leq}t\; q(y(s))) \wedge \langle x := y(t)\rangle p(x)\big) \qquad (y'(t) = f(y))$$

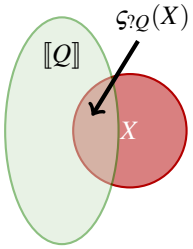
where $y(\cdot)$ solves the symbolic initial value problem $y'(t) = f(y), y(0) = x$.

16.3.5 Dynamic Axioms for Challenge Games

Test games or challenge games $?Q$ require Angel to pass the test Q or else she will lose the game prematurely for violating the rules of the game. Recall the semantics of test games from Definition 15.4:

$$\varsigma_{?Q}(X) = [\![Q]\!] \cap X \tag{16.2}$$

An illustration of the winning region in (16.2) is:



Correspondingly, if Angel wants to win $\langle ?Q\rangle P$ then she will have to be in a state where the postcondition P is already true, because tests do not change the state, and that initial state will also have to satisfy the test condition Q or else she will lose for having failed her test.

Lemma 16.7 ($\langle ?\rangle$ test axiom). *The* test axiom *is sound:*

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

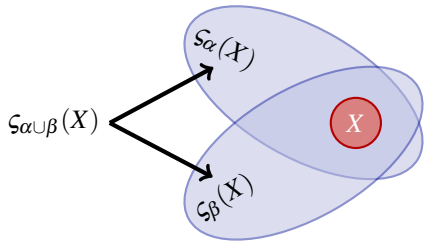
Proof. The axiom is sound iff each of its instances is valid, i.e. true in all states. The equivalence is valid iff the set of all states $[\![\langle ?Q\rangle P]\!]$ where its left-hand side is true is equal to the set of states $[\![Q \wedge P]\!]$ where its right-hand side is true. Indeed, $[\![\langle ?Q\rangle P]\!] = \varsigma_{?Q}([\![P]\!]) = [\![Q]\!] \cap [\![P]\!] = [\![Q \wedge P]\!]$. □

16.3.6 Dynamic Axioms for Choice Games

Proving the existence of winning strategies in a choice game $\alpha \cup \beta$ is more difficult, because this hybrid game involves a choice by Angel and may involve further choices by both players in the respective subgames α and β. Recall the semantics of choice games from Definition 15.4, which is a union of the semantics for the subgames:

$$\varsigma_{\alpha\cup\beta}(X) = \varsigma_\alpha(X) \cup \varsigma_\beta(X) \tag{16.3}$$

Let us illustrate what (16.3) means:



According to the winning region semantics (16.3), the states from which there is a winning strategy in the game $\alpha\cup\beta$ for Angel to achieve X is the union of the sets of states from which Angel has a winning strategy in the left subgame α to achieve X as well as the sets of states from which Angel has a winning strategy in the right subgame β to achieve X. Consequently, $\langle\alpha\cup\beta\rangle P$ is true, i.e. Angel has a winning strategy to achieve P in $\alpha\cup\beta$, iff Angel has a winning strategy to achieve P in α or in β.

Lemma 16.8 ($\langle\cup\rangle$ axiom of choice). *The* axiom of game of choice *is sound:*

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

Proof. The axiom is sound iff each of its instances is valid, i.e. true in all states. The equivalence is valid iff the set of all states $[\![\langle\alpha\cup\beta\rangle P]\!]$ where its left-hand side is true is equal to the set of states $[\![\langle\alpha\rangle P\vee\langle\beta\rangle P]\!]$ where its right-hand side is true. $[\![\langle\alpha\cup\beta\rangle P]\!] = \varsigma_{\alpha\cup\beta}([\![P]\!]) = \varsigma_\alpha([\![P]\!])\cup\varsigma_\beta([\![P]\!]) = [\![\langle\alpha\rangle P]\!]\cup[\![\langle\beta\rangle P]\!] = [\![\langle\alpha\rangle P\vee\langle\beta\rangle P]\!]$ □

Proving existence of a winning strategy for Angel in a game of choice under Angel's control merely amounts to proving the disjunction $\langle\alpha\rangle P\vee\langle\beta\rangle P$.

For Demon's choice $\alpha\cap\beta$, Angel has to invest more work to prove that she has a winning strategy for it, because her opponent Demon gets to make the choice. Consequently, Angel only has a winning strategy if she has a winning strategy for both subgames that Demon could choose:

$$\langle\alpha\cap\beta\rangle P \leftrightarrow \langle\alpha\rangle P\wedge\langle\beta\rangle P \tag{16.4}$$

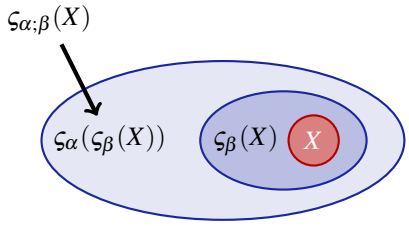
Even if this formula is valid, it will not be adopted as an axiom, because (16.4) can be derived easily from the choice axiom $\langle\cup\rangle$ together with the duality axiom $\langle^d\rangle$ that we will explore later. After all, Demon's choice $\alpha\cap\beta$ is built with a derived operator that is defined as the double dual $(\alpha^{\mathrm{d}}\cup\beta^{\mathrm{d}})^{\mathrm{d}}$ from Angel's choice.

16.3.7 Dynamic Axioms for Sequential Games

The next case to consider is a proof of existence of winning strategies in a sequential game $\alpha;\beta$. Recall the semantics of sequential games from Definition 15.4, which is a composition of the winning regions:

$$\varsigma_{\alpha;\beta}(X) = \varsigma_\alpha(\varsigma_\beta(X)) \tag{16.5}$$

An illustration of what (16.5) means is the following:



Thus, the states from which Angel has a winning strategy for $\alpha;\beta$ is the composition of the winning region for α after the winning region for β. The formula characterizing from which states Angel has a winning strategy in the game β to achieve postcondition P is the dGL formula $\langle\beta\rangle P$. Consequently, the formula characterizing from which states Angel has a winning strategy in the game α to reach $\langle\beta\rangle P$ is $\langle\alpha\rangle\langle\beta\rangle P$. By (16.5), that formula is exactly equivalent to $\langle\alpha;\beta\rangle P$ characterizing the states from which angel has a winning strategy in game $\alpha;\beta$ to achieve P.

Lemma 16.9 ($\langle;\rangle$ composition axiom). *The* composition axiom *is sound:*

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

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

16.3.8 Dynamic Axioms for Dual Games

So far, all axioms for hybrid games looked conspicuously familiar. Such a structural similarity may be somewhat surprising, because the new axioms of this chapter allow hybrid games, which have an entirely new semantics compared to the hybrid systems from Part I.

But then again, hybrid systems are special cases of hybrid games, the ones that do not need the other player, because HPs do not mention the duality operator so that control never passes to Demon. Every axiom for hybrid games also holds for hybrid systems, because hybrid systems are special cases of hybrid games. In retrospect it is, thus, not quite so surprising that the reasoning principles for hybrid games have a

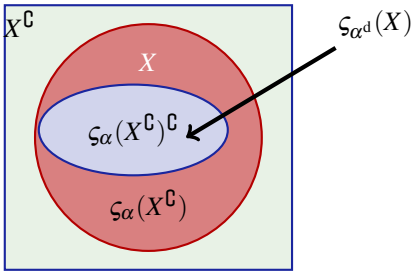
lot in common with reasoning principles for hybrid systems, even if they need new soundness proofs, because hybrid games have a more general semantics.

For the duality operator in the dual game α^d, however, we will run out of luck trying to find inspiration from generalizations of corresponding reasoning principles for hybrid systems, because the whole point is that the duality operator is the only difference between hybrid systems and hybrid games. Hybrid systems cannot yet know how to handle α^d, because α^d is a hybrid game but not a hybrid system.

Recall the semantics of dual games from Definition 15.4:

$$\varsigma_{\alpha^d}(X) = \varsigma_\alpha(X^{\complement})^{\complement} \tag{16.6}$$

An illustration of what (16.6) means is the following:



Now, how does that turn into a logical axiom? The complement $X^{\complement}$ corresponds to negation $\neg P$ of the postcondition P. Hence, the logical internalization of $\varsigma_\alpha([\![P]\!]^{\complement})$ corresponds to $\langle\alpha\rangle\neg P$ and its complement $\varsigma_\alpha([\![P]\!]^{\complement})^{\complement}$ corresponds to $\neg\langle\alpha\rangle\neg P$.

Lemma 16.10 ($\langle^d\rangle$ duality axiom). *The* duality axiom *is sound:*

$$\langle^d\rangle \quad \langle\alpha^d\rangle P \leftrightarrow \neg\langle\alpha\rangle\neg P$$

Proof. $[\![\langle\alpha^d\rangle P]\!] = \varsigma_{\alpha^d}([\![P]\!]) = \varsigma_\alpha(([\![P]\!])^{\complement})^{\complement} = \varsigma_\alpha([\![\neg P]\!])^{\complement} = ([\![\langle\alpha\rangle\neg P]\!])^{\complement} = [\![\neg\langle\alpha\rangle\neg P]\!]$ □

Example 16.1 (Demon's choice). Since Demon's choice $\alpha \cap \beta$ is $(\alpha^d \cup \beta^d)^d$, the duality axiom $\langle^d\rangle$ and the axiom for Angel's choice $\langle\cup\rangle$ can be used to derive the axiom (16.4) for Demon's choice:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{\vdash \langle\alpha\rangle P \wedge \langle\beta\rangle P \leftrightarrow \langle\alpha\rangle P \wedge \langle\beta\rangle P}}{\vdash \neg(\neg\langle\alpha\rangle\neg\neg P \vee \neg\langle\beta\rangle\neg\neg P) \leftrightarrow \langle\alpha\rangle P \wedge \langle\beta\rangle P}}{\vdash \neg(\langle\alpha^d\rangle\neg P \vee \langle\beta^d\rangle\neg P) \leftrightarrow \langle\alpha\rangle P \wedge \langle\beta\rangle P}\,\langle^d\rangle}{\vdash \neg\langle\alpha^d \cup \beta^d\rangle\neg P \leftrightarrow \langle\alpha\rangle P \wedge \langle\beta\rangle P}\,\langle\cup\rangle}{\vdash \langle(\alpha^d \cup \beta^d)^d\rangle P \leftrightarrow \langle\alpha\rangle P \wedge \langle\beta\rangle P}\,\langle^d\rangle}{\vdash \langle\alpha \cap \beta\rangle P \leftrightarrow \langle\alpha\rangle P \wedge \langle\beta\rangle P}$$

Having proved this formula once, we can, from now on, just use the corresponding derived axiom for Demon's choice instead of reproving it every time:

$$\langle\cap\rangle \quad \langle\alpha\cap\beta\rangle P \leftrightarrow \langle\alpha\rangle P \wedge \langle\beta\rangle P$$

$$[\cap] \quad [\alpha\cap\beta]P \leftrightarrow [\alpha]P \vee [\beta]P$$

The derived axiom $[\cap]$ for Demon's winning strategy in Demon's choice can be derived directly from derived axiom $\langle\cap\rangle$:

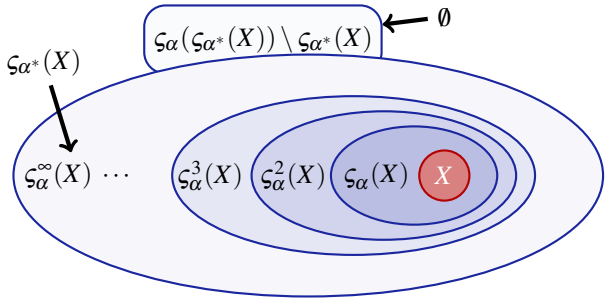
$$\dfrac{\dfrac{\dfrac{\dfrac{*}{\vdash [\alpha]P\vee[\beta]P \leftrightarrow [\alpha]P\vee[\beta]P}}{\vdash \neg\langle\alpha\rangle\neg P\vee\neg\langle\beta\rangle\neg P \leftrightarrow [\alpha]P\vee[\beta]P}[\cdot]}{\vdash \neg(\langle\alpha\rangle\neg P\wedge\langle\beta\rangle\neg P) \leftrightarrow [\alpha]P\vee[\beta]P}\langle\cap\rangle}{\vdash \neg\langle\alpha\cap\beta\rangle\neg P \leftrightarrow [\alpha]P\vee[\beta]P}[\cdot]$$

16.3.9 Dynamic Axioms for Repetition Games

The remaining challenge are axioms for repetition games α^*. Repetitions in hybrid games turned out to be semantically significantly more subtle than repetitions in hybrid systems (Chap. 15). Recall the semantics of repetition games from Definition 15.4, where we finally settled on defining it as a least fixpoint of the winning regions of α, because iteration went quite transfinite:

$$\varsigma_{\alpha^*}(X) = \bigcap\{Z\subseteq\mathscr{S} : X\cup\varsigma_\alpha(Z)\subseteq Z\} = \bigcap\{Z\subseteq\mathscr{S} : X\cup\varsigma_\alpha(Z)=Z\} \quad (16.7)$$

The second equation uses that the least pre-fixpoint was also a least fixpoint (Note 75 on p. 433). This semantics (16.7) is best illustrated as follows:



By the second equation of (16.7), $\varsigma_{\alpha^*}(X)$ is a fixpoint of $X\cup\varsigma_\alpha(Z)=Z$, so:

$$\varsigma_{\alpha^*}(X) = X\cup\varsigma_\alpha(\varsigma_{\alpha^*}(X)) \quad (16.8)$$

How can (16.8) be internalized as a syntactic reasoning principle in logic?

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

As usual, the set of states $X \subseteq \mathscr{S}$ does not fit into a logical formula, but its logical counterpart is a logical formula P, whose semantics $[\![P]\!]$ will be some set of states. Consequently, the left side of (16.8) corresponds to the logical formula $\langle\alpha^*\rangle P$ expressing that Angel has a winning strategy in the repeated hybrid game α^* to achieve P. What does the right side of (16.8) correspond to?

Since the set X is internalized by the logical formula P, $\varsigma_{\alpha^*}(X)$ corresponds to the logical formula $\langle\alpha^*\rangle P$, because $[\![\langle\alpha^*\rangle P]\!] = \varsigma_{\alpha^*}([\![P]\!])$. Consequently, $X \cup \varsigma_\alpha(\varsigma_{\alpha^*}(X))$ corresponds to the logical formula $P \vee \langle\alpha^*\rangle P$. This leads to the following axiom.

Lemma 16.11 ($\langle^*\rangle$ iteration axiom). *The* iteration axiom *is sound:*

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

Proof. The proof is a direct consequence of the fact that the winning region of repetition is a fixpoint (Note 75). Since $[\![\langle\alpha^*\rangle P]\!] = \varsigma_{\alpha^*}([\![P]\!])$ is a fixpoint, we have $[\![\langle\alpha^*\rangle P]\!] = [\![P]\!] \cup \varsigma_\alpha([\![\langle\alpha^*\rangle P]\!])$. Thus, $[\![P \vee \langle\alpha\rangle\langle\alpha^*\rangle P]\!] = [\![P]\!] \cup [\![\langle\alpha\rangle\langle\alpha^*\rangle P]\!] = [\![P]\!] \cup \varsigma_\alpha([\![\langle\alpha^*\rangle P]\!]) = [\![\langle\alpha^*\rangle P]\!]$. ∎

This axiom $\langle^*\rangle$ is identical to the iteration axiom for hybrid systems (which is the diamond version of Lemma 5.7), except that its soundness justification is completely different. But, once proved sound, the reasoning with axiom $\langle^*\rangle$ works in the same way. Does the axiom $\langle^*\rangle$ say all there is to say about repetition in hybrid games?

Before pursuing this question, first observe that the iteration axiom $\langle^*\rangle$ for Angel's winning strategy in Angel's repetition implies a corresponding iteration axiom for Demon's winning strategy in Demon's repetition.

Example 16.2 (Demon's repetition). Since Demon's repetition $\alpha^\times$ is $((\alpha^d)^*)^d$, the duality axiom $\langle^d\rangle$ and determinacy axiom $[\cdot]$ turn Angel's iteration axiom $\langle^*\rangle$ into a corresponding iteration axiom for Demon's winning strategy

$$[^\times] \quad [\alpha^\times]P \leftrightarrow P \vee [\alpha][\alpha^\times]P$$

This derived axiom $[^\times]$ can be proved easily:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{\vdash P \vee [\alpha][\alpha^\times]P \leftrightarrow P \vee [\alpha][\alpha^\times]P}}{\vdash P \vee [\alpha][((\alpha^d)^*)^d]P \leftrightarrow P \vee [\alpha][\alpha^\times]P}}{\vdash P \vee \langle\alpha^d\rangle\langle(\alpha^d)^*\rangle P \leftrightarrow P \vee [\alpha][\alpha^\times]P}\,\langle^d\rangle,[\cdot]}{\vdash \langle(\alpha^d)^*\rangle P \leftrightarrow P \vee [\alpha][\alpha^\times]P}\,\langle^*\rangle}{\vdash [((\alpha^d)^*)^d]P \leftrightarrow P \vee [\alpha][\alpha^\times]P}\,\langle^d\rangle,[\cdot]}{\vdash [\alpha^\times]P \leftrightarrow P \vee [\alpha][\alpha^\times]P}$$

16.3.10 Proof Rules for Repetition Games

The iteration axiom $[^*]$ was established to be sound in Sect. 5.3.7, but Chap. 7 identified a significantly more useful approach of proving properties of loops by induction. Similarly, one might wonder whether the iteration axiom $\langle^*\rangle$ really already captures all there is to say about repetition in hybrid games.

Taking a step back, axiom $\langle^*\rangle$ expresses that $\langle\alpha^*\rangle P$ is a fixpoint of (16.8), which follows from (16.7), but does not convey that, among all the possible fixpoints, $\langle\alpha^*\rangle P$ is the least fixpoint. How could this be rendered in a logical proof principle?

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

Since $\langle\alpha^*\rangle P$ is the least fixpoint, the set of all states in which it is true is smaller than any other fixpoint. The logical internalization is that if Q is a logical formula whose semantics also satisfies the fixpoint condition from (16.7), then the set of states where $\langle\alpha^*\rangle P$ is true is smaller, that is $[\![\langle\alpha^*\rangle P]\!] \subseteq [\![Q]\!]$, which means that $\langle\alpha^*\rangle P \to Q$ is valid. Since it is, here, a little more convenient to work with the pre-fixpoint condition from (16.7), saying that the logical formula Q is a pre-fixpoint amounts to assuming that $P \vee \langle\alpha\rangle Q \to Q$ is valid.

Lemma 16.12 (FP fixpoint rule). *The* fixpoint rule *is sound:*

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

Proof. The proof is a direct consequence of the fact that the winning region of repetition is the least fixpoint (Note 75). Assume the premise $P \vee \langle\alpha\rangle Q \to Q$ is valid, i.e. $[\![P \vee \langle\alpha\rangle Q]\!] \subseteq [\![Q]\!]$. That is, $[\![P]\!] \cup \varsigma_\alpha([\![Q]\!]) = [\![P]\!] \cup [\![\langle\alpha\rangle Q]\!] = [\![P \vee \langle\alpha\rangle Q]\!] \subseteq [\![Q]\!]$. Thus, Q is a pre-fixpoint of $Z = [\![P]\!] \cup \varsigma_\alpha(Z)$. By monotonicity (Lemma 15.1), $[\![\langle\alpha^*\rangle P]\!] = \varsigma_{\alpha^*}([\![P]\!])$ is the least fixpoint [7, Appendix A]. Hence, $[\![\langle\alpha^*\rangle P]\!] \subseteq [\![Q]\!]$, which implies that $\langle\alpha^*\rangle P \to Q$ is valid. ∎

Together with the iteration axiom $\langle^*\rangle$, the fixpoint proof rule FP is in most direct correspondence with the semantics of repetition in hybrid games, which is defined as a least fixpoint. The iteration axiom $\langle^*\rangle$ expresses that $\langle\alpha^*\rangle P$ is a fixpoint while rule FP expresses that it is the least fixpoint.

Admittedly, though, the fixpoint rule FP can be a bit unwieldy to use. Fortunately, the old familiar loop invariant rule, generalized to hybrid games, can be derived from the fixpoint rule FP and even vice versa [10, Lemma 4.1].

Corollary 16.1 (ind loop invariant rule). *The* loop invariant *proof rule is sound:*

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

Proof. The proof uses contraposition, i.e. that $A \to B$ is equivalent to $\neg B \to \neg A$ in classical logic or similarly simple propositional rewriting at the steps that are not marked.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdash P \to [\alpha]P}{\vdash P \to P \wedge [\alpha]P}}{\vdash P \to P \wedge \neg\langle\alpha\rangle\neg P}[\cdot]}{\vdash \neg P \vee \langle\alpha\rangle\neg P \to \neg P}}{\vdash \langle\alpha^*\rangle\neg P \to \neg P}\text{FP}}{\vdash P \to \neg\langle\alpha^*\rangle\neg P}}{\vdash P \to [\alpha^*]P}[\cdot]$$

This proof shows that rule ind is a derived rule, since its conclusion can be proved from rule FP using the other axioms and propositional reasoning. □

Example 16.3 (Invariants and fixpoints for Demon's repetition). Since Demon's repetition $\alpha^\times$ is $((\alpha^{\mathrm{d}})^*)^{\mathrm{d}}$, the duality axiom $\langle^d\rangle$ and determinacy axiom $[\cdot]$ turn Demon's invariant rule ind for Angel's repetition into a corresponding invariant rule for Angel's winning strategy in Demon's repetition:

$$\dfrac{P \to \langle\alpha\rangle P}{P \to \langle\alpha^\times\rangle P}\,{}^\times\text{ind}$$

Likewise, Demon's counterpart for Demon's repetition of the fixpoint rule FP derives by duality axiom $\langle^d\rangle$ and determinacy axiom $[\cdot]$:

$$\dfrac{P \vee [\alpha]Q \to Q}{[\alpha^\times]P \to Q}\,{}^\times\text{FP}$$

The proofs of correctness for rules ${}^\times$ind and ${}^\times$FP are explored in Exercise 16.5.

16.4 Example Proofs

This section shows how the dGL axioms can be used to prove the existence of winning strategies for some hybrid games.

Example 16.4 (Push-around cart). Recall the following dGL formula about the push-around cart game from Example 14.3:

$$x{\geq}0 \wedge v{\geq}0 \to \big[\big((d:=1 \cup d:=-1)^{\mathrm{d}}; (a:=1 \cup a:=-1); \{x'=v, v'=a+d\}\big)^*\big]\, x \geq 0$$

Using Demon's choice and the fact that the duals of assignments are the assignments themselves, recall that this dGL formula is equivalent to:

$$x{\geq}0 \wedge v{\geq}0 \to \big[\big((d:=1 \cap d:=-1); (a:=1 \cup a:=-1); \{x'=v, v'=a+d\}\big)^*\big]\, x \geq 0$$

$$\dfrac{J \vdash [\{x'=v,v'=1+1\}]J \wedge [\{x'=v,v'=-1+1\}]J}{J \vdash [a:=1][\{x'=v,v'=a+1\}]J \wedge [a:=-1][\{x'=v,v'=a+1\}]J}\,[:=]$$
$$\dfrac{J \vdash [a:=1 \cup a:=-1][\{x'=v,v'=a+1\}]J}{J \vdash [a:=1 \cup a:=-1][\{x'=v,v'=a+1\}]J}\,[\cup]$$
$$\dfrac{J \vdash [(a:=1 \cup a:=-1);\{x'=v,v'=a+1\}]J}{J \vdash [(a:=1 \cup a:=-1);\{x'=v,v'=a+1\}]J}\,[;]$$
$$\dfrac{J \vdash [d:=1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}{J \vdash [d:=1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}\,[:=]$$
$$\dfrac{J \vdash [d:=1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J \vee [d:=-1]\ldots}{J \vdash [d:=1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}\,\vee\text{R,WR}$$
$$\dfrac{J \vdash [d:=1 \cap d:=-1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}{J \vdash [d:=1][(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}\,[\cap]$$
$$\dfrac{J \vdash [(d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}{J \vdash [(d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}]J}\,[;]$$
$$\dfrac{}{J \vdash [\big((d:=1 \cap d:=-1);(a:=1 \cup a:=-1);\{x'=v,v'=a+d\}\big)^*]x \geq 0}\,\text{ind}$$

Choosing the loop invariant $J \overset{\text{def}}{\equiv} x \geq 0 \wedge v \geq 0$ will complete this proof, because both remaining differential equation properties can be proved by solving them.

$$[']\text{,}[:=]\dfrac{x \geq 0 \wedge v \geq 0 \vdash \forall t \geq 0\,(x+vt+t^2 \geq 0 \wedge v+2t \geq 0)}{J \vdash [\{x'=v,v'=1+1\}]J}$$

$$[']\text{,}[:=]\dfrac{x \geq 0 \wedge v \geq 0 \vdash \forall t \geq 0\,(x+vt \geq 0 \wedge v \geq 0)}{J \vdash [\{x'=v,v'=0\}]J}$$

They can also both be proved directly by differential invariants from Part II.

Example 16.5. The dual filibuster game formula from Chap. 14 proves easily in the dGL calculus by going back and forth between players [10] using the abbreviations $\cap,^\times$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{x=0 \vdash 0=0 \vee 1=0}\,\mathbb{R}}{x=0 \vdash \langle x:=0\rangle x=0 \vee \langle x:=1\rangle x=0}\,\langle:=\rangle}{x=0 \vdash \langle x:=0 \cup x:=1\rangle x=0}\,\langle\cup\rangle}{x=0 \vdash \neg\langle (x:=0 \cup x:=1)^{\mathrm{d}}\rangle \neg x=0}\,\langle^d\rangle}{x=0 \vdash \neg\langle x:=0 \cap x:=1\rangle \neg x=0}}{x=0 \vdash [x:=0 \cap x:=1]x=0}\,[\cdot]}{x=0 \vdash [(x:=0 \cap x:=1)^*]x=0}\,\text{ind}}{x=0 \vdash \neg\langle (x:=0 \cap x:=1)^*\rangle \neg x=0}\,[\cdot]}{x=0 \vdash \langle (x:=0 \cap x:=1)^{*\mathrm{d}}\rangle x=0}\,\langle^d\rangle}{x=0 \vdash \langle (x:=0 \cup x:=1)^\times\rangle x=0}$$

16.5 Axiomatization

The axiomatization for differential game logic [10] that we just developed gradually is summarized in Fig. 16.1.

The determinacy axiom $[\cdot]$ describes the duality of winning strategies for complementary winning conditions of Angel and Demon, i.e. that Demon has a winning

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

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

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

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

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

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

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

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

$$\mathrm{M}\ \frac{P\to Q}{\langle\alpha\rangle P\to\langle\alpha\rangle Q} \qquad \mathrm{FP}\ \frac{P\vee\langle\alpha\rangle Q\to Q}{\langle\alpha^*\rangle P\to Q} \qquad \mathrm{ind}\ \frac{P\to[\alpha]P}{P\to[\alpha^*]P}$$

Fig. 16.1 Differential game logic axiomatization

strategy to achieve P in hybrid game α if and only if Angel does not have a counter strategy, i.e. winning strategy to achieve $\neg P$ in the same game α. The determinacy axiom $[\cdot]$ internalizes Theorem 16.1. Axiom $\langle:=\rangle$ is the assignment axiom. In the differential equation axiom $\langle'\rangle$, $y(\cdot)$ is the unique [11, Theorem 10.VI] solution of the symbolic initial value problem $y'(t)=f(y), y(0)=x$. The duration t how long to follow solution y is for Angel to decide, hence existentially quantified. It goes without saying that variables like t are fresh in Fig. 16.1.

Axioms $\langle?\rangle$, $\langle\cup\rangle$, and $\langle;\rangle$ are as in differential dynamic logic [9] except that their meaning is quite different, because they refer to winning strategies of hybrid games instead of reachability relations of systems. The challenge axiom $\langle?\rangle$ expresses that Angel has a winning strategy to achieve P in the test game $?Q$ exactly from those positions that are already in P (because $?Q$ does not change the state) and that satisfy Q for otherwise she would fail the test and lose the game immediately. The axiom of choice $\langle\cup\rangle$ expresses that Angel has a winning strategy in a game of choice $\alpha\cup\alpha$ to achieve P iff she has a winning strategy in either hybrid game α or in α, because she can choose which one to play. The sequential game axiom $\langle;\rangle$ expresses that Angel has a winning strategy in a sequential game $\alpha;\alpha$ to achieve P iff she has a winning strategy in game α to achieve $\langle\alpha\rangle P$, i.e. to get to a position from which she has a winning strategy in game α to achieve P. The iteration axiom $\langle^*\rangle$ characterizes $\langle\alpha^*\rangle P$ as a pre-fixpoint. It expresses that, if the game is already in a state satisfying P or if Angel has a winning strategy for game α to achieve $\langle\alpha^*\rangle P$, i.e. to get to a position from which she has a winning strategy for game α^* to achieve P, then,

either way, Angel has a winning strategy to achieve P in game α^*. The converse of $\langle^*\rangle$ can be derived[2] and is also denoted by $\langle^*\rangle$. The dual axiom $\langle^d\rangle$ characterizes dual games. It says that Angel has a winning strategy to achieve P in dual game α^d iff Angel does not have a winning strategy to achieve $\neg P$ in game α. Combining dual game axiom $\langle^d\rangle$ with the determinacy axiom $[\cdot]$ yields $\langle\alpha^d\rangle P \leftrightarrow [\alpha]P$, i.e. that Angel has a winning strategy to achieve P in α^d iff Demon has a winning strategy to achieve P in α. Similar reasoning derives $[\alpha^d]P \leftrightarrow \langle\alpha\rangle P$.

Monotonicity rule M is the generalization rule of monotonic modal logic **C** [2] and internalizes Lemma 15.1. It expresses that, if the implication $P \rightarrow Q$ is valid, then, from wherever Angel has a winning strategy in a hybrid game α to achieve P, she also has a winning strategy to achieve Q, because Q holds wherever P does. So rule M expresses that easier objectives are easier to win. Fixpoint rule FP characterizes $\langle\alpha^*\rangle P$ as a *least* pre-fixpoint. It says that, if Q is another formula that is a pre-fixpoint, i.e. that holds in all states that satisfy P or from which Angel has a winning strategy in game α to achieve that condition Q, then Q also holds whereever $\langle\alpha^*\rangle P$ does, i.e. in all states from which Angel has a winning strategy in game α^* to achieve P.

The proof rules FP and the induction rule ind are equivalent in the sense that one can be derived from the other in the dGL calculus [10]. How the loop induction rule ind derives from the fixpoint rule FP was shown in Corollary 16.1.

16.6 There and Back Again Game

Quite unlike in hybrid systems and (poor test[3]) differential dynamic logic [8, 9], every hybrid game containing a differential equation $x' = f(x)\,\&\,Q$ with evolution domain constraints Q can be replaced equivalently by a hybrid game without evolution domain constrains. Evolution domains are definable in hybrid games [10] and can, thus, be removed equivalently.

Lemma 16.13 (Evolution domain reduction). *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 $x' = f(x)$.*

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

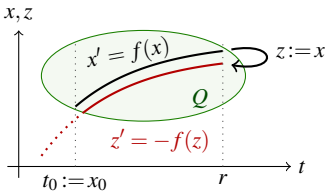
---

[2] $P \vee \langle\alpha\rangle\langle\alpha^*\rangle P \rightarrow \langle\alpha^*\rangle P$ derives by $\langle^*\rangle$. Thus, $\langle\alpha\rangle(P \vee \langle\alpha\rangle\langle\alpha^*\rangle P) \rightarrow \langle\alpha\rangle\langle\alpha^*\rangle P$ by M. Hence, $P \vee \langle\alpha\rangle(P \vee \langle\alpha\rangle\langle\alpha^*\rangle P) \rightarrow P \vee \langle\alpha\rangle\langle\alpha^*\rangle P$ by propositional congruence. Consequently, $\langle\alpha^*\rangle P \rightarrow P \vee \langle\alpha\rangle\langle\alpha^*\rangle P$ by FP.

[3] *Poor test* means that each test $?Q$ uses only first-order formulas Q. If modalities are used within Q, then $?Q$ is a *rich test*.

$$t_0 := x_0; x' = f(x); (z := x; z' = -f(z))^{\mathrm{d}}; ?(z_0 \geq t_0 \to Q(z)) \tag{16.9}$$

See Fig. 16.2 for an illustration. Suppose the current player is Angel. The idea be-



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

Fig. 16.2 "There and back again game": Angel evolves x forwards in time along $x' = f(x)$, Demon checks evolution domain backwards in time along $z' = -f(z)$ on a copy z of the state vector x

hind (16.9) is that the fresh variable t_0 remembers the initial time x_0, and Angel then evolves forward along $x' = f(x)$ 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 $(z' = -f(z))^{\mathrm{d}}$ for any amount of time (Demon's choice). The original player Angel must then pass the challenge $?(z_0 \geq t_0 \to Q(z))$, i.e. Angel loses immediately if Demon was able to evolve backwards and leave region $Q(z)$ while satisfying $z_0 \geq t_0$, which checks that Demon did not evolve backward for longer than Angel evolved forward, i.e. to before the initial time. 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 originally (by selecting a duration for the evolution that Demon could not invalidate). □

From now on, Lemma 16.13 can eliminate all evolution domain constraints equivalently in hybrid games. While evolution domain constraints are fundamental parts of standard hybrid systems [1, 4, 5, 8], 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. In theory, we never ever have to worry about evolution domains any more, because they are just part of the other operators for hybrid games. In practice, it still helps to handle evolution domain constraints directly, because axioms like DW for differential weakening and DI for differential invariants are conceptually easier than the reduction in (16.9).

16.7 Summary

This chapter developed an axiomatization for differential game logic [10]. The resulting axioms, summarized in Fig. 16.1 on p. 459 coincide with corresponding axioms for hybrid systems. But they needed entirely new soundness justification, because, due to the interactive game play features caused by the presence of the duality operator, the semantics of hybrid games is significantly more general than that

of hybrid systems. The simple syntactic reasoning principles of differential game logic are substantially more succinct than the corresponding subtleties with purely semantical arguments. Just contrast the simplicity of the axiomatization with the enormous (more than infinite) number of iterations needed in semantical arguments of winning regions for repetition from Chap. 15.

Exercises

16.1. Carefully identify how determinacy relates to the two possible understandings of the filibuster example discussed in an earlier chapter.

16.2. Prove the elided cases of Lemma 15.1.

16.3. Find the appropriate soundness notion for the axioms of dGL and prove that the axioms are sound.

16.4. Write down a valid formula that characterizes an interesting game between two robots.

16.5 (Demon's repetition). Use the duality axiom $\langle^d\rangle$ and determinacy axiom $[\cdot]$ to show that the following proof rules for Demon's repetition are derived rules:

$$^{\times}\text{ind}\ \frac{P \to \langle\alpha\rangle P}{P \to \langle\alpha^{\times}\rangle P} \qquad ^{\times}\text{FP}\ \frac{P \vee [\alpha]Q \to Q}{[\alpha^{\times}]P \to Q}$$

References

1. Alur, R., Courcoubetis, C., Henzinger, T. A. & Ho, P.-H. *Hybrid Automata: An Algorithmic Approach to the Specification and Verification of Hybrid Systems.* in *Hybrid Systems* (eds Grossman, R. L., Nerode, A., Ravn, A. P. & Rischel, H.) **736** (Springer, 1992), 209–229.
2. Chellas, B. F. *Modal Logic: An Introduction* (Cambridge Univ. Press, 1980).
3. Harel, D., Kozen, D. & Tiuryn, J. *Dynamic Logic* (MIT Press, 2000).
4. Henzinger, T. A. *The Theory of Hybrid Automata.* in *LICS* (IEEE Computer Society, Los Alamitos, 1996), 278–292. doi:10.1109/LICS.1996.561342.
5. Henzinger, T. A., Kopke, P. W., Puri, A. & Varaiya, P. *What's decidable about hybrid automata?* in *STOC* (eds Leighton, F. T. & Borodin, A.) (ACM, 1995), 373–382. doi:10.1145/225058.225162.
6. Kozen, D. Results on the Propositional μ-Calculus. *Theor. Comput. Sci.* **27,** 333–354 (1983).
7. Kozen, D. *Theory of Computation* (Springer, 2006).

8. Platzer, A. Differential Dynamic Logic for Hybrid Systems. *J. Autom. Reas.* **41,** 143–189 (2008).
9. Platzer, A. *The Complete Proof Theory of Hybrid Systems* in *LICS* (IEEE, 2012), 541–550. doi:10.1109/LICS.2012.64.
10. Platzer, A. Differential Game Logic. *ACM Trans. Comput. Log.* **17,** 1:1–1:51 (2015).
11. Walter, W. *Ordinary Differential Equations* (Springer, 1998).