André Platzer

# Lecture Notes on Foundations of Cyber-Physical Systems

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

# Chapter 6
# Truth & Proof

**Synposis** This chapter augments the dynamic axioms for dynamical systems from the previous chapter with the full mathematical rigor of a proof system. This proof system enables rigorous, systematic proofs for cyber-physical systems by providing systematic structuring mechanisms for their correctness arguments. The most important goals of such a proof system are that it guarantees to cover all cases of a correctness argument, so all possible behavior of a CPS, and that it provides guidance on what proof rules to apply. A high-level interface of proofs with reasoning for real arithmetic as well as techniques for logically simplifying real arithmetic questions are discussed as well.

## 6.1 Introduction[1]

Chap. 5 investigated dynamic axioms for dynamical systems, i.e. axioms in differential dynamic logic (dL) that characterize dynamical systems operators in terms of structurally simpler dL formulas. All it takes to understand the bigger system, thus, is to apply the appropriate axiom and investigate the smaller remainders. That chapter did not quite show all important axioms yet, but it still revealed enough to prove a property of a bouncing ball. While that chapter showed exactly how all the respective local properties about the system dynamics could be proved by invoking the corresponding dynamic axiom, it has not become clear yet how these individual inferences are best tied together to obtain a well-structured proof. That is what this chapter will identify.

After all, there's more to proofs than just axioms. Proofs also have proof rules for combining fragments of arguments into a bigger proof by well-structured proof

[1] By both sheer coincidence and by higher reason, the title of this chapter turns out to be closely related to the subtitle of a well-known book on mathematical logic [1], which summarizes the philosophy pursued here in a way that is impossible to improve upon any further: *To truth through proof*.

steps. Proofs, thus, are defined by the glue that holds axioms together into a single cohesive argument justifying its conclusion.

Granted, the working principle we followed with the axioms in Chap. 5 was quite intuitive. We repeatedly identified a subformula that we can simplify equivalently by applying any of the dL equivalence axioms from left to right. Since all dL axioms reduce more complex formulas on the left to structurally simpler formulas on the right, successively using them also simplified the conjecture correspondingly. That is quite systematic for such a simple mechanism.

Recall that our proof about the (single-hop) bouncing ball from the previous chapter still suffered from at least two issues, though. While it was a sound proof and an interesting proof, the way we had come up with it was somewhat undisciplined. We just applied axioms seemingly at random at all kinds of places all over the logical formula. After we see such a proof, that is not a concern, because we can just follow its justifications and appreciate the simplicity and elegance of the steps it took to justify the conclusion.[2] But better structuring would certainly help us find proofs more constructively in the first place. The second issue was that the axioms for the dynamics that Chap. 5 showed us did not actually help in proving the propositional logic and arithmetic parts remaining in the end. So we were left with informal justifications of the resulting arithmetic, which leaves plenty of room for subtle mistakes in correctness arguments.

The present chapter addresses both issues by imposing more structure on proofs and, as part of that, handle the operators of first-order logic that differential dynamic logic inherits (propositional *connectives* such as $\wedge, \vee, \neg, \rightarrow$) and quantifiers ($\forall, \exists$). As part of the structuring, we will make ample and crucial use of the dynamic axioms from Chap. 5. Yet, they will be used in a more structured way than so far. In a way that focuses their use on the top level of the formula and in the direction that actually simplifies the formulas.

While Chap. 5 laid down the most fundamental cornerstones of the Foundations of Cyber-Physical Systems and their rigorous reasoning principles, the present chapter revisits these fundamental principles and shapes them into a systematic proof approach. The chapter is loosely based on previous work [15, Chapter 2.5.2]. The most important learning goals of this chapter are:

**Modeling and Control:** This chapter deepens our understanding from the previous chapter on how discrete and continuous systems relate to one another in the presence of evolution domain constraints, a topic that the previous chapter only touched upon briefly. It also makes precise how proofs can soundly reason when only assuming evolution domains to hold in the end compared to the fact that evolution domains have to hold always throughout a continuous evolution.

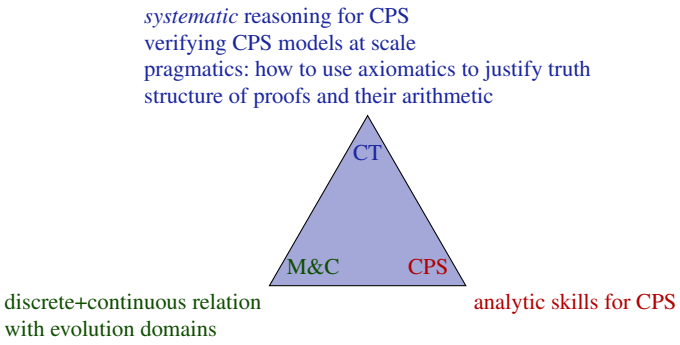
**Computational Thinking:** Based on the core rigorous reasoning principles for CPS developed in Chap. 5, this chapter is devoted to reasoning not only rigorously but also *systematically* about CPS models. Systematic ways of reasoning

[2] Indeed, the proof in Chap. 5 was creative in that it used axioms quite carefully in an order that minimizes the notational complexity. But it is not easy to come up with such (nonsystematic) shortcut proofs even if the KeYmaera X prover makes this rather easy with its proof-by-pointing feature [8].

rigorously about CPS are, of course, critical to getting more complex CPS right. The difference between the axiomatic way of reasoning rigorously about CPS [16] as put forth in Chap. 5 and the systematic way [14, 15] developed here is not a big difference conceptually, but more a difference in pragmatics.

That does not make it less important, though, and the occasion to revisit gives us a way of deepening our understanding of systematic CPS analysis principles. This chapter explains ways of developing CPS proofs systematically and is an important ingredient for verifying CPS models of appropriate scale. The chapter also adds a fourth leg to the logical trinity of syntax, semantics, and axiomatics considered in Chap. 5. It adds pragmatics, by which we mean the question of how to use axiomatics to justify the syntactic renditions of the semantical concepts of interest. That is, how to best go about conducting a proof to justify truth of a CPS conjecture. An understanding of such pragmatics follows from a more precise understanding of what a proof is and what arithmetic does.

**CPS Skills:** This chapter is mostly devoted to sharpening our analytic skills for CPS. We will also develop a slightly better intuition for the operational effects involved in CPS in that we understand in which order we should worry about operational effects and whether that has an impact on the overall understanding.




## 6.2 Truth and Proof

Truth is defined by the semantics of logical formulas. The semantics gives a mathematical meaning to formulas that, in theory, could be used to establish the truth of a logical formula by expanding all semantic definitions. In practice, this is quite infeasible, for one thing, because quantifiers of differential dynamic logic quantify over real numbers (after all their variables may represent real quantities like velocities and positions). Yet, there are (uncountably) infinitely many of those, so determining the truth value of a universally quantified logical formula directly by working with

its semantics is challenging since that'd require instantiating it with infinitely many real numbers, which would keep us busy for quite a while.

The semantics is even more challenging to deal with in the case of the hybrid systems in the modalities of differential dynamic logic formulas, because hybrid systems have so many possible behaviors and are highly nondeterministic. Literally following all possible behaviors to check all reachable states hardly sounds like a way that would ever enable us to stop and conclude the system would be safe. Except, of course, if we happen to be lucky and found a bug during just one execution, because that would be enough to falsify the formula. In fact, even following just one particular execution of a hybrid system can be tricky, because that still involves the need to compute a solution of its differential equations and check their evolution domain constraints at all times.

Yet, we are still interested in establishing whether a logical formula is true, no matter how complicated that may be, because we would very much like to know whether the hybrid systems they refer to can be used safely. Or, come to think of it, we are interested in finding out whether the formula is valid, since truth of a logical formula depends on the state (cf. definition of semantics $\omega \in [\![P]\!]$ in Definition 4.2) whereas validity of a logical formula is independent of the state (cf. definition of validity $\models P$), because validity means truth in all states. Validity of formulas is what we ultimately care about, because we want our safety analysis to hold in all permitted initial states of the CPS, not just one particular initial state $\omega$ because we may not even know the exact initial state of a CPS. In that sense, valid logical formulas are the most valuable ones. We should devote all of our efforts to finding out what is valid, because that will allow us to draw conclusions about all states, including the real world state as well.

While exhaustive enumeration and simulation is hardly an option for systems as challenging as CPS, the validity of logical formulas can be established by other means, namely by producing a proof of that formula. Like the formula itself, but unlike its semantics, a proof is a syntactical object that is amenable, e.g., to representation and manipulation in a computer. The finite syntactical argument represented in a proof witnesses the validity of the logical formula that it concludes. Proofs can be produced in a machine. They can be stored to be recalled as evidence for the validity of their conclusion. And they can be checked by humans or machines for correctness. Proofs can even be inspected for analytic insights about the reasons for the validity of a formula, which goes beyond the mere factual statement of validity. A proof justifies the judgment that a logical formula is valid, which, without such a proof as evidence, is no more than an empty claim. Empty claims would hardly be useful foundations for building any cyber-physical systems on.

Truth and proof should be related intimately, however, because we would only want to accept proofs that actually imply truth, i.e. proofs that imply their consequences to be valid if their premises are. That is, proof systems should be *sound* in order to allow us to draw reliable conclusions from the existence of a proof. This textbook will exercise great care to identify sound reasoning principles. The converse and equally intriguing question is that of *completeness*, i.e. whether all valid

formulas can be proved, which turns out to be much more subtle [14, 17–19] and won't concern us until much later in this textbook.

### 6.2.1 Sequents

The proof built from axioms in Sect. 5.4 to justify a safety property of a bouncing ball was creative and insightful, but also somewhat spontaneous or maybe even disorganized. In fact, it has not even quite become particularly obvious what exactly a proof was, except that it is somehow supposed to glue axioms together into a single cohesive argument. But that is not a definition of a proof.[3]

In order to have a chance to conduct more complex proofs, we need a way of structuring the proofs and keeping track of all questions that come up while working on a proof as well as all assumptions that are available. But despite all the lamenting about the proof in Sect. 5.4, it has, secretly, been much more systematic than we were aware of at the time. Even if it went in a non-systematic order as far as the application order of the axioms was concerned, we still structured the proof quite well (unlike the ad-hoc arguments in Sect. 4.8). So part of what this chapter needs to establish is to turn this lucky coincidence of a proper proof structure into an intentional principle. Rather than just coincidentally structuring the proof well, we want to structure all proofs well and make them all systematic by design.

Throughout this textbook, we will use *sequents*, which give us a structuring mechanism for conjectures and proofs. Sequent calculus was originally developed by Gerhard Gentzen [9, 10] for studying properties of natural deduction calculi, but sequent calculi have had tremendous successfor numerous other purposes since.

In a nutshell, sequents are a standard form for logical formulas that is convenient for proving purposes, because it neatly aligns all available assumptions on the left of the sequent turnstile $\vdash$ and gathers what needs to be shown on the right.

**Definition 6.1 (Sequent).** A *sequent* is of the form

$$\Gamma \vdash \Delta$$

where the *antecedent* $\Gamma$ and *succedent* $\Delta$ are finite sets of dL formulas. The semantics of $\Gamma \vdash \Delta$ is that of the dL formula $\bigwedge_{P\in\Gamma} P \rightarrow \bigvee_{Q\in\Delta} Q$.

The antecedent $\Gamma$ can be thought of as the list of formulas we assume to be true, whereas the succedent $\Delta$ can be understood as formulas for which we want to show that at least one of them is true, assuming all formulas of $\Gamma$ are true. So for proving a sequent $\Gamma \vdash \Delta$, we assume all $\Gamma$ and want to show that one of the $\Delta$ is true. For some simple sequents like $\Gamma, P \vdash P, \Delta$ where, among another set of formulas $\Gamma$ in the antecedent and another set of formulas $\Delta$ in the succedent, the same formula $P$

[3] It would have been very easy to define, though, by inductively defining formulas to be provable if they are either instances of axioms or follow from provable formulas using modus ponens [16].

is in the antecedent and the succedent, we directly know that they are valid, because we can certainly show $P$ if we assume $P$. In fact, we will use this we will use this as a way of finishing a proof. For other sequents, it is more difficult to see whether they are valid (true under all circumstances) and it is the purpose of a proof calculus to provide a means to find out.

The basic idea in sequent calculus is to successively transform all formulas such that $\Gamma$ forms a list of all assumptions and $\Delta$ the set of formulas that we would like to conclude from $\Gamma$ (or, to be precise, the set $\Delta$ whose disjunction we would like to conclude from the conjunction of all formulas in $\Gamma$). For example, when a formula of the form $P \wedge Q$ is in the antecedent, we will identify a proof rule that simplifies $P \wedge Q$ in the sequent $\Gamma, P \wedge Q \vdash \Delta$ by replacing it with its two subformulas $P$ and $Q$ to lead to $\Gamma, P, Q \vdash \Delta$, because assuming the two formulas $P$ and $Q$ separately is the same as assuming the conjunction $P \wedge Q$, but involves smaller formulas.

Arguably the easiest way of understanding sequent calculus would be to interpret $\Gamma \vdash \Delta$ as the task of proving one of the formulas in the succedent $\Delta$ from all of the formulas in the antecedent $\Gamma$. But since dL is a classical logic, not an intuitionistic logic, we need to keep in mind that it is actually enough for proving a sequent $\Gamma \vdash \Delta$ to just prove the disjunction of all formulas in $\Delta$ from the conjunction of all formulas in $\Gamma$. For the proof rules of real arithmetic, we will later make use of this fact by considering the sequent $\Gamma \vdash \Delta$ as an abbreviation for the formula $\bigwedge_{P \in \Gamma} P \rightarrow \bigvee_{Q \in \Delta} Q$, because both have the same semantics in dL. Indeed, a proof of the sequent $z = 0 \vdash x \geq z, x < z^2$ is only possible with this disjunctive interpretation of the succedent. We cannot say whether $x \geq z$ is true or whether $x < z^2$ is true, but if $z = 0$ is assumed, it is a classical triviality that their disjunction is true.

Empty conjunctions $\bigwedge_{P \in \emptyset} P$ are equivalent to *true*. Empty disjunctions $\bigvee_{P \in \emptyset} P$ are equivalent to *false*.[4] Hence, the sequent $\vdash A$ means the same as the formula $A$. The empty sequent $\vdash$ means the same as the formula *false*. The sequent $A \vdash$ means the same as formula $A \rightarrow$ *false*. Starting off a proof question is easy, too, because if we would like to prove a dL formula $P$, we turn it into a sequent with no assumptions, since we do not initially have any, and set out to prove the sequent $\vdash P$.

[4] Note that *true* is the neutral element for the operation $\wedge$ and *false* the neutral element for the operation $\vee$. That is $A \wedge$ *true* is equivalent to $A$ for any $A$ and $A \vee$ *false* is equivalent to $A$. So *true* plays the same role that 1 plays for multiplication. And *false* plays the role that 0 plays for addition. Another aspect of sequents $\Gamma \vdash \Delta$ that is worth mentioning is that other notations such as $\Gamma \Longrightarrow \Delta$ or $\Gamma \longrightarrow \Delta$ are also sometimes used in other contexts.

**Note 34 (Nonempty trouble with empty sequents)** *If you ever reduce a conjecture about your CPS to proving the empty sequent $\vdash$, then you are in trouble, because the empty sequent $\vdash$ means the same as the formula false and it is impossible to prove false, since false isn't ever true. In that case, either you have taken a wrong turn in your proof, e.g., by discarding an assumption that was actually required for the conjecture to be true, or your CPS might take the wrong turn, because its controller can make a move that is actually unsafe.*

In order to develop sequent calculus proof rules, we will again follow the logical guiding principle of compositionality from Chap. 5 by devising one suitable proof rule for each of the relevant operators. Only this time, we have two cases to worry about for each operator. We will need one proof rule for the case where the operator occurs in the antecedent so that it is available as an assumption. The corresponding rule for $\wedge$ will be called $\wedge$L rule since it operates on the left of the $\vdash$ sequent turnstile. And we will need another proof rule for the case where that operator occurs in the succedent so that it is available as an option to prove. That rule for $\wedge$ will be called $\wedge$R rule since it is for $\wedge$ and operates on the right of the $\vdash$ sequent turnstile. Fortunately, we will find a clever way of simultaneously handling all of the modality operators at once in sequent calculus by using the dL axioms from Chap. 5.

### 6.2.2 Proofs

Before developing any proof rules for sequent calculus, let us first understand what exactly a proof is, what it means to prove a logical formula, and how we know whether a proof rule is sound so that it actually implies what it tries to prove.

**Definition 6.2 (Global Soundness).** A *sequent calculus proof rule* of the form

$$\frac{\Gamma_1 \vdash \Delta_1 \quad \ldots \quad \Gamma_n \vdash \Delta_n}{\Gamma \vdash \Delta}$$

is *sound* iff validity of all *premises* (i.e. the sequents $\Gamma_i \vdash \Delta_i$ above the rule bar) implies validity of the *conclusion* (i.e. the sequent $\Gamma \vdash \Delta$ below the rule bar):

$$\text{If } \vDash (\Gamma_1 \vdash \Delta_1) \text{ and } \ldots \text{ and } \vDash (\Gamma_n \vdash \Delta_n) \text{ then } \vDash (\Gamma \vdash \Delta)$$

Recall that the meaning of a sequent $\Gamma \vdash \Delta$ is $\bigwedge_{P\in\Gamma} P \rightarrow \bigvee_{Q\in\Delta} Q$ by Definition 6.1, so that $\vDash (\Gamma \vdash \Delta)$ stands for $\vDash \big(\bigwedge_{P\in\Gamma} P \rightarrow \bigvee_{Q\in\Delta} Q\big)$ in Definition 6.2.

A formula $P$ is provable or derivable (in the dL sequent calculus) if we can find a dL proof for it that concludes the sequent $\vdash P$ at the bottom *from no premises* and that has only used dL sequent proof rules to connect the premises to their conclusion. The rules id, $\top$R and $\bot$L we discuss below will prove particularly obvious sequents such as $\Gamma, P \vdash P, \Delta$ from no premises and, thereby, provide a way of finishing a

proof. The shape of a dL sequent calculus proof, thus, is a tree with axioms at the top leaves and the formula that the proof proves at the bottom root.

While constructing proofs, however, we start with the desired goal $\vdash P$ at the bottom, since we want $\vdash P$ as the eventual conclusion of the proof. We work our way backwards to the subgoals until they can be proven to be valid. Once all subgoals have been proven to be valid, they entail their respective conclusion, which, recursively, entail the original goal $\vdash P$. This property of preserving truth or preserving validity is called soundness (Definition 6.2). While constructing proofs, we work bottom-up from the goal to the subgoals and apply all proof rules from the desired conclusion to the required premises. Once we have found a proof, we justify formulas conversely from the leaves top-down to the original goal at the bottom, because validity transfers from the premises to the conclusion with sound proof rules.

construct proofs upwards $\uparrow$ $\dfrac{\Gamma_1 \vdash \Delta_1 \quad \ldots \quad \Gamma_n \vdash \Delta_n}{\Gamma \vdash \Delta}$ $\downarrow$ validity transfers downwards

We write $\vdash_{\mathsf{dL}} P$ iff dL formula $P$ can be *proved* with dL rules from dL axioms. That is, a dL formula is inductively defined to be *provable* in the dL sequent calculus iff it is the conclusion (below the rule bar) of an instance of one of the dL sequent proof rules, whose premises (above the rule bar) are all provable. A formula $Q$ is *provable* from a set $\Phi$ of formulas, denoted by $\Phi \vdash_{\mathsf{dL}} Q$, iff there is a finite subset $\Phi_0 \subseteq \Phi$ of formulas for which the sequent $\Phi_0 \vdash Q$ is provable.

### 6.2.3 Propositional Proof Rules

The first logical operators encountered during proofs are usually propositional logical connectives, because many dL formulas use shapes such as $A \rightarrow [\alpha]B$ to express that all behaviors of HP $\alpha$ lead to safe states satisfying $B$ when starting the system in initial states satisfying $A$. For propositional logic, dL uses the standard propositional rules with the cut rule, which are listed in Fig. 6.1. Each of these propositional rules decompose the propositional structure of formulas and neatly divides everything up into assumptions (which will ultimately be moved to the antecedent) and what needs to be shown (which will be moved to the succedent). The rules will be developed one at a time in the order that is most conducive to their intuitive understanding.

#### Rules for Propositional Connectives

Proof rule $\wedge$L is for handling conjunctions $(P \wedge Q)$ as one of the assumptions in the antecedent on the left of the sequent turnstile ($\vdash$). Assuming the conjunction $P \wedge Q$ is the same as assuming each conjunct $P$ as well as $Q$ separately.

$$\neg\mathrm{R}\ \frac{\Gamma, P \vdash \Delta}{\Gamma \vdash \neg P, \Delta} \qquad \wedge\mathrm{R}\ \frac{\Gamma \vdash P, \Delta \quad \Gamma \vdash Q, \Delta}{\Gamma \vdash P \wedge Q, \Delta} \qquad \vee\mathrm{R}\ \frac{\Gamma \vdash P, Q, \Delta}{\Gamma \vdash P \vee Q, \Delta}$$

$$\neg\mathrm{L}\ \frac{\Gamma \vdash P, \Delta}{\Gamma, \neg P \vdash \Delta} \qquad \wedge\mathrm{L}\ \frac{\Gamma, P, Q \vdash \Delta}{\Gamma, P \wedge Q \vdash \Delta} \qquad \vee\mathrm{L}\ \frac{\Gamma, P \vdash \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \vee Q \vdash \Delta}$$

$$\rightarrow\mathrm{R}\ \frac{\Gamma, P \vdash Q, \Delta}{\Gamma \vdash P \rightarrow Q, \Delta} \qquad \mathrm{id}\ \frac{}{\Gamma, P \vdash P, \Delta} \qquad \top\mathrm{R}\ \frac{}{\Gamma \vdash \mathit{true}, \Delta}$$

$$\rightarrow\mathrm{L}\ \frac{\Gamma \vdash P, \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \rightarrow Q \vdash \Delta} \qquad \mathrm{cut}\ \frac{\Gamma \vdash C, \Delta \quad \Gamma, C \vdash \Delta}{\Gamma \vdash \Delta} \qquad \bot\mathrm{L}\ \frac{}{\Gamma, \mathit{false} \vdash \Delta}$$

**Fig. 6.1** Propositional proof rules of sequent calculus

$$\wedge\mathrm{L}\ \frac{\Gamma, P, Q \vdash \Delta}{\Gamma, P \wedge Q \vdash \Delta}$$

Rule $\wedge$L expresses that if a conjunction $P \wedge Q$ is among the list of available assumptions in the antecedent, then we might just as well assume both conjuncts ($P$ and $Q$, respectively) separately. Assuming a conjunction $P \wedge Q$ is the same as assuming both conjuncts $P$ and $Q$. So, if we set out to prove a sequent of the form in the conclusion ($\Gamma, P \wedge Q \vdash \Delta$), then we can justify this sequent by instead proving the sequent in the premise ($\Gamma, P, Q \vdash \Delta$), where the only difference is that the two assumptions $P$ and $Q$ are now assumed separately in the premise rather than jointly as a single conjunction as in the conclusion.

If we keep on using proof rule $\wedge$L often enough, then all conjunctions in the antecedent will ultimately have been split into their smaller pieces. Recall that the order of formulas in a sequent $\Gamma \vdash \Delta$ is irrelevant because $\Gamma$ and $\Delta$ are sets, so we can always pretend that the formula that we want to apply the rule $\wedge$L to is last in the antecedent. Rule $\wedge$L takes care of all conjunctions that appear as top-level operators in antecedents even if its notation seems to indicate it would expect $P \wedge Q$ at the end of the antecedent. Of course, $\wedge$L does not say how to prove $A \vee (B \wedge C) \vdash C$ or $A \vee \neg(B \wedge C) \vdash C$, because its conjunction $B \wedge C$ is not a top-level formula in the antecedent but merely occurs somewhere deep inside as a subformula. But there are other logical operators to worry about as well, whose proof rules will decompose the formulas and ultimately reveal $B \wedge C$ at the top-level somewhere in the sequent.

Proof rule $\wedge$R is for handling conjunction $P \wedge Q$ in the succedent by proving $P$ and, in a separate premise, also proving $Q$:

$$\wedge\mathrm{R}\ \frac{\Gamma \vdash P, \Delta \quad \Gamma \vdash Q, \Delta}{\Gamma \vdash P \wedge Q, \Delta}$$

Rule $\wedge$R has to prove two premises, because if we are trying to prove a sequent $\Gamma \vdash P \wedge Q, \Delta$ with a conjunction $P \wedge Q$ in its succedent, it would not be enough at all to just prove $\Gamma \vdash P, Q, \Delta$, because the meaning of the succedent is a disjunction, so it would only enable us to conclude the weaker $\Gamma \vdash P \vee Q, \Delta$. Proving a conjunction in the succedent as in the conclusion of $\wedge$R, thus, requires proving both conjuncts. It needs a proof of $\Gamma \vdash P, \Delta$ *and* a proof of $\Gamma \vdash Q, \Delta$. This is why rule $\wedge$R splits the proof into two branches, one for proving $\Gamma \vdash P, \Delta$ and one for proving $\Gamma \vdash Q, \Delta$. If

both premises of rule ∧R are valid then so is its conclusion. To see this, it is easier to first consider the case where $\Delta$ is empty. A proof of $\Gamma \vdash P$ together with a proof of $\Gamma \vdash Q$ implies that $\Gamma \vdash P \wedge Q$ is valid, because the conjunction $P \wedge Q$ follows from the assumptions $\Gamma$ if both $P$ and $Q$ individually follow from $\Gamma$. Rule ∧R is justified by arguing by cases, once for the case where the disjunction corresponding to $\Delta$ is false (in which case the argument for $\Gamma \vdash P \wedge Q$ suffices) and once where it is true (in which case the conclusion is true without $P \wedge Q$). Overall, proof rule ∧R captures that proving a conjunction $P \wedge Q$ amounts to proving both $P$ and $Q$ separately.

Proof rule ∨R is similar to rule ∧L but for handling disjunctions in the succedent. If we set out to prove the sequent $\Gamma \vdash P \vee Q, \Delta$ in the conclusion with a disjunction $P \vee Q$ in the succedent, then we might as well split the disjunction into its two disjuncts and prove the premise $\Gamma \vdash P, Q, \Delta$ instead, since the succedent has a disjunctive meaning anyhow, so both sequents mean the same formula.

Proof rule ∨L handles a disjunction in the antecedent. When the assumptions listed in the antecedent of a sequent contain a disjunction $P \vee Q$, then there is no way of knowing which of the two disjuncts can be assumed, merely that at least one of them is assumed to be true. Rule ∨L, thus, splits the proof into cases. The left premise considers the case where the assumption $P \vee Q$ held because $P$ was true. The right premise considers the case where assumption $P \vee Q$ held because $Q$ was true. If both premises are valid (because we can find a proof for them), then, either way, the conclusion $\Gamma, P \vee Q \vdash \Delta$ will be valid no matter which of the two cases applies. Overall, rule ∨L captures that assuming a disjunction $P \vee Q$ requires two separate proofs that assume each disjunct instead.

Proof rule →R handles implications in the succedent by using the implicational meaning of sequents. The way to understand it is to recall how we would prove an implication in mathematics. In order to prove an implication $P \to Q$, we would assume the left-hand side $P$ (which →R pushes into the assumptions listed in the antecedent) and try to prove its right-hand side $Q$ (which →R thus leaves in the succedent). This is how left-hand sides of implications ultimately end up as assumptions in the antecedent. Rule →R, thus, captures that proving an implication $P \to Q$ amounts to assuming the left-hand $P$ and proving the right-hand $Q$.

Proof rule →L is more involved. It it used to handle assumptions that are implications $P \to Q$. When assuming an implication $P \to Q$, we can only assume its right-hand side $Q$ (second premise) after we have shown its respective assumption $P$ on its left-hand side (first premise). Another way to understand it is to recall that classical logic obeys the equivalence $(P \to Q) \equiv (\neg P \vee Q)$ and then using the other propositional rules. Rule →L captures that using an assumed implication $P \to Q$ allows us to assume its right-hand side $Q$ if we can prove its left-hand side $P$.

Proof rule ¬R proves a negation $\neg P$ by, instead, assuming $P$. Again, the easiest way of understanding this rule is for an empty $\Delta$ in which case rule ¬R expresses that the way of proving a negation $\neg P$ in the succedent of the conclusion is to instead assume $P$ in the antecedent in the premise and proving a contradiction, which is the formula *false* that an empty succedent means. When $\Delta$ is not empty, arguing by cases of whether the disjunction that $\Delta$ means is true or false will again do the trick. Alternatively, rule ¬R can be understood using the semantics of sequents from

Definition 6.1, since a conjunct $P$ on the left-hand side of an implication is semantically equivalent to a disjunct $\neg P$ on the right-hand side in classical logic. Overall, rule $\neg$R captures that for proving a negation $\neg P$, it is enough to assume $P$ and prove a contradiction (or the remaining options $\Delta$).

Proof rule $\neg$L handles a negation $\neg P$ among the assumptions in the antecedent of the conclusion by, instead, pushing $P$ into the succedent of the premise. Indeed, for the case of empty $\Delta$, if $P$ were shown to hold from the remaining assumptions $\Gamma$, then $\Gamma$ and $\neg P$ imply a contradiction in the form of the empty sequent, which is *false*. A semantic argument using the semantics of sequents also justifies $\neg$L directly since a conjunct $\neg P$ on the left-hand side of an implication is semantically equivalent to a disjunct $P$ on the right-hand side in classical logic.

### Identity and Cut Rules

All these propositional rules make progress by splitting operators. There is exactly one proof rule for each propositional logical connective on each side of the turnstile. All it takes is to look at the top-level operator of a formula and use the appropriate propositional sequent calculus rule from Fig. 6.1 to split the formula into its pieces. Such splitting will ultimately lead to *atomic formulas*, i.e. those formulas without any logical operators. But there is no way to ever stop the proof yet. That is what the identity rule id from Fig. 6.1 is meant for. The identity rule id closes a goal (there are no further subgoals, which we sometimes mark by a $*$ instead of a sequent to indicate that we didn't just forget to finish the proof), because assumption $P$ in the antecedent trivially implies $P$ in the succedent (the sequent $\Gamma, P \vdash P, \Delta$ is a simple syntactic tautology). If, in our proving activities, we ever find a sequent of the form $\Gamma, P \vdash P, \Delta$, for any formula $P$, we can immediately use the identity rule id to close this part of the proof. The proof attempt succeeds if all premises are closed by id, or by other closing rules such as $\top$R (it is trivial to prove the valid formula *true*) or $\bot$L (assuming the unsatisfiable formula *false* means assuming the impossible).

Rule cut is Gentzen's *cut* rule [9, 10] that can be used for case distinctions or to prove a lemma and then use it. The right premise assumes any additional formula $C$ in the antecedent that the left premise shows in the succedent. Semantically: regardless of whether $C$ is actually true or false, both cases are covered by proof branches. Alternatively, and more intuitively, the cut rule is a fundamental lemma rule. The left premise proves an auxiliary lemma $C$ in its succedent, which the right premise then assumes in its antecedent for the rest of the proof (again consider the case of empty $\Delta$ first to understand why this is sound). We only use cuts in an orderly fashion to derive simple rule dualities and to simplify meta-proofs. In practical applications, cuts are not needed in principle. In practice, complex CPS proofs still make use of cuts for efficiency reasons. Cuts can be used, for example, to substantially simplify arithmetic, or to first prove lemmas and then make ample use of them, in a number of places in the remaining proof.

Even though we write sequent rules as if the *principal formula* (which is the one that the sequent rule acts on like $P \wedge Q$ in rules $\wedge$R and $\wedge$L) were at the end of

the antecedent or at the beginning of the succedent, respectively, the sequent proof rules can be applied to other formulas in the antecedent or succedent, respectively, because we consider their order to be irrelevant. Antecedents and succedents are finite sets.

### Sequent Proof Example

Even if the propositional sequent proof rules could hardly be the full story behind reasoning for cyber-physical systems, they still provide a solid basis and deserve to be explored with a simple example.

*Example 6.1.* A propositional proof of the exceedingly simple formula

$$v^2 \leq 10 \land b > 0 \rightarrow b > 0 \land (\neg(v \geq 0) \lor v^2 \leq 10) \tag{6.1}$$

is shown in Fig. 6.2. The proof starts with the desired goal as a sequent at the bottom:

$$\vdash v^2 \leq 10 \land b > 0 \rightarrow b > 0 \land (\neg(v \geq 0) \lor v^2 \leq 10).$$

and proceeds by applying suitable sequent proof rules upwards until we run out of subgoals and have finished the proof (the notation $*$ is used to indicate when there are no subgoals, which happens after rules id,$\top$R,$\bot$L).

$$\dfrac{\dfrac{\dfrac{*}{v^2 \leq 10, b > 0 \vdash b > 0}\,\text{id}}{v^2 \leq 10 \land b > 0 \vdash b > 0}\,\land\text{L} \qquad \dfrac{\dfrac{*}{v^2 \leq 10, b > 0 \vdash \neg(v \geq 0), v^2 \leq 10}\,\text{id}}{v^2 \leq 10 \land b > 0 \vdash \neg(v \geq 0), v^2 \leq 10}\,\land\text{L}}{v^2 \leq 10 \land b > 0 \vdash \neg(v \geq 0) \lor v^2 \leq 10}\,\lor\text{R}}{v^2 \leq 10 \land b > 0 \vdash b > 0 \land (\neg(v \geq 0) \lor v^2 \leq 10)}\,\land\text{R}}{\vdash v^2 \leq 10 \land b > 0 \rightarrow b > 0 \land (\neg(v \geq 0) \lor v^2 \leq 10)}\,\rightarrow\text{R}$$

**Fig. 6.2** A simple propositional example proof in sequent calculus

The first (i.e., bottom most) proof step applies proof rule $\rightarrow$R to turn the implication ($\rightarrow$) to the sequent level by moving its left-hand side into the assumptions tracked in the antecedent. The next proof step applies rule $\land$R to split the proof into the left branch for showing that conjunct $b > 0$ follows from the assumptions in the antecedent and into the right branch for showing that conjunct $\neg(v \geq 0) \lor v^2 \leq 10$ follows from the antecedent also. On the left branch, the proof closes with an axiom id after splitting the conjunction $\land$ in the antecedent into its conjuncts with rule $\land$L. We mark closed proof goals with $*$, to indicate that we did not just stopped writing but that a subgoal is actually proved successfully. Of course, the left branch closes by rule id, because its assumption $b > 0$ in the antecedent trivially implies the formula $b > 0$ in the succedent, as both formulas are identical. The right branch closes with rule id after splitting the disjunction ($\lor$) in the succedent with rule $\lor$R and then

splitting the conjunction ($\wedge$) in the antecedent with rule $\wedge$L. On the right branch, the first assumption formula $v^2 \leq 10$ in the antecedent trivially implies the last formula in the succedent $v^2 \leq 10$, because both are identical, so rule id applies.

Now that all branches of the proof have closed (with id and marked by $*$), we know that all leaves at the top are valid. Since the premises are valid, each application of a proof rule ensures that their respective conclusions are valid also, by soundness. By recursively following this proof from the leaves at the top to the original root at the bottom, we conclude that the original goal at the bottom is valid and formula (6.1) is, indeed, true under all circumstances (valid). The conjecture that formula (6.1) is valid is exactly what the proof in Fig. 6.2 justifies.

While this proof does not prove any particularly exciting formula, it still shows how a proof can be built systematically in the dL calculus and gives an intuition as to how validity is inherited from the premises to the conclusions. The proof has been entirely systematic. All we did to come up with it was successively inspect the top-level operator in one of the logical formulas in the sequent and apply its corresponding propositional proof rule to find the resulting subgoals. All the while we were doing this, we carefully watched to see if the same formula shows up in the antecedent and succedent, for then the rule id closes that subgoal. There would be no point in proceeding with any other proof rule if the rule id closes a subgoal.

Most interesting formulas will not be provable with the sequent proof rules we have seen so far, because those were only for propositional connectives. Next, we, thus, set out to find proof rules for the other operators of differential dynamic logic.

### 6.2.4 Soundness

Before proceeding with an investigation of additional sequent calculus proof rules, notice that the sequent proof rules for propositional logic are sound [9, 10, 15] according to the global soundness notion defined in Definition 6.2. We consider only one of the proof rules here to show how soundness works. Soundness is crucial, however, so you are invited to prove soundness for the other rules (Exercise 6.6).

*Proof.* The proof rule $\wedge$R is sound. For this, consider any instance for which both premises $\Gamma \vdash P, \Delta$ and $\Gamma \vdash Q, \Delta$ are valid and show that the conclusion $\Gamma \vdash P \wedge Q, \Delta$ is valid. To show the latter, consider any state $\omega$. If there is a formula $F \in \Gamma$ in the antecedent that is not true in $\omega$ (i.e. $\omega \notin [\![F]\!]$) there is nothing to show, because $\omega \in [\![\Gamma \vdash P \wedge Q, \Delta]\!]$ then holds trivially, because not all assumptions in $\Gamma$ are satisfied in $\omega$. Likewise, if there is a formula $G \in \Delta$ in the succedent that is true in $\omega$ (i.e. $\omega \in [\![G]\!]$) there is nothing to show, because $\omega \in [\![\Gamma \vdash P \wedge Q, \Delta]\!]$ then holds trivially, because one of the formulas in the succedent is already satisfied in $\omega$. Hence, the only interesting case to consider is the case where all formulas in $F \in \Gamma$ are true in $\omega$ and all formulas $G \in \Delta$ are false. In that case, since both premises were assumed to be valid, and $\Gamma$ is true in $\omega$ but $\Delta$ false in $\omega$, the left premise implies that $\omega \in [\![P]\!]$ and the right premise implies that $\omega \in [\![Q]\!]$. Consequently, $\omega \in [\![P \wedge Q]\!]$ by the se-

mantics of $\wedge$. Thus, $\omega \in [\![\Gamma \vdash P \wedge Q, \Delta]\!]$. As the state $\omega$ was arbitrary, this implies $\models (\Gamma \vdash P \wedge Q, \Delta)$, i.e. the conclusion of the considered instance of $\wedge$R is valid. □

### 6.2.5 Proofs with Dynamics

Now that we identified a left and a right proof rule for all propositional connectives we could literally continue the logical guiding principle of connectivity and proceed to also identify a left and a right proof rule for all top-level operator in all modalities.

#### Sequent Calculus Proof Rules for Dynamics

We could add a pair of sequent calculus proof rules for nondeterministic choices in box modalities, one in the antecedent (rule $[\cup]R$) and one in the succedent ($[\cup]L$):

$$[\cup]R\ \frac{\Gamma \vdash [\alpha]P \wedge [\beta]P, \Delta}{\Gamma \vdash [\alpha \cup \beta]P, \Delta}$$

$$[\cup]L\ \frac{\Gamma, [\alpha]P \wedge [\beta]P \vdash \Delta}{\Gamma, [\alpha \cup \beta]P \vdash \Delta}$$

These rules directly follow from the axioms from Chap. 5, though, and would, thus, lead to quite some unnecessary duplication of concepts.[5] Furthermore, such a list of sequent rules is less flexible than the axioms from Chap. 5 are. The sequent rules $[\cup]R$,$[\cup]L$ can only be applied when a nondeterministic choice is at the top-level position of a sequent, not when it occurs somewhere in a subformula such as at the underlined position in the following sequent near the bottom of the proof of single-hop bouncing balls from Sect. 5.4:

$$A \vdash [x'' = -g]\underline{[?x = 0; v := -cv \cup ?x \geq 0]B(x,v)} \tag{6.2}$$

#### Substituting Equals for Equals

Thus, instead of writing down a pair of (rather redundant and quite inflexible) sequent rules for each dynamic axiom, we instead cover all axioms at once. The key observation was already foreshadowed in Chap. 5:

[5] One subsequent difference will be that applying rule $\wedge$R to the premise of $[\cup]$ will split the proof into two premises while subsequently applying $\wedge$L to the premise of $[\cup]$ will not.

**Note 35 (Substituting equals for equals)** *If an equivalence $P \leftrightarrow Q$ is a valid formula, then any occurrence of its left-hand side $P$ in any subformula can be replaced by its right-hand side $Q$ (or vice versa), equivalently.*

For example, using at the underlined position in the middle of dL formula (6.2) the equivalence

$$\underline{[?x=0;v:=-cv\cup ?x\geq 0]B(x,v)} \leftrightarrow [?x=0;v:=-cv]B(x,v)\wedge[?x\geq 0]B(x,v) \tag{6.3}$$

that is a direct instance of axiom [∪] $[\alpha\cup\beta]P \leftrightarrow [\alpha]P\wedge[\beta]Q$ from Chap. 5, the formula (6.2) is equivalent to

$$A \vdash [x''=-g]\big(\underline{[?x=0;v:=-cv]B(x,v)\wedge[?x\geq 0]B(x,v)}\big) \tag{6.4}$$

since (6.4) is constructed from (6.2) by replacing the left-hand side of equivalence (6.3) by its right-hand side in the middle of formula (6.2) at the indicated position.

### Contextual Equivalence

The intuition of substituting equals for equals serves us well and is perfectly sufficient for all practical purposes. Logic is ultimately about precision, though, which is why we elaborate Note 35 as follows:

**Lemma 6.1 (Contextual equivalence).** *The contextual equivalence rewriting rules are sound:*

$$\text{CER}\ \frac{\Gamma \vdash C(Q),\Delta \quad \vdash P\leftrightarrow Q}{\Gamma\vdash C(P),\Delta} \qquad \text{CEL}\ \frac{\Gamma,C(Q)\vdash\Delta \quad \vdash P\leftrightarrow Q}{\Gamma,C(P)\vdash\Delta}$$

That is, if the equivalence $P\leftrightarrow Q$ in the second premise proves, then $P$ can be replaced by $Q$ in any context $C(\_)$ anywhere in the succedent (rule CER) or in the antecedent (rule CEL) in the first premise. Here we read $C(\_)$ as the *context* in which the formula $P$ occurs in the formula $C(P)$ and read $C(Q)$ as the result of replacing $P$ in that context $C(\_)$ by $Q$. While a concise technical treatment and precise definitions of contexts and soundness proof for CER,CEL is surprisingly simple [19], this intuitive understanding is enough for our purposes here. If $P$ and $Q$ are equivalent (second premise of CER and of CEL), then we can replace $P$ by $Q$ no matter in what context $C(\_)$ they occur in the sequents in the succedent (CER) or antecedent (CEL), respectively. These contextual equivalence rules provide the perfect lifting device to use all equivalence axioms from Chap. 5 in any context in any proof.

Of course, it is crucial that $P$ and $Q$ are actually equivalent (second premise of CER and CEL) unconditionally without any assumptions from $\Gamma$, because those assumptions from $\Gamma$ may no longer hold in the context $C(\_)$. For example, even if

$x=1$ and $x^2=1$ are equivalent when assuming $x\geq 0$, that assumption is no longer available in the context $[x:=-1]\_$, so the following cannot be proved by CER:

$$\lightning\ \frac{x\geq 0\vdash [x:=-1]x^2=1 \quad x\geq 0\vdash x=1\leftrightarrow x^2=1}{x\geq 0\vdash [x:=-1]x=1}$$

This inference would, indeed, be unsound, because the premises are valid but the conclusion is not.

The flexible device of contextual equivalence rewriting by CER,CEL enables flexible and intuitive reasoning steps. Of course, we should still take care to use the axioms in the direction that actually simplifies the problem at hand. The dL axioms such as axiom $[\cup]$ are primarily meant to be used for replacing the left-hand side $[\alpha\cup\beta]P$ by the structurally simpler right-hand side $[\alpha]P\wedge[\beta]P$, because that direction of use assigns meaning to $[\alpha\cup\beta]P$ in logically simpler terms, i.e. as a structurally simpler logical formula. Furthermore, that direction reduces a dL formula to a formula with more formulas but smaller hybrid programs, which will terminate after finitely many such reductions, because every hybrid program only has finitely many subprograms.

Finally note that we will usually not explicitly mention the use of CEL and CER in proofs but leave it at a mention of the axiom that they invoked. For example, the sequent proof step reducing conclusion (6.2) to premise (6.4) using axiom $[\cup]$ (and, of course, the implicit rule CER) is simply written as:

$$[\cup]\ \frac{A\vdash [x''=-g]\big([?x=0;v:=-cv]B(x,v)\wedge[?x\geq 0]B(x,v)\big)}{A\vdash [x''=-g][?x=0;v:=-cv\cup ?x\geq 0]B(x,v)}$$

In fact the full proof in Sect. 5.4 can suddenly be made sense of as a sequent proof in this way by adding a sequent turnstile $\vdash$ and implicitly using CER in addition to the respective indicated dynamic axioms.

### Sequent Proof Example with Dynamics

See Fig. 6.3 for a simple example proof. This proof is not very interesting. Inciden-

$$\cfrac{\cfrac{\cfrac{\vdash v^2\leq 10\wedge -(-b)>0\rightarrow b>0\wedge(\neg(v\geq 0)\vee v^2\leq 10)}{[:=]\ \vdash [c:=10]\big(v^2\leq 10\wedge -(-b)>0\rightarrow b>0\wedge(\neg(v\geq 0)\vee v^2\leq c)\big)}}{[:=]\ \vdash [a:=-b][c:=10]\big(v^2\leq 10\wedge -a>0\rightarrow b>0\wedge(\neg(v\geq 0)\vee v^2\leq c)\big)}}{[;]\ \vdash [a:=-b;c:=10]\big(v^2\leq 10\wedge -a>0\rightarrow b>0\wedge(\neg(v\geq 0)\vee v^2\leq c)\big)}$$

**Fig. 6.3** A simple dynamics example proof in sequent calculus

tally, though, the proof in Fig. 6.3 ends with a premise at the top that is identical to the (provable) conclusion at the bottom of Fig. 6.2. So gluing both proofs together

leads to a proof of the conclusion at the bottom of Fig. 6.3:

$$[a:=-b;c:=10]\big(v^2 \leq 10 \land -a > 0 \rightarrow b > 0 \land (\neg(v \geq 0) \lor v^2 \leq c)\big)$$

Since this completes the proof (no more premises) and dL proof rules and axioms are sound, this conclusion is valid, so true in all states. Most crucially, this dL formula now has the proof as a finite and entirely syntactic justification of why it is valid. That is certainly more practical than enumerating all of the infinitely many possible real values for the variables and checking whether the semantics evaluates to true.

A minor wrinkle foreshadowing further developments is that the proof in Fig. 6.3 ends in a formula mentioning $-(-b) > 0$ while the proof in Fig. 6.2 starts with a formula mentioning $b > 0$ in the same place. Both formulas are, of course, equivalent, but, in order to really glue both proofs togther, we still need to add some proof rule that justifies this arithmetic transformation. We could add the following special-purpose proof rule for this purpose, but will ultimately decide on adding a more powerful proof rule instead (Sect. 6.5):

$$\frac{\Gamma, \theta > 0 \vdash \Delta}{\Gamma, -(-\theta) > 0 \vdash \Delta}$$

### 6.2.6 *Quantifier Proof Rules*

When trying to make the proof for the bouncing ball from Sect. 5.4 systematic by turning it into a sequent calculus proof, the first propositional step succeeds with $\rightarrow$R, then a couple of steps succeed for splitting the hybrid program with dynamic axioms from Chap. 5, but, ultimately, the differential equation solution axiom $[']$ produces a quantifier for time that still needs to be handled. Of course, even a mere inspection of the syntax of dL shows that there are logical operators that have no proof rules yet, namely the universal and existential quantifiers.

$$\forall\text{R}\ \frac{\Gamma \vdash p(y), \Delta}{\Gamma \vdash \forall x\, p(x), \Delta}\ (y \notin \Gamma, \Delta, \forall x\, p(x)) \qquad \exists\text{R}\ \frac{\Gamma \vdash p(e), \Delta}{\Gamma \vdash \exists x\, p(x), \Delta}$$

$$\forall\text{L}\ \frac{\Gamma, p(e) \vdash \Delta}{\Gamma, \forall x\, p(x) \vdash \Delta} \qquad \exists\text{L}\ \frac{\Gamma, p(y) \vdash \Delta}{\Gamma, \exists x\, p(x) \vdash \Delta}\ (y \notin \Gamma, \Delta, \exists x\, p(x))$$

**Fig. 6.4** Quantifier sequent calculus proof rules

The quantifier proof rules are listed in Fig. 6.4 and work much as in mathematics. In the proof rule $\forall$R, we want to show a universally quantified property. When a mathematician wants to show a universally quantified property $\forall x\, p(x)$ to hold, he

could choose a fresh symbol[6] $y$ and set out to prove that $p(y)$ holds. Once he found a proof for $p(y)$, the mathematician would remember that $y$ was arbitrary and his proof did not assume anything special about the value of $y$. So he would conclude that $p(y)$ must indeed hold for all $y$ since $y$ was arbitrary, and that, hence, $\forall x\, p(x)$ holds true. For example, to show that the square of all numbers is nonnegative, a mathematician could start out by saying "let $y$ be an arbitrary number", prove $y^2 \geq 0$ for that $y$, and then conclude $\forall x\,(x^2 \geq 0)$, since $y$ was arbitrary. Proof rule $\forall$R makes this reasoning formally rigorous. It chooses a *new* variable symbol $y$ and replaces the universally quantified formula in the succedent by a formula for $y$. Notice, of course, how crucially important it is to actually choose a new symbol $y$ that has not been used free anywhere else in the sequent before. Otherwise, we would assume special properties about $y$ in $\Gamma, \Delta$ that would not be justified to assume. In fact, it is enough if the variable $y$ just is no free variable in the sequent $\Gamma \vdash \forall x\, p(x), \Delta$, in which case the variable $x$ itself can be used for the fresh symbol $y$, see Sect. 5.6.5.

In proof rule $\exists$R, we want to show an existentially quantified property. When a mathematician proves $\exists x\, p(x)$, he could directly produce any specific term $e$ as a witness for this existential property and prove that, indeed, $p(e)$, for then he would have shown $\exists x\, p(x)$ with this witness. For example, to show that there is a number whose cube is less than its square, a mathematician could start by saying "let me choose, say, $\frac{2-1}{2}$ and show the property for $\frac{2-1}{2}$". Then he could prove $(\frac{2-1}{2})^3 < (\frac{2-1}{2})^2$, because $0.125 < 0.25$, and conclude that there, thus, is such a number, i.e., $\exists x\,(x^3 < x^2)$, because $\frac{2-1}{2}$ was a perfectly good witness. This reasoning is exactly what proof rule $\exists$R enables. It allows the choice of *any* term $e$ for $x$ and accepts a proof of $p(e)$ as a proof of $\exists x\, p(x)$. Unlike in rule $\forall$R, it is perfectly normal for the witness $e$ to mention other variables. For example, the witness for $a > 0 \vdash \exists x\,(x > y^2 \wedge x < y^2 + a)$ is $y^2 + \frac{a}{2}$, which has to depend on $y$ and $a$.

However note that the claim "$e$ is a witness" may turn out to be wrong, for example, the choice 2 for $x$ would have been a pretty bad start for attempting to show $\exists x\,(x^3 < x^2)$. Consequently, proof rule $\exists$R is sometimes discarded in favor of a rule that keeps both options $p(e)$ and $\exists x\, p(x)$ in the succedent. KeYmaera X instead allows undoing proof steps if a proof attempt failed. If the proof with $e$ is successful, the sequent is valid and the part of the proof can be closed successfully. If the proof with $e$ later turns out to be unsuccessful, another proof attempt can be started.

This approach already hints at a practical problem. If we are very smart about our choice of the witness $e$, rule $\exists$R leads to very short and elegant proofs. If not, we may end up going in circles without much progress in the proof. That is why KeYmaera X allows you to specify a witness if you can find one (and you should if you can, because that gives significantly faster proofs) but also allows you to keep going without a witness, e.g., by applying axioms to the formula $p(e)$ without touching the quantifier.

Rules $\forall$L,$\exists$L are dual to $\exists$R,$\forall$L. In proof rule $\forall$L, we have a universally quantified formula in the assumptions (antecedent) that we can use, instead of in the succedent,

[6] In logic, these fresh symbols are known as *Skolem function symbol* [21] or Herbrand function symbol [11], except that here we can just use fresh variables for the same purpose.

which we want to show. In mathematics, when we know a universal fact, we can use this knowledge for any particular instance. If we know that all positive numbers have a square root, then we can also use the fact that 5 has a square root, because 5 is a positive number. Hence from assumption $\forall x\,(x > 0 \rightarrow \exists y\, x = y^2)$ in the antecedent, we can also assume the particular instance $5 > 0 \rightarrow \exists y\, x = y^2)$ that uses 5 for $x$. Rule $\forall$L can produce an instance $p(e)$ of the assumption $\forall x\, p(x)$ for an arbitrary term $e$. We sometimes need the universal fact $\forall x\, p(x)$ for multiple instantiations with $e_1, e_2, e_3$ during the proof. Fortunately, rule $\forall$L is also sound when it keeps the assumption $\forall x\, p(x)$ in the antecedent so that it can be used repeatedly to obtain different instances.

In proof rule $\exists$L, we can use an existentially quantified formula from the antecedent. If we know an existential fact in mathematics, then we can give a name to the object that we then know does exist. If we know that there is a smallest integer less than 10 that is a square, we can call it $y$, but we cannot denote it by a different term like 5 or 4+2, because they may be (and in fact are) the wrong answer. Rule $\exists$L gives a fresh name $y$ to the object that was assumed to exist. Since it does not make sense to give a different name for the same object later, $\exists x\, p(x)$ is removed from the antecedent when rule $\exists$L adds $p(y)$.

Note how the quantifier proof rules in Fig. 6.4 continue the trend of the propositional sequent calculus rules in Fig. 6.1: they decompose logical formulas into simpler subformulas. Admittedly, the instances $e$ chosen in rules $\exists$R,$\forall$L can be rather large terms. But that is a matter of perspective. All it takes is for us to understand that concrete terms, no matter how large, are still structurally simpler than quantifiers.

## 6.3 Derived Proof Rules

The universal quantifier rule $\forall$L for the antecedent shown in Fig. 6.4 does not retain the universal assumption $\forall x\, p(x)$ in the antecedent even if it said it could. The following proof rule helps in cases where multiple instantiations of a universal assumption are needed, because it can be used repeatedly to produce $p(e)$ and $p(\tilde{e})$:

$$\forall\forall\text{L}\ \frac{\Gamma, \forall x\, p(x), p(e) \vdash \Delta}{\Gamma, \forall x\, p(x) \vdash \Delta}$$

But it is not very practical to adopt every possible proof rule. Instead, the newly suggested proof rule $\forall\forall$L is a *derived rule*, which means that it can be proved using the other proof rules already. Obviously, the only other proof rule that could produce an assumption $p(e)$ from the assumption $\forall x\, p(x)$ is rule $\forall$L from Fig. 6.4, and that rule swallows said assumption.

What we could do to derive $\forall\forall$L is to first copy the assumption $\forall x\, p(x)$ to obtain a duplicate, and then use $\forall$L to turn one copy into $p(e)$, leaving the other copy of $\forall x\, p(x)$ for later use. Only how do we copy assumptions?

Would it even be fine to duplicate assumptions in a sequent? Fortunately, sequents consist of a finite set of assumptions $\Gamma$ and a finite set $\Delta$, so that assuming the same formula twice does not change the meaning of the sequent (Sect. 6.5.4).

Operationally, assumptions can be duplicated by the cut rule to prove the formula $\forall x\, p(x)$ as a new lemma, which is trivial because it is among the assumptions, and then subsequently work with the extra assumption. This derives rule $\forall\forall$L by the following sequent calculus proof:

$$\text{cut}\dfrac{\text{id}\dfrac{*}{\Gamma, \forall x\, p(x) \vdash \forall x\, p(x), \Delta} \qquad \forall\text{L}\dfrac{\Gamma, \forall x\, p(x), p(e) \vdash \Delta}{\Gamma, \forall x\, p(x), \forall x\, p(x) \vdash \Delta}}{\Gamma, \forall x\, p(x) \vdash \Delta}$$

This sequent calculus proof starts with the conclusion of derived rule $\forall\forall$L at the bottom and ends with only the premises that rule $\forall\forall$L has at the top. What makes rule $\forall\forall$L a derived rule is that we can use it in any proof and expand it into the above more verbose proof using rules cut,id,$\forall$L instead.

## 6.4 A Sequent Proof for a Non-Bouncing Ball

Recall the bouncing ball abbreviations from Sect. 5.4:

$$\begin{aligned} A &\overset{\text{def}}{\equiv} 0{\leq}x \wedge x{=}H \wedge v{=}0 \wedge g{>}0 \wedge 1{\geq}c{\geq}0 \\ B(x,v) &\overset{\text{def}}{\equiv} 0 \leq x \wedge x \leq H \\ (x'' = -g) &\overset{\text{def}}{\equiv} \{x' = v, v' = -g\} \end{aligned}$$

And consider the single-hop bouncing ball formula again:

$$A \rightarrow [x'' = -g; (?x = 0; v := -cv \cup ?x \geq 0)]B(x,v) \tag{5.14*}$$

Sect. 5.4 already had a proof of (5.14) with the dynamic axioms from Chap. 5. By simply adding a sequent turnstile $\vdash$ that happens to be a sequent calculus proof, too. Instead of repeating this proof in sequent calculus style, we consider a similar property where we now include the evolution domain but leave out the discrete part:

$$A \rightarrow [x'' = -g \,\&\, x \geq 0]B(x,v) \tag{6.5}$$

To prove (6.5), we convert it to a sequent and conduct a sequent calculus proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{A,r\geq 0\vdash 0\leq r\leq r}\,\mathbb{R}\quad \dfrac{A,r\geq 0,H-\frac{g}{2}r^2\geq 0\vdash B(H-\frac{g}{2}r^2,-gt)}{A,r\geq 0,[x:=H-\frac{g}{2}r^2]x\geq 0\vdash [x:=H-\frac{g}{2}r^2]B(x,v)}\,[:=]}{A,r\geq 0,0\leq r\leq r\to [x:=H-\frac{g}{2}r^2]x\geq 0\vdash [x:=H-\frac{g}{2}r^2]B(x,v)}\,\to\mathrm{L}}{A,r\geq 0,\forall 0\leq s\leq r\,[x:=H-\frac{g}{2}s^2]x\geq 0\vdash [x:=H-\frac{g}{2}r^2]B(x,v)}\,\forall\mathrm{L}}{A,r\geq 0\vdash \forall 0\leq s\leq r\,[x:=H-\frac{g}{2}s^2]x\geq 0\to [x:=H-\frac{g}{2}r^2]B(x,v)}\,\to\mathrm{R}}{A\vdash r\geq 0\to(\forall 0\leq s\leq r\,[x:=H-\frac{g}{2}s^2]x\geq 0\to [x:=H-\frac{g}{2}r^2]B(x,v))}\,\to\mathrm{R}}{A\vdash \forall t\geq 0\,(\forall 0\leq s\leq t\,[x:=H-\frac{g}{2}s^2]x\geq 0\to [x:=H-\frac{g}{2}t^2]B(x,v))}\,\forall\mathrm{R}}{A\vdash [x''=-g\,\&\,x\geq 0]B(x,v)}\,[']}{\vdash A\to [x''=-g\,\&\,x\geq 0]B(x,v)}\,\to\mathrm{R}$$

This proof boldly stated that the first premise closes, except that

$$A,r\geq 0\vdash 0\leq r\leq r$$

is not exactly an instance of the rule id. Even here we need simple arithmetic to conclude that $0\leq r\leq r$ is equivalent to $r\geq 0$ by reflexivity and flipping sides, at which point the first premise turns into a formula that can be closed by the id rule:

$$\mathrm{id}\,\frac{*}{A,r\geq 0\vdash r\geq 0}$$

A full formal proof and a KeYmaera X proof, thus, need an extra proof step of arithmetic in the left premise (marked by rule $\mathbb{R}$). In paper proofs, we will frequently accept such minor steps as abbreviations but always take note of the reason. In the above example, we might, for example remark alongside $\mathbb{R}$ the arithmetic reason "by reflexivity of $\leq$ and flipping $0\leq r$ to $r\geq 0$".

The second remaining premise in the above proof is

$$A,r\geq 0,H-\frac{g}{2}r^2\geq 0\vdash B(H-\frac{g}{2}r^2,-gt)$$

which, when resolving abbreviations turns into

$$0\leq x\wedge x=H\wedge v=0\wedge g>0\wedge 1\geq c\geq 0,r\geq 0,H-\frac{g}{2}r^2\geq 0\vdash 0\leq H-\frac{g}{2}r^2\wedge H-\frac{g}{2}r^2\leq H$$

This sequent proves using rule $\wedge$R plus simple arithmetic for its branch

$$0\leq x\wedge x=H\wedge v=0\wedge g>0\wedge 1\geq c\geq 0,r\geq 0,H-\frac{g}{2}r^2\geq 0\vdash 0\leq H-\frac{g}{2}r^2$$

We again bite the arithmetic reason as "by flipping $0\leq H-\frac{g}{2}r^2$ to $H-\frac{g}{2}r^2\geq 0$". Some more arithmetic is needed on the respective right branch resulting from $\wedge$R:

$$0\leq x\wedge x=H\wedge v=0\wedge g>0\wedge 1\geq c\geq 0,r\geq 0,H-\frac{g}{2}r^2\geq 0\vdash H-\frac{g}{2}r^2\leq H$$

where we note the arithmetic reason "$g > 0$ and $r^2 \geq 0$". Finishing the above sequent proof up as discussed for the second premise, thus, shows that dL formula (6.5) at the conclusion of the proof is provable. This time, we have a well-structured and entirely systematic sequent calculus proof in which proof rules and axioms are only used on the top-level.

In order to make sure you do not forget why some arithmetic facts are true, you are strongly advised to write down such arithmetic reasons in your paper proofs to justify that the arithmetic is valid. KeYmaera X provides a number of ways for proving real arithmetic that will be discussed next.

## 6.5 Real Arithmetic

What, in general, can be done to prove real arithmetic? We managed to convince ourselves with ad-hoc arithmetic reasons that the simple arithmetic in the above proofs was fine. But that is neither a proper proof rule nor should we expect to get away with such simple arithmetic arguments for the full complexity of CPS.

Chapters 18 and 19 will discuss the handling of real arithmetic in much more detail. For now, the focus is on the most crucial elements for proving CPSs. Differential dynamic logic and KeYmaera X make use of a fascinating miracle: the fact that first-order logic of real arithmetic, however challenging it might sound, is perfectly decidable according to a seminal result by Alfred Tarski [23]. *First-order logic of real arithmetic* ($\text{FOL}_{\mathbb{R}}$) is the fragment of dL consisting of quantifiers over reals and propositional connectives of polynomial (or rational) term arithmetic with (real-valued) variables and rational constant symbols such as $\frac{5}{7}$, but no modalities. The most immediate way of incorporating uses of real-arithmetic reasoning into our proofs is, thus, by the rule $\mathbb{R}$ that considers as proved all the sequents whose corresponding formulas in $\text{FOL}_{\mathbb{R}}$ that are valid, which is decidable.

**Lemma 6.2 ($\mathbb{R}$ Real arithmetic).** *First-order logic of real arithmetic is decidable so that all valid facts of* $\text{FOL}_{\mathbb{R}}$ *are obtained by this proof rule:*

$$\mathbb{R}\ \frac{}{\Gamma \vdash \Delta} \qquad (\textit{if } \bigwedge_{P\in\Gamma} P \rightarrow \bigvee_{Q\in\Delta} Q \textit{ is valid in } \text{FOL}_{\mathbb{R}})$$

The proof rule $\mathbb{R}$ is remarkably different from all other proof rules we ever consider in this book. All other axioms and proof rules provide straightforward syntactic transformations that are easily implementable on a computer, for example in the theorem prover KeYmaera X [8]. The real arithmetic proof rule $\mathbb{R}$, however, has a side condition about a formula being valid in real arithmetic, which is not at all obvious how to check, but fortunately still decidable. It is the conceptually simple-most interface between proof-theoretic logic on the one side and model-theoretic algebraic decision procedures for real arithmetic on the other side. The real arithmetic

proof rule $\mathbb{R}$ proves exactly the sequents representing valid formulas in first-order real arithmetic. But the formula actually has to be in first-order real arithmetic, so cannot contain any modalities or differential equations, which are out of scope for Tarski's result.

*Example 6.2.* For example, proof rule $\mathbb{R}$ would prove the following list of sequents because they represent valid first-order real arithmetic formulas:

$$\mathbb{R}\frac{*}{\vdash x^2 \geq 0} \qquad \mathbb{R}\frac{*}{x>0 \vdash x^3>0}$$

$$\mathbb{R}\frac{*}{\vdash x>0 \leftrightarrow x^5>0} \qquad \mathbb{R}\frac{*}{a>0, b>0 \vdash y \geq 0 \rightarrow ax^2+by \geq 0}$$

But rule $\mathbb{R}$ would not prove $x^2>0 \vdash x>0$, because it is not valid. Rule $\mathbb{R}$ would not prove $x \geq 0, v>0 \vdash [x'=v]x \geq 0$, either, because it is not in pure real arithmetic.

### *6.5.1 Real Quantifier Elimination*

On the surface, proof rule $\mathbb{R}$ represents all we need to know at this stage about first-order real arithmetic. How does that miracle work, though? Without any doubt, the most complex features of first-order real arithmetic are its quantifiers. And even if a real arithmetic formula has no quantifiers, we can pretend it had by prefixing it with universal quantifiers for all free variables (forming the *universal closure*). After all, if we would like to show a formula is valid, then we need to show it is true for all values of all its variables, which semantically corresponds to having all universal quantifiers in front. That is why an understanding of first-order real arithmetic proceeds by understanding the role of quantifiers over the reals.

In a nutshell, the notation $\mathrm{QE}(P)$ denotes the use of real arithmetic reasoning on formula $P$ to obtain a formula $\mathrm{QE}(P)$ over the same free variables that is equivalent to $P$ but simpler, because $\mathrm{QE}(P)$ is quantifier-free. When starting with a first-order real arithmetic formula $P$ in which all variables are quantified, the quantifier-free equivalent $\mathrm{QE}(P)$ has no variables, so directly evaluates to either *true* or *false*.

*Example 6.3.* Real quantifier elimination yields, e.g., the following equivalence:

$$\mathrm{QE}(\exists x(ax+b=0)) \;\equiv\; (a \neq 0 \vee b=0) \tag{6.6}$$

Both sides are easily seen to be equivalent, i.e.

$$\vDash \exists x(ax+b=0) \leftrightarrow (a \neq 0 \vee b=0) \tag{6.7}$$

because a linear equation with nonzero inhomogeneous part has a solution iff its linear part is nonzero as well. And a constant equation (with $a=0$) only has a solution if $b=0$. The left-hand side of the equivalence may be hard to evaluate, because it conjectures the existence of an $x$ and it is not clear how we might get

**Expedition 6.1 (Quantifier elimination)**

One of Alfred Tarski's many seminal results from the 1930s proves quantifier elimination and decidability for real arithmetic [23].

**Definition 6.3 (Quantifier elimination).** A first-order logic theory (such as first-order logic $\text{FOL}_{\mathbb{R}}$ over the reals) admits *quantifier elimination* if, with each formula $P$, a quantifier-free formula $\text{QE}(P)$ can be associated effectively that is equivalent, i.e. $P \leftrightarrow \text{QE}(P)$ is valid (in that theory).

**Theorem 6.1 (Tarski's quantifier elimination).** *The first-order logic of real arithmetic admits quantifier elimination and is, thus, decidable.*

That is, there is an algorithm that accepts any first-order real arithmetic formula $P$ in $\text{FOL}_{\mathbb{R}}$ as input and computes a formula $\text{QE}(P)$ in $\text{FOL}_{\mathbb{R}}$ that is equivalent to $P$ but quantifier-free (and does not mention new variables or function symbols either).

The operation QE can be assumed to evaluate ground formulas (i.e., without variables) such as $\frac{1+9}{4} < 2+1$, yielding a decision procedure for closed formulas of this theory (i.e., formulas without free variables, which one obtains when forming the universal closure by prefixing the formula with universal quantifiers for all free variables). For a closed formula $P$, all it takes is to compute its quantifier-free equivalent $\text{QE}(P)$ by quantifier elimination. The closed formula $P$ is closed, so has no free variables or other free symbols, and neither will its quantifier-free equivalent $\text{QE}(P)$. Hence, $P$ as well as its equivalent $\text{QE}(P)$ are either equivalent to *true* or to *false*. Yet, $\text{QE}(P)$ is quantifier-free, so which one it is can be found out simply by evaluating the (variable-free) concrete arithmetic in $\text{QE}(P)$.

While a full account of the nuances of quantifier elimination [2, 3, 5–7, 12, 20, 22–24] is beyond the scope of this book, one useful procedure for quantifier elimination in real arithmetic will be investigated in Chaps. 18 and 19.

such a real number for $x$, since there are so many reals. The right-hand side, instead, is trivial to evaluate, because it is quantifier-free and directly says to compare the values of $a$ and $b$ to zero and that an $x$ such that $ax+b=0$ will exist if and only if $a \neq 0$ or $b=0$. This is easy to check at least if $a,b$ are either concrete numbers or fixed parameters for your CPS. Then all you need to do is make sure your choices for those parameters satisfy these constraints. If $a$ or $b$ are symbolic terms (not mentioning $x$ otherwise the equivalence (6.7) is false and QE gives a different result), then (6.7) still identifies the conditions for the existence of an $x$ such that $ax+b=0$.

*Example 6.4.* Quantifier elimination also handles universal quantifiers:

$$\text{QE}(\forall x\,(ax+b \neq 0)) \;\equiv\; (a=0 \wedge b \neq 0)$$

Again, both sides are easily seen to be equivalent, because all $x$ ensure $ax+b \neq 0$ only if $b$ is nonzero and no $x$ can cancel $b$ since $a = 0$. This proves the validity:

$$\models \forall x\,(ax+b \neq 0) \leftrightarrow (a = 0 \wedge b \neq 0)$$

Overall, if we have quantifiers, QE can remove them for us. But we first need such quantifiers. Rules ∀R,∃R,∀L,∃R went through a lot of trouble to get rid of the quantifiers in the first place. Oh my! That makes it kind of hard to eliminate them equivalently later on. Certainly the proof rules in Fig. 6.4 have not been particularly careful about eliminating quantifiers equivalently. Just think of what might happen if we did try to use rule ∃R with the wrong witness. That is certainly cheaper than quantifier elimination, but hardly as precise and useful.

Yet, if we misplaced a quantifier using the ordinary quantifier rules from Fig. 6.4, then all we need to do is to dream it up again and we are back in business for eliminating quantifiers by QE. The key to understanding how that works is to recall that the fresh (Skolem) variable symbols introduced by rule ∀R were originally universal. And, in fact, whether they were or not, we can always prove a property by proving it with an extra universal quantifier $\forall x$ around.

**Lemma 6.3 (Reintroducing universal quantifiers).** *This rule is sound:*

$$\text{i}\forall\ \frac{\Gamma \vdash \forall x P, \Delta}{\Gamma \vdash P, \Delta}$$

With the rule i∀, we can reintroduce a universal quantifier, which can then promptly be eliminated again by QE.

*Example 6.5.* Together with rule i∀, quantifier elimination can decide whether $\text{FOL}_{\mathbb{R}}$ formula $\exists x\,(ax+b=0)$ is valid. The equivalence (6.6) already indicates that there are values of $a$ and $b$ that falsify $\exists x\,(ax+b=0)$, because there are values that falsify the equivalent formula $a \neq 0 \vee b = 0$. The direct way of deciding this formula by quantifier elimination first uses i∀ for the remaining free variables $a, b$ and then handles the fully quantified universal closure by quantifier elimination to obtain a quantifier-free equivalent (with the same free variables so none):

$$\text{QE}(\forall a \forall b \exists x\,(ax+b=0)) \;\equiv\; \mathit{false}$$

So rule i∀ can reintroduce a universal quantifier, which can then be eliminated again by QE. Wait, why did it make sense to first swallow a quantifier with the lightweight rule ∀R and then later reintroduce it with rule i∀ and then eliminate it once again with the big steamroller in the form of QE?

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

It can be pretty useful to get quantifiers out of the way first using the quick rules ∀R,∃R,∀L,∃L, because other sequent rules such as propositional rules only work in the top-level, so quantifiers need to get out of the way before any other proof

rules could be applied.[7] If the formula underneath the quantifier contains modalities with hybrid programs, then that is too much to ask from QE to solve them for us as well. The key is to first get rid of quantifiers by using extra symbols, work out the proof arguments for the remaining hybrid program modalities and then reintroduce quantifiers by i$\forall$ to ask QE for the answer to the remaining real arithmetic.

*Example 6.6.* The following sequent proof illustrates how a quantifier would first be handled by rule $\forall$R, then dynamic axioms handle the modalities and finally a universal quantifier is reintroduced with rule i$\forall$ before quantifier elimination proves the resulting arithmetic. In fact, the top-most use of rule i$\forall$ also introduces a universal quantifier for $x$, which was never quantified in the original goal. All free variables are implicitly universally quantified, which fits to the fact that we seek to prove validity, so truth in all states for all real values of all variables. Besides, rule i$\forall$ can always introduce a universal quantifier to prove a formula if that succeeds.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{\vdash \forall x \forall d \left(d \geq -x \rightarrow 0 \geq 0 \wedge x+d \geq 0\right)}\,\mathbb{R}}{\vdash \forall d \left(d \geq -x \rightarrow 0 \geq 0 \wedge x+d \geq 0\right)}\,\text{i}\forall}{\vdash d \geq -x \rightarrow 0 \geq 0 \wedge x+d \geq 0}\,\text{i}\forall}{\vdash d \geq -x \rightarrow 0 \geq 0 \wedge [x:=x+d]x \geq 0}\,[:=]}{\vdash d \geq -x \rightarrow [x:=0]x \geq 0 \wedge [x:=x+d]x \geq 0}\,[:=]}{\vdash d \geq -x \rightarrow [x:=0 \cup x:=x+d]x \geq 0}\,[\cup]}{\vdash \forall d \left(d \geq -x \rightarrow [x:=0 \cup x:=x+d]x \geq 0\right)}\,\forall\text{R}$$

While this is a rather canonical proof structure, dynamic axioms can be applied anywhere. So, in this case, we could have skipped the rule $\forall$R and directly apply the dynamic axioms, bypassing also the need to reintroduce $\forall d$ by rule i$\forall$ later.

*Example 6.7.* Even if quantifier elimination handles existential quantifiers just as well as universal quantifiers, some care is needed with existential quantifiers. The additional complication is that when we turn an existential quantifier into a witness with rule $\exists$R, even with a variable as a witness, then there is no way of getting said existential quantifier back later, but only a stronger universal quantifier using rule i$\forall$. Genuine existential quantifier, though, usually cannot be proved by a universal quantifier instead, even if it would be sound to do so. That is why the following sequent proof uses dynamic axioms in the middle of the formula directly until the remaining formula is pure arithmetic such that rule $\mathbb{R}$ can handle it:

[7] The exception are contextual equivalence rules CER,CEL, which, fortunately, can even proceed within the context of a quantifier. This can be particularly helpful for existential quantifiers.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{\vdash \forall x\,(x\geq 0 \rightarrow \exists d\,(d\geq 0\wedge 0\geq 0\wedge x+d\geq 0))}\,\mathbb{R}}{\vdash x\geq 0 \rightarrow \exists d\,(d\geq 0\wedge 0\geq 0\wedge x+d\geq 0)}\,i\forall}{\vdash x\geq 0 \rightarrow \exists d\,(d\geq 0\wedge 0\geq 0\wedge [x:=x+d]x\geq 0)}\,[:=]}{\vdash x\geq 0 \rightarrow \exists d\,(d\geq 0\wedge [x:=0]x\geq 0\wedge [x:=x+d]x\geq 0)}\,[:=]}{\vdash x\geq 0 \rightarrow \exists d\,(d\geq 0\wedge [x:=0\cup x:=x+d]x\geq 0)}\,[\cup]$$

### 6.5.2 Instantiating Real Arithmetic

Real arithmetic can be very challenging. That does not come as a surprise, because cyber-physical systems and the behavior of dynamical systems themselves is challenging. On the contrary, it is pretty amazing that differential dynamic logic reduces challenging questions about CPS to just plain real arithmetic. Of course, that means that you may be left with challenging arithmetic, of quite noticeable computational complexity. This is one part where you can use your creativity to master challenging verification questions by helping the KeYmaera X prover figure them out. While there will soon be more tricks in your toolbox to overcome the challenges of arithmetic, we discuss some of them in this chapter.

Providing instantiations for quantifier rules ∃R,∀L can significantly speed up real arithmetic decision procedures. The proof in Sect. 6.4 instantiated the universal quantifier $\forall s$ for an evolution domain constraint by the end point $r$ of the time interval using quantifier proof rule ∀L. This is a very common simplification that speeds up arithmetic significantly (Note 36). It does not always work, though, because the instance one guesses may not always be the right one. Even worse, there may not always be a single instance that is sufficient for the proof.

**Note 36 (Extreme instantiation)** *The proof rule ∀L for universal quantifiers in the antecedent and the rule ∃R for existential quantifiers in the succedent allow instantiation of the quantified variable $x$ with any term $e$. Such an instantiation is very helpful if only a single instance $e$ is important for the argument.*

*For quantifiers coming from the handling of evolution domains in axiom [′] from Lemma 5.4, most uses only require a single time instance, where an extremal value for time often is all it takes. The proof steps that often help then is instantiation of the intermediate time $s$ by the end time $t$:*

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overset{*}{\overline{\mathbb{R}\ \Gamma,t\geq 0 \vdash 0\leq t\leq t,\ldots}} \qquad \overset{\ldots}{\overline{\Gamma,t\geq 0,q(y(t)) \vdash [x:=y(t)]p(x)}}}{\Gamma,t\geq 0,0\leq t\leq t \to q(y(t)) \vdash [x:=y(t)]p(x)}\,{\to}L}{\Gamma,t\geq 0,\forall 0\leq s\leq t\, q(y(s)) \vdash [x:=y(t)]p(x)}\,\forall L}{\Gamma,t\geq 0 \vdash (\forall 0\leq s\leq t\, q(y(s))) \to [x:=y(t)]p(x)}\,{\to}R}{\Gamma \vdash t\geq 0 \to \big((\forall 0\leq s\leq t\, q(y(s))) \to [x:=y(t)]p(x)\big)}\,{\to}R}{\Gamma \vdash \forall t\geq 0\, \big((\forall 0\leq s\leq t\, q(y(s))) \to [x:=y(t)]p(x)\big)}\,\forall R}{\Gamma \vdash [x' = f(x)\,\&\,q(x)]p(x)}\,[']$$

*This happens so frequently that KeYmaera X defaults to just using this instantiation. Similar instantiations can simplify arithmetic in other cases as well.*

### 6.5.3 Weakening Real Arithmetic

It can be very useful to just drop arithmetic assumptions that are irrelevant for the proof to make sure they are no distraction for real arithmetic decision procedures.

In the proof in Sect. 6.4, the left premise was

$$A, r\geq 0 \vdash 0\leq r\leq r$$

The proof of this sequent did not make use of $A$ at all. Here, the proof worked easily. But if $A$ were a very complicated formula, then proving the same sequent might have been very difficult, because our proving attempts could have been distracted by the presence of $A$ and all the lovely assumptions it provides. We might have applied lots of proof rules to $A$ before finally realizing that the sequent proves because of $r\geq 0 \vdash 0\leq r\leq r$ alone.

While quantifier elimination is not based on applying propositional proof rules, unnecessary assumptions can still cause considerable distraction [15, Chapter 5]. Think of how much easier it is to see that $ax^2+bx\geq 0$ is true if somebody only tells you the relevant assumptions $a\geq 0, bx\geq 0$ rather than listing a lot of other true but presently useless assumptions about the values of $a,b$ and $x$. Consequently, it often saves a lot of proof effort to simplify irrelevant assumptions away as soon as they have become unnecessary. Fortunately, sequent calculus already comes with a general-purpose proof rule for the job called weakening (WL,WR that will be elaborated in Sect. 6.5.4), which we can use on our example from the left premise in the proof of Sect. 6.4 to remove the assumption $A$:

$$\dfrac{r\geq 0 \vdash 0\leq r\leq r}{A, r\geq 0 \vdash 0\leq r\leq r}\,\mathrm{WL}$$

**Note 37 (Occam's assumption razor)** *Think how hard it would be to prove a theorem with all the facts in all books of mathematics as assumptions. Compared to a proof from just the two facts that matter for that proof.*

You are generally advised to get rid of assumptions that you no longer need. This will help you manage the relevant facts about your CPS, will make sure you stay on top of your CPS agenda, and will also help the arithmetic in KeYmaera X to succeed much quicker. Just be careful not to hide an assumption that you still need. But if you accidentally do, then that alone can also be a valuable insight, because you just found out what the safety of your system critically depends on.

Finally recall how the real arithmetic proof of the first premise in Note 36 did not need the potentially long list of unnecessary assumptions in $\Gamma$. And, in fact, the proof also weakened away the modal formula $[x:=y(t)]p(x)$ from the sequent with WR to make the sequent arithmetic and amenable to real arithmetic rule $\mathbb{R}$.

### 6.5.4 Structural Proof Rules

The antecedent and succedent of a sequent are considered as sets. That implies that the order of formulas is irrelevant, and we implicitly adopt what is called the *exchange rule* and do not distinguish between the following two sequents

$$\Gamma, A, B \vdash \Delta \qquad \text{and} \qquad \Gamma, B, A \vdash \Delta$$

ultimately since $A \wedge B$ and $B \wedge A$ are equivalent. Nor do we distinguish between

$$\Gamma \vdash C, D, \Delta \qquad \text{and} \qquad \Gamma \vdash D, C, \Delta$$

ultimately since $C \vee D$ and $D \vee C$ are equivalent. Antecedent and succedent are considered as sets, not multisets, so we implicitly adopt what is called the *contraction rule* and do not distinguish between the following two sequents

$$\Gamma, A, A \vdash \Delta \qquad \text{and} \qquad \Gamma, A \vdash \Delta$$

because $A \wedge A$ and $A$ are equivalent. It does not matter whether we make an assumption $A$ once or multiple times. Nor do we distinguish between

$$\Gamma \vdash C, C, \Delta \qquad \text{and} \qquad \Gamma \vdash C, \Delta$$

because $C \vee C$ and $C$ are equivalent. We could adopt these exchange rules and contraction rules explicitly, but usually leave them implicit:

$$\text{PR}\ \frac{\Gamma \vdash Q, P, \Delta}{\Gamma \vdash P, Q, \Delta} \qquad \text{cR}\ \frac{\Gamma \vdash P, P, \Delta}{\Gamma \vdash P, \Delta}$$

$$\text{PL}\ \frac{\Gamma, Q, P \vdash \Delta}{\Gamma, P, Q \vdash \Delta} \qquad \text{cL}\ \frac{\Gamma, P, P \vdash \Delta}{\Gamma, P \vdash \Delta}$$

The only structural rule of sequent calculus that we will find reason to use explicitly in practice is the *weakening* proof rule (alias *hide* rule) that can be used to remove formulas from the antecedent (WL) or succedent (WR), respectively:

$$\text{WR}\ \frac{\Gamma \vdash \Delta}{\Gamma \vdash P, \Delta}$$

$$\text{WL}\ \frac{\Gamma \vdash \Delta}{\Gamma, P \vdash \Delta}$$

Weakening rules are sound, since it is always fine to prove a sequent with more formulas in the antecedent or succedent by a proof that uses only some of those formulas. Proof rule WL proves the conclusion $\Gamma, P \vdash \Delta$ from the premise $\Gamma \vdash \Delta$, which dropped the assumption $P$. Surely, if premise $\Gamma \vdash \Delta$ is valid, then conclusion $\Gamma, P \vdash \Delta$ is valid as well, because it even has one more (unused) assumption available, namely $P$. Proof rule WR proves the conclusion $\Gamma \vdash P, \Delta$ from the premise $\Gamma \vdash \Delta$, which is fine because $\Gamma \vdash \Delta$ just has one less (disjunctive) option in its succedent. To see why that is sound, recall the disjunctive meaning of succedents.

At first sight, weakening may sound like a stupid thing to do in any proof, because rule WL discards available assumptions ($P$ in the antecedent) and rule WR discards available options ($P$ in the succedent) for proving the statement. This seems to make it harder to prove the statement after using a weakening rule. But weakening is actually useful for managing computational and conceptual proof complexity by enabling us to throw away irrelevant assumptions. These assumptions may have been crucial for another part of the proof, but have just become irrelevant for the particular sequent at hand, which can, thus, be simplified to $\Gamma \vdash \Delta$. Weakening, thus, streamlines proofs, which also helps speed up arithmetic immensely (Sect. 6.5.3).

Of course, the opposite of the weakening rules would be terribly unsound. We cannot just invent extra assumptions out of thin air just because we feel like wanting to have them at our disposal. But once we have the assumptions, we are free to not use them. That is, the premise of WL implies the conclusion but *not* vice versa.

### 6.5.5 Substituting Equations

If we have an equation $x = e$ among our assumptions (in the antecedent), it is often significantly more efficient to use that equation for substituting $e$ for all other occurrences of $x$ instead of waiting for a real arithmetic decision procedure to figure this out. If we have $x = e$ among our assumptions, then any (free) occurrence of $x$ can be replaced by $e$, both in the succedent as well as in the antecedent:

$$=\text{R}\ \frac{\Gamma, x=e \vdash p(e), \Delta}{\Gamma, x=e \vdash p(x), \Delta} \qquad =\text{L}\ \frac{\Gamma, x=e, p(e) \vdash \Delta}{\Gamma, x=e, p(x) \vdash \Delta}$$

It would be okay to use the equation in the other direction for replacing all occurrences of $e$ by $x$, because the equation $e=x$ is equivalent to $x=e$ by symmetry. Both proof rules, =R and =L apply an equation $x=e$ from the antecedent to an occurrence of $x$ in the antecedent or succedent to substitute $e$ for $x$. By using the proof rule sufficiently often, multiple occurrences of $x$ in $\Gamma$ and $\Delta$ can be substituted. Especially if $x$ does not occur in $e$, then using the proof rules =R,=L exhaustively and weakening $x=e$ away by rule WL removes the variable $x$ entirely, which is what quantifier elimination will otherwise have to achieve by a complex algorithm.

Quantifier elimination would have been able to prove the same fact, but with significantly more time and effort. So you are advised to exploit these proof shortcuts whenever you spot them. Of course, KeYmaera X is clever enough to spot certain uses of equality rewriting as well, but you may be a better judge of how you would like to structure your proof, because you are more familiar with your CPS of interest.

### 6.5.6 Abbreviating Terms

The opposite of exhaustively substituting in equations by rules =L,=R can also be helpful sometimes. When there are complicated terms whose precise relation to the other variables is not important, a new variable can be introduced as an abbreviation for the complicated term.

For example, the following sequent looks complicated but becomes easy when abbreviating all occurrences of the complex term $\frac{a}{2}t^2+vt+x$ by a new variable $z$:

$$a \geq 0, v \geq 0, t \geq 0, 0 \leq \underbrace{\frac{a}{2}t^2+vt+x}_{z}, \underbrace{\frac{a}{2}t^2+vt+x}_{z} \leq d, d \leq 10 \vdash \underbrace{\frac{a}{2}t^2+vt+x}_{z} \leq 10$$

The sequent resulting from that abbreviation lost how exactly the value of the new variable $z$ relates to the values of $a,t,v,x$ but exposes the simple transitivity argument that easily proves the sequent by rule $\mathbb{R}$:

$$a \geq 0, v \geq 0, t \geq 0, 0 \leq z, z \leq d, d \leq 10 \vdash z \leq 10$$

A proof rule for introducing such abbreviations will be investigated in Chap. 12.

### 6.5.7 Creatively Cutting Real Arithmetic

Weakening is not the only propositional proof rule that can help accelerate arithmetic. The cut rule is not just a logical curiosity, but can actually be shockingly

helpful in practice [4]. It can speed up real arithmetic a lot when using a cut to replace a difficult arithmetic formula by a simpler one that is sufficient for the proof.

For example, suppose $p(x)$ is a big and very complicated formula of first-order real arithmetic. Then proving the following formula

$$(x-y)^2 \leq 0 \land p(y) \rightarrow p(x)$$

by real arithmetic will turn out to be surprisingly difficult and can take ages (even if it ultimately terminates). Yet, upon closure inspection, $(x-y)^2 \leq 0$ implies that $y = x$, which makes the rest of the proof easy since, $p(y)$ easily implies $p(x)$ if, indeed, $x = y$. How do we exhibit a proof based on these thoughts?

The critical idea for such a proof work is to use a creative cut with the suitable arithmetic. Choosing $x = y$ as the cut formula $C$, we use rule cut and proceed:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{(x-y)^2 \leq 0 \vdash x = y}\,\mathbb{R}}{(x-y)^2 \leq 0 \vdash x = y, p(x)}\,\text{WR}}{(x-y)^2 \leq 0, p(y) \vdash x = y, p(x)}\,\text{WL} \qquad \dfrac{\dfrac{*}{p(y), x = y \vdash p(y)}\,\text{id}}{p(y), x = y \vdash p(x)}\,\text{=R}}{(x-y)^2 \leq 0, p(y), x = y \vdash p(x)}\,\text{WL}}{(x-y)^2 \leq 0, p(y) \vdash p(x)}\,\text{cut}}{(x-y)^2 \leq 0 \land p(y) \vdash p(x)}\,\land\text{L}}{\vdash (x-y)^2 \leq 0 \land p(y) \rightarrow p(x)}\,\rightarrow\text{R}$$

Indeed, the left premise proves easily using real arithmetic. The right premise proves comparably easily as well by the equality substitution proof rule =R and rule id. Observe that proofs like this one benefit substantially from weakening to get rid of superfluous assumptions, thereby simplifying the resulting arithmetic.

## 6.6 Summary

The differential dynamic logic sequent proof rules from this chapter are summarized in Fig. 6.5. They are sound [14, 19]. There are further proof rules of differential dynamic logic that later chapters will examine [14, 16, 17, 19], but this chapter laid a rock-solid foundation for CPS verification. In addition to having seen the foundation and working principles of how systematic CPS proofs assemble arguments, this chapter discussed techniques to tame the complexity of real arithmetic.

## Exercises

**6.1.** Prove soundness of the following special-purpose proof rule from p. 188 and use it to continue the proof in Fig. 6.3 similar to the proof in Fig. 6.2:

$$\neg\text{R}\ \frac{\Gamma, P \vdash \Delta}{\Gamma \vdash \neg P, \Delta} \qquad \wedge\text{R}\ \frac{\Gamma \vdash P, \Delta \quad \Gamma \vdash Q, \Delta}{\Gamma \vdash P \wedge Q, \Delta} \qquad \vee\text{R}\ \frac{\Gamma \vdash P, Q, \Delta}{\Gamma \vdash P \vee Q, \Delta}$$

$$\neg\text{L}\ \frac{\Gamma \vdash P, \Delta}{\Gamma, \neg P \vdash \Delta} \qquad \wedge\text{L}\ \frac{\Gamma, P, Q \vdash \Delta}{\Gamma, P \wedge Q \vdash \Delta} \qquad \vee\text{L}\ \frac{\Gamma, P \vdash \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \vee Q \vdash \Delta}$$

$$\rightarrow\text{R}\ \frac{\Gamma, P \vdash Q, \Delta}{\Gamma \vdash P \rightarrow Q, \Delta} \qquad \text{id}\ \frac{}{\Gamma, P \vdash P, \Delta} \qquad \top\text{R}\ \frac{}{\Gamma \vdash \mathit{true}, \Delta} \qquad \text{WR}\ \frac{\Gamma \vdash \Delta}{\Gamma \vdash P, \Delta}$$

$$\rightarrow\text{L}\ \frac{\Gamma \vdash P, \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \rightarrow Q \vdash \Delta} \qquad \text{cut}\ \frac{\Gamma \vdash C, \Delta \quad \Gamma, C \vdash \Delta}{\Gamma \vdash \Delta} \qquad \bot\text{L}\ \frac{}{\Gamma, \mathit{false} \vdash \Delta} \qquad \text{WL}\ \frac{\Gamma \vdash \Delta}{\Gamma, P \vdash \Delta}$$

$$\forall\text{R}\ \frac{\Gamma \vdash p(y), \Delta}{\Gamma \vdash \forall x\, p(x), \Delta}\ (y \notin \Gamma, \Delta, \forall x\, p(x)) \qquad \exists\text{R}\ \frac{\Gamma \vdash p(e), \Delta}{\Gamma \vdash \exists x\, p(x), \Delta}$$

$$\forall\text{L}\ \frac{\Gamma, p(e) \vdash \Delta}{\Gamma, \forall x\, p(x) \vdash \Delta} \qquad \exists\text{L}\ \frac{\Gamma, p(y) \vdash \Delta}{\Gamma, \exists x\, p(x) \vdash \Delta}\ (y \notin \Gamma, \Delta, \exists x\, p(x))$$

$$\text{CER}\ \frac{\Gamma \vdash C(Q), \Delta \quad \vdash P \leftrightarrow Q}{\Gamma \vdash C(P), \Delta} \qquad =\text{R}\ \frac{\Gamma, x = e \vdash p(e), \Delta}{\Gamma, x = e \vdash p(x), \Delta}$$

$$\text{CEL}\ \frac{\Gamma, C(Q) \vdash \Delta \quad \vdash P \leftrightarrow Q}{\Gamma, C(P) \vdash \Delta} \qquad =\text{L}\ \frac{\Gamma, x = e, p(e) \vdash \Delta}{\Gamma, x = e, p(x) \vdash \Delta}$$

**Fig. 6.5** Proof rules of the dL sequent calculus considered in this chapter

$$\text{R1}\ \frac{\Gamma, \theta > 0 \vdash \Delta}{\Gamma, -(-\theta) > 0 \vdash \Delta}$$

**6.2 (*).** Since we are not adding proof rule R1 from p. 188 to the dL proof calculus, show how you can derive the same proof step using a creative combination of arithmetic and the other proof rules.

**6.3.** The sequent calculus proof in Fig. 6.2 proves the following dL formula

$$v^2 \leq 10 \wedge b > 0 \rightarrow b > 0 \wedge (\neg(v \geq 0) \vee v^2 \leq 10)$$

Its proof only used propositional sequent calculus rules and no arithmetic or dynamic axioms. What does that mean about the validity of the following formula of the same propositional structure?

$$x^5 = y^2 + 5 \wedge a^2 > c^2 \rightarrow a^2 > c^2 \wedge (\neg(z < x^2) \vee x^5 = y^2 + 5)$$

**6.4 (Bouncing ball sequent proof).** Using just dL axioms and arithmetic, Sect. 5.4 showed a proof of a single-hop bouncing ball formula:

$$0 \leq x \wedge x = H \wedge v = 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \rightarrow \\ \left[\{x' = v, v' = -g\}; (?x = 0; v := -cv \cup ?x \geq 0)\right](0 \leq x \wedge x \leq H) \quad (5.14^*)$$

What is the minimal change needed to be changed to make this proof a proof in sequent calculus? Also conduct a sequent calculus proof for formula (5.14) that only applies proof rules and axioms at the top-level.

**6.5.** Could we have used the following proof rule for $\wedge$ instead of rule $\wedge$R? Is it sound? Does it have any advantages or disadvantages compared to rule $\wedge$R?

$$\frac{\Gamma \vdash P,\Delta \quad \Gamma,P \vdash Q,\Delta}{\Gamma \vdash P \wedge Q,\Delta}$$

**6.6 (Propositional soundness).** Prove soundness for the structural and propositional sequent proof rules considered in Fig. 6.1.

**6.7.** Without alluding to dynamic axiom $[\cup]$ or contextual equivalence CER, give a direct soundness proof for the following sequent proof rules

$$[\cup]R\ \frac{\Gamma \vdash [\alpha]P \wedge [\beta]P,\Delta}{\Gamma \vdash [\alpha\cup\beta]P,\Delta} \qquad [\cup]R2\ \frac{\Gamma \vdash [\alpha]P,\Delta \quad \Gamma \vdash [\beta]P,\Delta}{\Gamma \vdash [\alpha\cup\beta]P,\Delta}$$

$$[\cup]L\ \frac{\Gamma,[\alpha]P \wedge [\beta]P \vdash \Delta}{\Gamma,[\alpha\cup\beta]P \vdash \Delta} \qquad [\cup]L2\ \frac{\Gamma,[\alpha]P,[\beta]P \vdash \Delta}{\Gamma,[\alpha\cup\beta]P \vdash \Delta}$$

**6.8 (dL sequent proof rules).** Develop dynamic sequent calculus proof rules for the modalities similar to either the rules $[\cup]R$ and $[\cup]L$ that this chapter discussed briefly but did not pursue or similar to the rules $[\cup]R2$ and $[\cup]L2$ from Exercise 6.7. Prove soundness for these sequent calculus proof rules. You can use a general argument how soundness of the dynamic sequent proof rules follows from soundness of the dL axioms considered in Chap. 5, but you first need to prove soundness of those dL axioms (Exercise 5.11).

**6.9.** If we define the formula *true* as $1 > 0$ and the formula *false* as $1 > 2$, then are the proof rules $\top$R and $\bot$L derivable from the other proof rules?

**6.10.** Let $y(t)$ be the solution at time $t$ of the differential equation $x' = f(x)$ with initial value $y(0) = x$. Show that the following sequent proof rule, which checks the evolution domain $q(x)$ at the end, is sound:

$$\frac{\Gamma \vdash \forall t{\geq}0\,\big([x{:=}y(t)](q(x) \rightarrow p(x))\big),\Delta}{\Gamma \vdash [x' = f(x)\,\&\,q(x)]p(x),\Delta}$$

Would the following also be a sound axiom? Prove or disprove.

$$[x' = f(x)\,\&\,Q]P \leftrightarrow \forall t{\geq}0\,\big([x{:=}y(t)](Q \rightarrow P)\big)$$

Is the following sequent proof rule sound, which checks the evolution domain $q(x)$ in the beginning and in the end?

$$\frac{\Gamma \vdash \forall t{\geq}0\,\big(q(x) \rightarrow [x{:=}y(t)](q(x) \rightarrow p(x))\big),\Delta}{\Gamma \vdash [x' = f(x)\,\&\,q(x)]p(x),\Delta}$$

**6.11 (*).** Generalize the solution axiom schema $[']$ from Chap. 5 for differential equations to the case of differential equation systems:

$$x_1' = e_1, .., x_n' = e_n \,\&\, Q$$

First consider the easier case where $Q \equiv \mathit{true}$ and $n = 2$.

**6.12.** Sect. 5.2 argued why the following proof rule is sound

$$\text{HM;}\ \frac{A \to [\alpha]E \quad E \to [\beta]B}{A \to [\alpha;\beta]B}$$

where a proof rule is sound if validity of all premises implies validity of the conclusion. Prove that rule HM; is indeed sound. Would the following be a sound axiom? Or can you find a counterexample?

$$[\alpha;\beta]B \leftrightarrow ([\alpha]E) \wedge (E \to [\beta]B)$$

**6.13.** By Sect. 6.5.1, quantifier elimination can be used to show the equivalence:

$$\mathrm{QE}(\exists x\,(ax+b=0)) \ \equiv\ (a \neq 0 \vee b = 0) \tag{6.6*}$$

What is the result of applying quantifier elimination to $\exists x\,(ax^2+bx+c=0)$ instead?

**6.14 (Derived propositional rules).** Prove that the following rules are derived rules:

$$\text{cutR}\ \frac{\Gamma \vdash Q, \Delta \quad \Gamma \vdash Q \to P, \Delta}{\Gamma \vdash P, \Delta}$$

$$\text{cutL}\ \frac{\Gamma, Q \vdash \Delta \quad \Gamma \vdash P \to Q, \Delta}{\Gamma, P \vdash \Delta}$$

## *References*


1. Andrews, P. B. *An Introduction to Mathematical Logic and Type Theory: To Truth Through Proof* 2nd (Kluwer, 2002).
2. Basu, S., Pollack, R. & Roy, M.-F. *Algorithms in Real Algebraic Geometry* 2nd. doi:10.1007/3-540-33099-2 (Springer, 2006).
3. Bochnak, J., Coste, M. & Roy, M.-F. *Real Algebraic Geometry* (Springer, 1998).
4. Boolos, G. Don't eliminate cut. *Journal of Philosophical Logic.* doi:10.1007/BF00247711 (1984).
5. Collins, G. E. *Hauptvortrag: Quantifier elimination for real closed fields by cylindrical algebraic decomposition.* in *Automata Theory and Formal Languages* (ed Barkhage, H.) **33** (Springer, 1975), 134–183.
6. Collins, G. E. & Hong, H. Partial Cylindrical Algebraic Decomposition for Quantifier Elimination. *J. Symb. Comput.* **12,** 299–328 (1991).
7. Davenport, J. H. & Heintz, J. Real Quantifier Elimination is Doubly Exponential. *J. Symb. Comput.* **5,** 29–35 (1988).

8. Fulton, N., Mitsch, S., Quesel, J.-D., Völp, M. & Platzer, A. *KeYmaera X: An Axiomatic Tactical Theorem Prover for Hybrid Systems* in *CADE* (eds Felty, A. & Middeldorp, A.) **9195** (Springer, 2015), 527–538. doi:10.1007/978-3-319-21401-6_36.
9. Gentzen, G. Untersuchungen über das logische Schließen. I. *Math. Zeit.* **39,** 176–210 (1935).
10. Gentzen, G. Untersuchungen über das logische Schließen. II. *Math. Zeit.* **39,** 405–431 (1935).
11. Herbrand, J. Recherches sur la théorie de la démonstration. *Travaux de la Société des Sciences et des Lettres de Varsovie, Class III, Sciences Mathématiques et Physiques* **33,** 33–160 (1930).
12. Jovanovic, D. & de Moura, L. M. *Solving Non-linear Arithmetic* in *Automated Reasoning - 6th International Joint Conference, IJCAR 2012, Manchester, UK, June 26-29, 2012. Proceedings* (eds Gramlich, B., Miller, D. & Sattler, U.) **7364** (Springer, 2012), 339–354.
13. *Proceedings of the 27th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2012, Dubrovnik, Croatia, June 25–28, 2012* (IEEE, 2012).
14. Platzer, A. Differential Dynamic Logic for Hybrid Systems. *J. Autom. Reas.* **41,** 143–189 (2008).
15. Platzer, A. *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics* doi:10.1007/978-3-642-14509-4 (Springer, Heidelberg, 2010).
16. Platzer, A. *Logics of Dynamical Systems* in *LICS* (IEEE, 2012), 13–24. doi:10.1109/LICS.2012.13.
17. Platzer, A. *The Complete Proof Theory of Hybrid Systems* in *LICS* (IEEE, 2012), 541–550. doi:10.1109/LICS.2012.64.
18. Platzer, A. Differential Game Logic. *ACM Trans. Comput. Log.* **17,** 1:1–1:51 (2015).
19. Platzer, A. A Complete Uniform Substitution Calculus for Differential Dynamic Logic. *J. Autom. Reas.* doi:10.1007/s10817-016-9385-1 (2016).
20. Seidenberg, A. A New Decision Method for Elementary Algebra. *Annals of Mathematics* **60,** 365–374 (1954).
21. Skolem, T. Logisch-kombinatorische Untersuchungen über die Erfüllbarkeit oder Beweisbarkeit mathematischer Sätze nebst einem Theorem über dichte Mengen. *Videnskapsselskapet Skrifter, I. Matematisk-naturvidenskabelig Klasse* **6,** 1–36 (1920).
22. Stengle, G. A Nullstellensatz and a Positivstellensatz in semialgebraic geometry. *Math. Ann.* **207,** 87–97 (1973).
23. Tarski, A. *A Decision Method for Elementary Algebra and Geometry* 2nd (University of California Press, Berkeley, 1951).
24. Weispfenning, V. Quantifier Elimination for Real Algebra — the Quadratic Case and Beyond. *Appl. Algebra Eng. Commun. Comput.* **8,** 85–101 (1997).