15-424: Foundations of Cyber-Physical Systems

Lecture Notes on Truth & Proof

André Platzer

Carnegie Mellon University

Lecture 6

1 Introduction

[1] Lecture 5 investigated dynamic axioms for dynamical systems, i.e. axioms in differential dynamic logic ($\mathsf{d}\mathcal{L}$) that characterize operators of the dynamical systems that $\mathsf{d}\mathcal{L}$ describes by hybrid programs in terms of structurally simpler $\mathsf{d}\mathcal{L}$ formulas. That lecture did not show all important axioms yet, but still showed enough to prove a property of a bouncing ball. Yet, there's more to proofs than just axioms. Proofs also have proof rules for combining fragments of arguments into a bigger proof by proof steps.

Recall that our proof about the (single-hop) bouncing ball still suffered from at least two issues. It was a sound proof and an interesting proof. But the way we had come up with the proof was somewhat undisciplined, because we just applied axioms seemingly at random at all kinds of places all over the logical formulas. After we see such a proof, that is not a concern. But better structuring would help us find proofs more constructively. The second issue was that the axioms for the dynamics that Lecture 5 showed us did not actually help in proving the propositional logic and arithmetic parts.

The lecture today 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 $\land, \lor, \rightarrow$) and quantifiers $\forall, \exists$). As part of the structuring, we will make ample and crucial use of the dynamic axioms from Lecture 5. Yet, they will be used in a more structured way than so far.

These notes are based on [Pla08, Pla10, Chapter 2.5.2], where more information can be found in addition to more information in [Pla10, Appendix A]. Sequent calculus is

[1] By both sheer coincidence and by higher reason, the title of this lecture turns out to be closely related to the subtitle of a well-known book on mathematical logic [And02], which summarizes the philosophy we pursue here in a way that is impossible to improve upon any further: *To truth through proof.*

discussed in more detail also in the handbook of proof theory [Bus98]. More resources and background material on first-order logic is also listed on the course web page.

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 truth of a logical formula. In practice, this is usually less feasible, 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 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. The same matter is even more difficult for the hybrid dynamics involved in modalities of differential dynamic logic formulas, because hybrid systems have so many possible behaviors.

Yet, we are still interested in establishing whether a logical formula is true. Or, actually, whether the formula is valid, since truth of a logical formula depends on the state (cf. definition of $\nu \models \phi$ in Lecture 4) whereas validity of a logical formula is independent of the state (cf. definition of $\vDash \phi$), because validity means truth in all states.

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. This finite syntactical argument represented in a proof witnesses validity of a logical formula. Proofs can be produced in a machine. They can be stored to be recalled as witnesses and evidence for the validity of their conclusion. And they can be checked by humans or machines for correctness. They can also be inspected for analytic insights about the reasons for the validity of a formula, which goes beyond the 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.

Truth and proof should be related intimately, because we would only want to accept proofs that imply truth, i.e. proofs that imply their consequences to be valid if their premises are. That is, proof systems should be sound to be reliable. The converse question is that of completeness, whether all true formulas (again in the sense of valid) can be proved, which turns out to be much more subtle.

3 Sequents

Sequent calculus was originally developed by Gerhard Gentzen [Gen35] for studying properties of natural deduction calculi. Sequent calculus has been used very successfully for numerous other purposes since.

Sequents are essentially a standard form for logical formulas that is convenient for proving purposes.

Note 1. *A* sequent *is of the form* $\Gamma \vdash \Delta$*, where the* antecedent Γ *and* succedent Δ *are finite sets of formulas. The semantics of* $\Gamma \vdash \Delta$ *is that of the formula* $\bigwedge_{\phi\in\Gamma} \phi \to \bigvee_{\psi\in\Delta} \psi$*.*

For quantifier elimination rules, we will later make use of this fact by considering sequent $\Gamma \vdash \Delta$ as an abbreviation for the latter formula. Empty conjunctions are equivalent to $true$. Empty disjunctions are equivalent to $false$. Hence, the sequent $\vdash A$ means the same as the formula A. The empty sequent $\vdash$ means the same as the formula $false$.

The antecedent Γ can be thought of as the formulas we assume to be true, whereas the succedent Δ can be understood as formulas for which we want to show that at least one of them is true assuming all formulas of Γ are true. So for proving a sequent $\Gamma \vdash \Delta$, we assume all Γ and want to show that one of the Δ is true. For some simple sequents like $\Gamma, \phi \vdash \phi, \Delta$, we directly know that they are valid, because we can certainly show ϕ if we assume ϕ (in fact, we will use this as an axiom). 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 antecedent and succedent of a sequent are considered as sets. So the order of formulas is irrelevant, so we implicitly adopt what is called the *exchange rule* and do not distinguish between the following two sequents

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

nor do we distinguish between

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

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

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

nor do we distinguish between

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

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

$$\text{(Wr)}\ \frac{\Gamma \vdash \Delta}{\Gamma \vdash \phi, \Delta}$$

$$\text{(Wl)}\ \frac{\Gamma \vdash \Delta}{\Gamma, \phi \vdash \Delta}$$

Weakening rules are sound, since it is fine in structural logics to prove a sequent with more formulas in the antecedent or succedent by a proof that uses only some of those formulas. This is different in substructural logics such as linear logic.

$$(\neg r)\ \frac{\Gamma, \phi \vdash \Delta}{\Gamma \vdash \neg\phi, \Delta} \qquad (\vee r)\ \frac{\Gamma \vdash \phi, \psi, \Delta}{\Gamma \vdash \phi \vee \psi, \Delta} \qquad (\wedge r)\ \frac{\Gamma \vdash \phi, \Delta \quad \Gamma \vdash \psi, \Delta}{\Gamma \vdash \phi \wedge \psi, \Delta}$$

$$(\neg l)\ \frac{\Gamma \vdash \phi, \Delta}{\Gamma, \neg\phi \vdash \Delta} \qquad (\vee l)\ \frac{\Gamma, \phi \vdash \Delta \quad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \vee \psi \vdash \Delta} \qquad (\wedge l)\ \frac{\Gamma, \phi, \psi \vdash \Delta}{\Gamma, \phi \wedge \psi \vdash \Delta}$$

$$(\rightarrow r)\ \frac{\Gamma, \phi \vdash \psi, \Delta}{\Gamma \vdash \phi \rightarrow \psi, \Delta} \qquad (ax)\ \frac{}{\Gamma, \phi \vdash \phi, \Delta}$$

$$(\rightarrow l)\ \frac{\Gamma \vdash \phi, \Delta \quad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \rightarrow \psi \vdash \Delta} \qquad (cut)\ \frac{\Gamma \vdash \phi, \Delta \quad \Gamma, \phi \vdash \Delta}{\Gamma \vdash \Delta}$$

Figure 1: Propositional proof rules of sequent calculus

4 Propositional Proof Rules

For propositional logic, standard propositional rules ¬r–*cut* with the cut rule are listed in Fig. 1. They decompose the propositional structure of formulas. Rules ¬r and ¬l use simple dualities caused by the implicative semantics of sequents. Essentially, instead of showing $\neg\phi$ in the succedent, we assume the contrary ϕ in the antecedent with rule ¬r. In rule ¬l, instead of assuming $\neg\phi$ in the antecedent, we show the contrary ϕ in the succedent. Rule ∨r uses the fact that formulas are combined disjunctively in succedents, rule ∧l that they are conjunctive in antecedents. The comma between formulas in an antecedent has the same effect as a conjunction, and the comma between formulas in the succedent has the same effect as a disjunction. Rules ∨l and ∧r split the proof into two cases, because conjuncts in the succedent can be proven separately (∧r) and, dually, disjuncts of the antecedent can be assumed separately (∨l). For ∧r we want to show conjunction $\phi \wedge \psi$, so in the left branch we proceed to show $\Gamma \vdash \phi, \Delta$ and, in addition, in the right branch we show $\Gamma \vdash \psi, \Delta$, which, together, entail $\Gamma \vdash \phi \wedge \psi, \Delta$. If, as in rule ∨l, we assume disjunction $\phi \vee \psi$ as part of the antecedent, then we do not know if we can assume ϕ to hold or if we can assume ψ to hold in the antecedent, but know only that one of them holds. Hence, as in a case distinction, ∨l considers both cases, the case where we assume ϕ in the antecedent, and the case where we assume ψ. If both subgoals can be proven, this entails $\Gamma, \phi \vee \psi \vdash \Delta$. Rules →r and →l can be derived from the equivalence of $\phi \rightarrow \psi$ and $\neg\phi \vee \psi$. Rule →r uses the fact that implication → has the same meaning as the sequent arrow ⊢ of a sequent. Intuitively, to show implication $\phi \rightarrow \psi$, rule →r assumes ϕ (in the antecedent) and shows ψ (in the succedent). Rule →l assumes an implication $\phi \rightarrow \psi$ to hold in the antecedent, but we do not know if this implication holds because ϕ is false, or because ψ is true, so →l splits into those two branches.

The axiom rule ax closes a goal (there are no further subgoals, which we sometimes mark $*$ explicitly), because assumption ϕ in the antecedent trivially entails ϕ in the succedent (sequent $\Gamma, \phi \vdash \phi, \Delta$ is a simple syntactic tautology).

Rule *cut* is the *cut* rule that can be used for case distinctions: The right subgoal assumes any additional formula ϕ in the antecedent that the left subgoal shows in the succedent. Dually: regardless of whether ϕ is actually true or false, both cases are covered by proof branches. 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 theory. But in practice, complex practical applications make use of cuts for efficiency reasons. Cuts an be used, for example, to simplify arithmetic.

Even though we write sequent rules as if the principal formula (like $\phi \land \psi$ in $\land$r,$\land$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.

5 Proofs

The d$\mathcal{L}$ calculus has further proof rules. But before investigating those, let us first understand already what a proof is and what it means to prove a logical formula. The same notion of proof and provability works for propositional logic as it does for differential dynamic logic, except that the latter has more proof rules.[2]

A formula ϕ is provable or derivable (in the d$\mathcal{L}$ calculus) if we can find a d$\mathcal{L}$ proof for it that starts with axioms (rule ax) at the leaves and ends with a sequent $\vdash \phi$ at the bottom and that has only used d$\mathcal{L}$ proof rules in between. While constructing proofs, however, we would start with the desired goal $\vdash \phi$ at the bottom and work our way backwards to the subgoals until they can be proven to be valid as axioms (ax). Once all subgoals have been proven to be valid axioms, they entail their consequences, which, recursively, entail the original goal $\vdash \phi$. This property of preserving truth or preserving entailment is called soundness. Thus, while constructing proofs, we work bottom-up from the goal. When we have found a proof, we justify formulas from the axioms top-down to the original goal.

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

Example 1. A very simple (in fact propositional) proof of the formula

$$v^2 \leq 10 \land b > 0 \to b > 0 \land (\neg(v \geq 0) \lor v^2 \leq 10) \tag{1}$$

is shown in Fig. 2. The proof starts with the proof goal as a sequent at the bottom:

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

and proceeds applying proof rules upwards.

The first (i.e., bottom most) proof step applies proof rule $\to$r to turn the implication ($\to$) to the sequent level by moving the assumption into the antecedent. The next

[2] There is one subtlety with quantifier elimination that

$$\to r\,\dfrac{\land r\,\dfrac{\land l\,\dfrac{ax\,\dfrac{*}{v^2 \le 10, b > 0 \vdash b > 0}}{v^2 \le 10 \land b > 0 \vdash b > 0} \qquad \lor r\,\dfrac{\land l\,\dfrac{ax\,\dfrac{*}{v^2 \le 10, b > 0 \vdash \neg(v \ge 0), v^2 \le 10}}{v^2 \le 10 \land b > 0 \vdash \neg(v \ge 0), v^2 \le 10}}{v^2 \le 10 \land b > 0 \vdash \neg(v \ge 0) \lor v^2 \le 10}}{v^2 \le 10 \land b > 0 \vdash b > 0 \land (\neg(v \ge 0) \lor v^2 \le 10)}}{\vdash v^2 \le 10 \land b > 0 \to b > 0 \land (\neg(v \ge 0) \lor v^2 \le 10)}$$

Figure 2: Simple propositional example proof

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 $\neg(v \ge 0) \lor v^2 \le 10$ follows from the antecedent also. On the left branch, the proof closes with an axiom ax after splitting the conjunction $\land$ on the antecedent with rule $\land$l. We mark closed proof goals with $*$, just to indicate that we did not just stopped writing. The right branch closes with an axiom ax after splitting the disjunction ($\lor$) in the succedent with rule $\lor$r and then splitting the conjunction ($\land$) in the antecedent with rule $\land$l. Now that all branches of the proof have closed (with ax), we know that all leaves at the top are valid, and, hence, since the premises are valid, each application of a proof rule ensures that their respective conclusions are valid also. By recursively following this derivation from the leaves at the top to the original root at the bottom, we see that the original goal is valid and formula (1) is, indeed, true under all circumstances (valid).

While this proof does not show anything particularly exciting, because it only uses propositional rules, it shows how a proof can be built systematically in the d$\mathcal{L}$ calculus and gives an intuition as to how validity is inherited from the premises to the conclusions.

6 Dynamic Proof Rules

Lecture 5 has shown axioms for dynamical systems that correspond to the operators of hybrid programs in $[\cdot]$ modalities of differential dynamic logic [Pla12]. These were equivalence axioms which represent schemata of valid formulas such as

$$([\cup])\ [\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \land [\beta]\phi$$

How can such valid equivalences be used in the context of a sequent calculus? There is more than one productive way to do that.

The d$\mathcal{L}$ axioms such as $[\cup]$ are primarily meant to be used for replacing the left-hand side $[\alpha \cup \beta]\phi$ by the structurally simpler right-hand side $[\alpha]\phi \land [\beta]\phi$, because that direction of use assigns meaning to $[\alpha \cup \beta]\phi$ in logically simpler terms, i.e. as a structurally simpler logical formula. The following two sequent proof rules allow replacements in that direction for formulas in the antecedent ($[\cup]l$) and succedent ($[\cup]r$), respectively.

$$([\cup]r)\ \frac{\Gamma \vdash [\alpha]\phi \wedge [\beta]\phi, \Delta}{\Gamma \vdash [\alpha \cup \beta]\phi, \Delta}$$

$$([\cup]l)\ \frac{\Gamma, [\alpha]\phi \wedge [\beta]\phi \vdash \Delta}{\Gamma, [\alpha \cup \beta]\phi \vdash \Delta}$$

The sequent proof rules $[\cup]r$,$[\cup]l$ are more systematic in that they orient the use of the axiom $[\cup]$ in the direction that makes formulas structurally simpler. Without such direction, proofs could apply axiom $[\cup]$ from left to right and then from right to left and from left to right again forever without making any progress. That does not happen with $[\cup]r$,$[\cup]l$, because they cannot simply go back.[3] Furthermore, the sequent rules $[\cup]r$,$[\cup]l$ focus the application of axiom $[\cup]$ to the top level of sequents. That is, $[\cup]r$,$[\cup]l$ can only be used for formulas of the succedent or antecedent, respectively, that are of the form $[\alpha \cup \beta]\phi$, not to any subformulas within that happen to be of this form. Abiding both of those restrictions imposes more structure on the proof, compared to the proof we produced in Lecture 5.

Reconsidering the contract-type rules from Lecture 4, we could have turned $[\cup]$ into the following two sequent proof rules instead of into $[\cup]r$,$[\cup]l$:

$$(\text{R14})\ \frac{\Gamma \vdash [\alpha]\phi, \Delta \quad \Gamma \vdash [\beta]\phi, \Delta}{\Gamma \vdash [\alpha \cup \beta]\phi, \Delta}$$

$$(\text{R15})\ \frac{\Gamma, [\alpha]\phi, [\beta]\phi \vdash \Delta}{\Gamma, [\alpha \cup \beta]\phi \vdash \Delta}$$

These rules R14,R15 already split into separate subgoals (R14) or separate formulas (R15), respectively. It would be fine to use sequent rules R14,R15 instead of $[\cup]r$,$[\cup]l$, and, in fact, earlier versions of KeYmaera did. The disadvantage of rules R14,R15 compared to $[\cup]r$,$[\cup]l$ is that rules R14,R15 have a less obvious relation to axiom $[\cup]$ and that they are asymmetric (they both look surprisingly different). This nuisance is overcome in $[\cup]r$,$[\cup]l$, from which rules R14,R15 follow immediately with just one more application of rules $\wedge$r or $\wedge$l, respectively. Thus, $[\cup]r$,$[\cup]l$ are more elementary and more atomic in that they isolate the proof-theoretical meaning of $[\alpha \cup \beta]\phi$, as opposed to already incorporating parts of the meaning of $\wedge$ as well, which is what propositional rules $\wedge$r,$\wedge$l are supposed to capture.

The other d$\mathcal{L}$ axioms from Lecture 5 translate into sequent calculus proof rules in the same way. The dynamic modality rules transform a hybrid program into structurally simpler logical formulas by symbolic decomposition.

For Fig. 3, we adopt a convention to simplify notation. Instead of rules $[\cup]r$,$[\cup]l$, Fig. 3 shows a single *symmetric rule* $[\cup]$ that does not mention the sequent sign $\vdash$:

$$\frac{[\alpha]\phi \wedge [\beta]\phi}{[\alpha \cup \beta]\phi}$$

This is abbreviated notation to say that the same rule from a conclusion with a formula $[\alpha \cup \beta]$ in either antecedent or succedent can be proved from a premise with formula

[3] Albeit, going back is still possible indirectly when using a reasonably creative *cut*. But that requires an intentional extra effort to do so.

$[\alpha]\phi \land [\beta]\phi$ in the antecedent or succedent, respectively. That is, we consider the symmetric rule $[\cup]$ as an abbreviation for the two rules $[\cup]r$,$[\cup]l$. Fig. 3 lists a single symmetric rule $[\cup]$ but we pretend it had both rules $[\cup]r$,$[\cup]l$. The same applies to the other symmetric rules in Fig. 3, which each have a version of the rule for the antecedent and a version of the rule for the succedent. The antecedent version of [;] is called [;]l, its succedent version is called [;]r. The antecedent version of $[']$ is called $[']$l, its succedent version is called $[']$r and so on.

$$
\begin{array}{llllll}
(\langle;\rangle) & \dfrac{\langle\alpha\rangle\langle\beta\rangle\phi}{\langle\alpha;\beta\rangle\phi} & (\langle^{*n}\rangle) & \dfrac{\phi \lor \langle\alpha\rangle\langle\alpha^*\rangle\phi}{\langle\alpha^*\rangle\phi} & (\langle:=\rangle) & \dfrac{\phi_x^\theta}{\langle x:=\theta\rangle\phi} \\[2ex]
([;]) & \dfrac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi} & ([^{*n}]) & \dfrac{\phi \land [\alpha][\alpha^*]\phi}{[\alpha^*]\phi} & ([:=]) & \dfrac{\phi_x^\theta}{[x:=\theta]\phi} \\[2ex]
(\langle\cup\rangle) & \dfrac{\langle\alpha\rangle\phi \lor \langle\beta\rangle\phi}{\langle\alpha\cup\beta\rangle\phi} & (\langle?\rangle) & \dfrac{H \land \psi}{\langle ?H\rangle\psi} & (\langle'\rangle) & \dfrac{\exists t{\geq}0\,\big((\forall 0{\leq}\tilde{t}{\leq}t\,\langle x:=y(\tilde{t})\rangle H) \land \langle x:=y(t)\rangle\phi\big)}{\langle x'=\theta \,\&\, H\rangle\phi}\,\text{[1]} \\[2ex]
([\cup]) & \dfrac{[\alpha]\phi \land [\beta]\phi}{[\alpha\cup\beta]\phi} & ([?]) & \dfrac{H \to \psi}{[?H]\psi} & (['])& \dfrac{\forall t{\geq}0\,\big((\forall 0{\leq}\tilde{t}{\leq}t\,[x:=y(\tilde{t})]H) \to [x:=y(t)]\phi\big)}{[x'=\theta \,\&\, H]\phi}\,\text{[1]}
\end{array}
$$

[1] t and $\tilde{t}$ are fresh logical variables and $\langle x:=y(t)\rangle$ is the discrete assignment belonging to the solution y of the differential equation with constant symbol x as symbolic initial value.

Figure 3: Dynamic proof rules of d$\mathcal{L}$ sequent calculus

Nondeterministic choices split into their alternatives ($\langle\cup\rangle$,$[\cup]$). For rule $[\cup]$: If all α transitions lead to states satisfying ϕ (i.e., $[\alpha]\phi$ holds) and all β transitions lead to states satisfying ϕ (i.e., $[\beta]\phi$ holds), then, all transitions of program $\alpha \cup \beta$ that choose between following α and following β also lead to states satisfying ϕ (i.e., $[\alpha\cup\beta]\phi$ holds). Dually for rule $\langle\cup\rangle$, if there is an α transition to a ϕ state ($\langle\alpha\rangle\phi$) or a β-transition to a ϕ state ($\langle\beta\rangle\phi$), then, in either case, there is a transition of $\alpha\cup\beta$ to ϕ ($\langle\alpha\cup\beta\rangle\phi$ holds), because $\alpha\cup\beta$ can choose which of those transitions to follow. A general principle behind the d$\mathcal{L}$ proof rules that is most noticeable in $\langle\cup\rangle$,$[\cup]$ is that these proof rules symbolically decompose the reasoning into two separate parts and analyse the fragments α and β separately, which is good for scalability. For these symbolic structural decompositions, it is very helpful that d$\mathcal{L}$ is a full logic that is closed under all logical operators, including disjunction and conjunction, for then the premises in $[\cup]$,$\langle\cup\rangle$ are d$\mathcal{L}$ formulas again (unlike in Hoare logic [Hoa69]).

Sequential compositions are proven using nested modalities ($\langle;\rangle$,[;]). For rule [;]: If after all α-transitions, all β-transitions lead to states satisfying ϕ (i.e., $[\alpha][\beta]\phi$ holds), then also all transitions of the sequential composition $\alpha;\beta$ lead to states satisfying ϕ (i.e., $[\alpha;\beta]\phi$ holds). The dual rule $\langle;\rangle$ uses the fact that if there is an α-transition, after which there is a β-transition leading to ϕ (i.e., $\langle\alpha\rangle\langle\beta\rangle\phi$), then there is a transition of $\alpha;\beta$ leading to ϕ (that is, $\langle\alpha;\beta\rangle\phi$), because the transitions of $\alpha;\beta$ are just those that first do any α-transition, followed by any β-transition.

Rules $\langle^{*n}\rangle$,$[^{*n}]$ are the usual iteration rules, which partially unwind loops. Rule $\langle^{*n}\rangle$

uses the fact that ϕ holds after repeating α (i.e., $\langle\alpha^*\rangle\phi$), if ϕ holds at the beginning (for ϕ holds after zero repetitions then), or if, after one execution of α, ϕ holds after any number of repetitions of α, including zero repetitions (i.e., $\langle\alpha\rangle\langle\alpha^*\rangle\phi$). So rule $\langle{*^n}\rangle$ expresses that for $\langle\alpha^*\rangle\phi$ to hold, ϕ must hold either immediately or after one or more repetitions of α. Rule $[{*^n}]$ is the dual rule expressing that ϕ must hold after all of those combinations for $[\alpha^*]\phi$ to hold.

Tests are proven by showing (with a conjunction in rule $\langle ?\rangle$) or assuming (with an implication in rule $[?]$) that the test succeeds, because test $?H$ can only make a transition when condition H actually holds true. Thus, for $\mathsf{d}\mathcal{L}$ formula $\langle ?H\rangle\phi$, rule $\langle ?\rangle$ is used to prove that H holds true (otherwise there is no transition and thus the reachability property is false) and that ϕ holds after the resulting no-op. Rule $[?]$ for $\mathsf{d}\mathcal{L}$ formula $[?H]\phi$, in contrast, assumes that H holds true (otherwise there is no transition and thus nothing to show) and shows that ϕ holds after the resulting no-op.

Given first-order definable flows for their differential equations, proof rules $\langle '\rangle$,$[']$ handle continuous evolutions. These flows are combined in the discrete jump set $x := y(t)$. Given a solution $x := y(t)$ for the differential equation system with symbolic initial values $x_1, \dots, x_n$, continuous evolution along differential equations can be replaced by a discrete jump $\langle x := y(t)\rangle$ with an additional quantifier for the evolution time t. The effect of the constraint on H is to restrict the continuous evolution such that its solution $x := y(\tilde{t})$ remains in the evolution domain H at all intermediate times $\tilde{t} \leq t$. This constraint simplifies to $true$ if the evolution domain restriction H is $true$, which makes sense, because there are no special constraints on the evolution (other than the differential equations) if the evolution domain region is described by $true$, hence the full space $\mathbb{R}^n$. A notable special case of rules $[']$ and $\langle '\rangle$ is when the evolution domain H is $true$:

$$\frac{\forall t{\geq}0\, \langle x := y(t)\rangle\phi}{[x_1' = \theta_1, .., x_n' = \theta_n]\phi} \qquad \frac{\exists t{\geq}0\, \langle x := y(t)\rangle\phi}{\langle x_1' = \theta_1, .., x_n' = \theta_n\rangle\phi} \tag{2}$$

7 Quantifier Proof Rules

$$(\exists r)\ \frac{\Gamma \vdash \phi(\theta), \exists x\, \phi(x), \Delta}{\Gamma \vdash \exists x\, \phi(x), \Delta}\,{}^{1} \qquad (\forall r)\ \frac{\Gamma \vdash \phi(s(X_1, .., X_n)), \Delta}{\Gamma \vdash \forall x\, \phi(x), \Delta}\,{}^{2}$$

$$(\forall l)\ \frac{\Gamma, \phi(\theta), \forall x\, \phi(x) \vdash \Delta}{\Gamma, \forall x\, \phi(x) \vdash \Delta}\,{}^{1} \qquad (\exists l)\ \frac{\Gamma, \phi(s(X_1, .., X_n)) \vdash \Delta}{\Gamma, \exists x\, \phi(x) \vdash \Delta}\,{}^{2}$$

[1] θ is an arbitrary term, often a new (existential) logical variable X.
[2] s is a new (Skolem) function and $X_1, .., X_n$ are all (existential) free logical variables of $\forall x\, \phi(x)$.

Figure 4: Proof rules for first-order quantifiers

Rules $\exists$r,$\forall$l,$\forall$r,$\exists$l are standard proof rules for first-order logic. For explaining these quantifier proof rules, let us first assume for a moment there are no (existential) free variables $X_1, \dots, X_n$ (i.e. $n = 0$) and use what is known as the ground calculus.

The quantifier proof rules work much as in mathematics. Consider $\forall$r, where we want to show a universally quantified property. When a mathematician wants to show a universally quantified property $\forall x\, \phi(x)$ to hold, he could choose a fresh symbol s (called Skolem function symbol) and prove that $\phi(s)$ holds (for s). Then the mathematician would remember that s was arbitrary and his proof did not assume anything special about the value of s. So he would conclude that $\phi(s)$ must indeed hold for all s, and that hence $\forall x\, \phi(x)$ holds true. For example, to show that the square of all numbers is nonnegative, a mathematician could start out by saying "let s be an arbitrary number", prove $s^2 \geq 0$ for s, and then conclude $\forall x\, (x^2 \geq 0)$, since s was arbitrary. Proof rule $\forall$r essentially makes this reasoning formal. It chooses a *new* (function) symbol s and replaces the universally quantified formula in the succedent by a formula for s (with all free logical variables $X_1, \dots, X_n$ added as arguments, as we explain below). Notice, of course, that it is important to choose a new symbol s that has not been used (in the sequent) before. Otherwise, we would assume special properties about s that may not be justified.

Consider $\exists$r, where we want to show an existentially quantified property. When a mathematician proves $\exists x\, \phi(x)$, he could directly produce any witness θ for this existential property and prove that, indeed, $\phi(\theta)$, for then he would have shown $\exists x\, \phi(x)$ 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 0.5 and show the property for 0.5". Then he could prove $0.5^3 < 0.5^2$, because $0.125 < 0.25$, and conclude that there, thus, is such a number, i.e., $\exists x\, (x^3 < x^2)$. Proof rule $\exists$r does that. It allows the choice of *any* term θ for x and accepts a proof of $\phi(\theta)$ as a proof of $\exists x\, \phi(x)$. However note that the claim "θ is a witness" may turn out to be wrong, for example, the choice 2 for x would be a bad start for attempting to show $\exists x\, (x^3 < x^2)$. Consequently, proof rule $\exists$r keeps both options $\phi(\theta)$ and $\exists x\, \phi(x)$ in the succedent.[4] If the proof with θ is successful, the sequent is valid and the part of the proof can be closed successfully. If the proof with θ later turns out to be unsuccessful, another attempt can be used to prove $\exists x\, \phi(x)$, e.g., by applying $\exists$r again with another attempt for a different witness θ_2.

Rules $\forall$l,$\exists$l are dual to $\exists$r,$\forall$l. Consider $\forall$l, where we have a universally quantified formula in the assumptions (antecedent) that we can use, and not in the succedent, 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 $\forall x\, (x > 0 \rightarrow \mathit{hasSqrt}(x))$ in the antecedent, we can also assume instance $5 > 0 \rightarrow \mathit{hasSqrt}(5))$. Rule $\forall$l can produce an instance $\phi(\theta)$ for arbitrary terms θ of the assumption $\forall x\, \phi(x)$. Since we may need the universal fact $\forall x\, \phi(x)$ for multiple instantiations with $\theta_1, \theta_2, \theta_3$ during the proof, rule $\forall$l keeps the

[4] KeYmaera does not actually keep $\exists x\, \phi(x)$ around in the succedent for rule $\exists$r and, for a fundamental reason [Pla08], does not have to. The same holds for rule $\forall$l, where KeYmaera does not keep $\forall x\, \phi(x)$ around in the antecedent, because it does not have to. That means, however, that if you conjecture θ to produce the right instance, and your conjecture turns out wrong during the proof, then you have to go back in the proof and undo your instantiation with θ.

assumption $\forall x\, \phi(x)$ in the antecedent so that it can be used repeatedly.

Consider rule ∃l in which we can use an existentially quantified formula from the antecedent. In mathematics, if we know an existential fact, 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 s, but we cannot denote it by a different term like 5, because 5 may be (and in fact is) the wrong answer. Rule ∃l gives a fresh name s (with all logical variables $X_1, \dots, X_n$ as arguments) to the object that exists. Since it does not make sense to give a different name for the same existing object later, $\exists x\, \phi(x)$ is removed from the antecedent when adding $\phi(s(X_1, \dots, X_n))$.

There are two ways of using the proof rules in Fig. 4. One way is to avoid free variables X_i altogether and only choose ground terms without variables for instantiations θ in ∃r,∀l. Then the Skolem functions used in ∀r,∃l have $n = 0$ free logical variables $X_1, \dots, X_n$ as arguments. This case is called a *ground calculus*, because free variables are never used and all term instantiations are ground (no free variables).

The other way is to work with free variables and always use some fresh (existential) logical variable X for instantiation of θ every time ∃r,∀l are used. This is a free-variable calculus [HS94, Fit96, FM99] where ∃r,∀l are called γ-rules and ∀r,∃l are called δ^+-rules [HS94], which is an improvement of what is known as the δ-rule [Fit96, FM99]. This case is called a *free-variable calculus*, because instantiations are with free variables. Later in the proof, these free variables can be requantified [Pla08]. The free variables $X_1, \dots, X_n$ in the Skolem terms keep track of the dependencies of symbols and prevent instantiations where we instantiate X_1 by a term such as $s(X_1, \dots, X_n)$ depending on X_1. The ground calculus and free-variable calculus uses of Fig. 4 can also be mixed.

8 Real Arithmetic

We will see more details on the handling of real arithmetic in a later lecture. In a nutshell, $\mathrm{QE}(\phi)$ denotes the use of real arithmetic on formula ϕ. That is, for a formula ϕ of first-order real arithmetic, $\mathrm{QE}(\phi)$ is a logical formula that is equivalent to ϕ but simpler, because $\mathrm{QE}(\phi)$ is quantifier-free.

Theorem 2 (Quantifier elimination)**.** *The first-order theory of real arithmetic admits* quantifier elimination *that is, with each formula ϕ, a quantifier-free formula $\mathrm{QE}(\phi)$ can be associated effectively that is equivalent (i.e., $\phi \leftrightarrow \mathrm{QE}(\phi)$ is valid) and has no additional free variables or function symbols. The operation QE is further assumed to evaluate ground formulas (i.e., without variables), yielding a decision procedure for closed formulas of this theory (i.e., formulas without free variables).*

Quantifier elimination yields, e.g., the following equivalence by real arithmetic:

$$\mathrm{QE}(\exists x\, (ax + b = 0)) \;\equiv\; (a \neq 0 \lor b = 0).$$

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

$$\vDash \exists x\, (ax + b = 0) \leftrightarrow (a \neq 0 \lor b = 0)$$

because a linear equation with nonzero inhomogeneous part has a solution iff its linear part is nonzero as well. Real arithmetic equivalences can be used in differential dynamic logic to eliminate quantifiers (or otherwise simplify arithmetic).

With the rule i∀, we can reintroduce a universal quantifier for a Skolem term $s(X_1, \ldots, X_n)$, which corresponds to a previously universally quantified variable in the succedent or a previously existentially quantified variable in the antecedent. The point of reintroducing the quantifier is that this makes sense when the remaining formulas are first-order in the quantified variable so that they can be handled equivalently by quantifier elimination in real-closed fields. When we have proven the subgoal (with for all X) then this entails the goal for the particular $s(X_1, \ldots, X_n)$. In particular, when we remove a quantifier with ∀r,∃l to obtain a Skolem term, we can continue with other proof rules to handle the dynamic modalities and then reintroduce the quantifier for the Skolem term with i∀ once quantifier elimination for real arithmetic becomes applicable.

The dual rule i∃ can reintroduce an existential quantifier for a free logical variable that was previously existentially quantified in the succedent or previously universally quantified in the antecedent. Again, this makes sense when the resulting formula in the premise is first-order in the quantified variable X so that quantifier elimination can eliminate the quantifier equivalently. When we remove a quantifier with ∃r,∀l to obtain a free logical variable, we can continue using other proof rules to handle the dynamic modalities and then reintroduce the quantifier for the free logical variable with i∃ once quantifier elimination is applicable.

$$(\mathrm{i}\forall)\ \frac{\vdash \mathrm{QE}(\forall X\,(\Phi(X) \vdash \Psi(X)))}{\Phi(s(X_1,..,X_n)) \vdash \Psi(s(X_1,..,X_n))}\,^{1} \qquad (\mathrm{i}\exists)\ \frac{\vdash \mathrm{QE}(\exists X\,\bigwedge_i(\Phi_i \vdash \Psi_i))}{\Phi_1 \vdash \Psi_1 \quad \ldots \quad \Phi_n \vdash \Psi_n}\,^{2}$$

[1] X is a new logical variable. Further, QE needs to be defined for the formula in the premise.

[2] Among all open branches, free logical variable X only occurs in the branches $\Phi_i \vdash \Psi_i$. Further, QE needs to be defined for the formula in the premise, especially, no Skolem dependencies on X can occur.

Recall abbreviations from Lecture 5:

$$\begin{aligned}
A_{h,v} &\overset{\text{def}}{\equiv} 0 \leq h \land h = H \land v = 0 \land g > 0 \land 1 > c \geq 0 \\
B_{h,v} &\overset{\text{def}}{\equiv} 0 \leq h \land h \leq H \\
(h'' = -g) &\overset{\text{def}}{\equiv} (h' = v, v' = -g)
\end{aligned}$$

And the single-hop bouncing ball formula from Lecture 5:

$$A_{h,v} \to [h'' = -g; (?h = 0; v := -cv \cup ?h \geq 0)]B_{h,v}$$

We only consider a simpler formula instead:

$$A_{h,v} \to [h'' = -g]B_{h,v} \tag{3}$$

Let there be sequent proof:

$$
{\scriptstyle \to r}\dfrac{{\scriptstyle [']r}\dfrac{{\scriptstyle \forall r}\dfrac{{\scriptstyle \to r}\dfrac{{\scriptstyle \to r}\dfrac{{\scriptstyle \forall l}\dfrac{{\scriptstyle \to l}\dfrac{{\scriptstyle ax}\dfrac{*}{A_{h,v}, r{\ge}0 \vdash 0{\le}r{\le}r} \qquad {\scriptstyle [:=]r}\dfrac{A_{h,v}, r{\ge}0, H-\frac{g}{2}s^2 h \ge 0 \vdash B_{H-\frac{g}{2}r^2,-gt}}{A_{h,v}, r{\ge}0, [h:=H-\frac{g}{2}s^2]h\ge 0 \vdash [h:=H-\frac{g}{2}r^2]B_{h,v}}}{A_{h,v}, r{\ge}0, 0{\le}r{\le}r \to [h:=H-\frac{g}{2}s^2]h\ge 0 \vdash [h:=H-\frac{g}{2}r^2]B_{h,v}}}{A_{h,v}, r{\ge}0, \forall 0{\le}s{\le}r\, [h:=H-\frac{g}{2}s^2]h\ge 0 \vdash [h:=H-\frac{g}{2}r^2]B_{h,v}}}{A_{h,v}, r{\ge}0 \vdash \forall 0{\le}s{\le}r\, [h:=H-\frac{g}{2}s^2]h\ge 0 \to [h:=H-\frac{g}{2}r^2]B_{h,v}}}{A_{h,v} \vdash r{\ge}0 \to (\forall 0{\le}s{\le}r\, [h:=H-\frac{g}{2}s^2]h\ge 0 \to [h:=H-\frac{g}{2}r^2]B_{h,v})}}{A_{h,v} \vdash \forall t{\ge}0\, (\forall 0{\le}s{\le}t\, [h:=H-\frac{g}{2}s^2]h\ge 0 \to [h:=H-\frac{g}{2}t^2]B_{h,v})}}{A_{h,v} \vdash [h''=-g\,\&\,h\ge 0]B_{h,v}}}{\vdash A_{h,v} \to [h''=-g\,\&\,h\ge 0]B_{h,v}}
$$

We just wrote that the left premise closes by ax, except that

$$A_{h,v}, r{\ge}0 \vdash 0{\le}r{\le}r$$

is not exactly an instance of the ax rule, so even here we need simple arithmetic to conclude that $0 \le r \le r$ is the same as $r \ge 0$, at which point that premise turns into a literal instance of ax

$$A_{h,v}, r{\ge}0 \vdash r{\ge}0$$

A full formal proof and a KeYmaera proof, thus, need an extra proof step of arithmetic in the left premise.

The right premise is

$$A_{h,v}, r{\ge}0, H - \frac{g}{2}s^2 h \ge 0 \vdash B_{H-\frac{g}{2}r^2,-gt}$$

which, when resolving abbreviations turns into

$$0 \le h \land h = H \land v = 0 \land g > 0 \land 1 > c \ge 0, r{\ge}0, H - \frac{g}{2}s^2 h \ge 0 \vdash 0 \le H - \frac{g}{2}r^2 \land H - \frac{g}{2}r^2 \le H$$

This sequent proves using $\land$r plus simple arithmetic for the left branch resulting from $\land$r and a little more arithmetic on the right branch resulting from $\land$r. Finishing the above sequent proof up as indicated shows that d$\mathcal{L}$ formula (3) is provable.

9 Instantiating Real Arithmetic

Providing instantiations for quantifier rules $\exists$r,$\forall$l can speed up real arithmetic decision procedures. The proof in Sect. 8 instantiated the universal quantifier $\forall s$ for an evolution domain constraint by the end point r of the time interval using quantifier proof rule $\forall$l. This is a very common simplification that usually speeds up arithmetic significantly. It does not always work, 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, but that is a phenomenon that later lectures will examine.

10 Weakening Real Arithmetic

Weakening rules Wl,Wr can be useful to hide irrelevant parts of a sequent to make sure they do not be a distraction for real arithmetic decision procedures.

In the proof in Sect. 8, the left premise was

$$A_{h,v}, r{\geq}0 \vdash 0{\leq}r{\leq}r$$

The proof of this sequent did not make use of $A_{h,v}$ at all. Here, the proof worked easily. But if $A_{h,v}$ 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 $A_{h,v}$. We might have applied lots of proof rules to $A_{h,v}$ before finally realising that the sequent proves because of $r{\geq}0 \vdash 0{\leq}r{\leq}r$ alone.

The same kind of distraction can happen in decision procedures for real arithmetic, sometimes shockingly so [Pla10, Chapter 5]. Consequently, it can sometimes save a lot of proof effort to simplify irrelevant assumptions away as soon as they have become unnecessary. Fortunately, there already is a proof rule for that purpose called weakening, which we can use on our example from the left premise in the proof of Sect. 8:

$$\text{Wl}\,\frac{r{\geq}0 \vdash 0{\leq}r{\leq}r}{A_{h,v}, r{\geq}0 \vdash 0{\leq}r{\leq}r}$$

11 Summary

The differential dynamic logic sequent proof rules that we have seen in this lecture are summarized in Fig. 5. They turn out to be sound [Pla08]. Yet, the notion of soundness for axioms that we investigated in Lecture 5 does not directly apply to proof rules. We will investigate soundness of the proof rules in Fig. 5 in a later lecture. There are further proof rules of differential dynamic logic that later lectures will examine [Pla08].

References

[And02] Peter B. Andrews. *An Introduction to Mathematical Logic and Type Theory: To Truth Through Proof*. Kluwer, 2nd edition, 2002.

[Bus98] Samuel R. Buss. An introduction to proof theory. In Samuel R. Buss, editor, *Handbook of Proof Theory*, chapter 1, pages 1–78. Elsevier, 1998.

[Fit96] Melvin Fitting. *First-Order Logic and Automated Theorem Proving*. Springer, New York, 2nd edition, 1996.

[FM99] Melvin Fitting and Richard L. Mendelsohn. *First-Order Modal Logic*. Kluwer, Norwell, MA, USA, 1999.

[Gen35] Gerhard Gentzen. Untersuchungen über das logische Schließen. I. *Math. Zeit.*, 39(2):176–210, 1935.

$$(\neg r)\ \frac{\Gamma, \phi \vdash \Delta}{\Gamma \vdash \neg\phi, \Delta} \qquad (\vee r)\ \frac{\Gamma \vdash \phi, \psi, \Delta}{\Gamma \vdash \phi \vee \psi, \Delta} \qquad (\wedge r)\ \frac{\Gamma \vdash \phi, \Delta \quad \Gamma \vdash \psi, \Delta}{\Gamma \vdash \phi \wedge \psi, \Delta}$$

$$(\neg l)\ \frac{\Gamma \vdash \phi, \Delta}{\Gamma, \neg\phi \vdash \Delta} \qquad (\vee l)\ \frac{\Gamma, \phi \vdash \Delta \quad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \vee \psi \vdash \Delta} \qquad (\wedge l)\ \frac{\Gamma, \phi, \psi \vdash \Delta}{\Gamma, \phi \wedge \psi \vdash \Delta}$$

$$(\rightarrow r)\ \frac{\Gamma, \phi \vdash \psi, \Delta}{\Gamma \vdash \phi \rightarrow \psi, \Delta} \qquad (ax)\ \frac{}{\Gamma, \phi \vdash \phi, \Delta} \qquad (\mathrm{Wr})\ \frac{\Gamma \vdash \Delta}{\Gamma \vdash \phi, \Delta}$$

$$(\rightarrow l)\ \frac{\Gamma \vdash \phi, \Delta \quad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \rightarrow \psi \vdash \Delta} \qquad (cut)\ \frac{\Gamma \vdash \phi, \Delta \ \ \Gamma, \phi \vdash \Delta}{\Gamma \vdash \Delta} \qquad (\mathrm{Wl})\ \frac{\Gamma \vdash \Delta}{\Gamma, \phi \vdash \Delta}$$

$$(\langle ; \rangle)\ \frac{\langle\alpha\rangle\langle\beta\rangle\phi}{\langle\alpha;\beta\rangle\phi} \qquad (\langle {}^{*n} \rangle)\ \frac{\phi \vee \langle\alpha\rangle\langle\alpha^*\rangle\phi}{\langle\alpha^*\rangle\phi} \qquad (\langle := \rangle)\ \frac{\phi_x^\theta}{\langle x := \theta\rangle\phi}$$

$$([;])\ \frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi} \qquad ([{}^{*n}])\ \frac{\phi \wedge [\alpha][\alpha^*]\phi}{[\alpha^*]\phi} \qquad ([:=])\ \frac{\phi_x^\theta}{[x := \theta]\phi}$$

$$(\langle \cup \rangle)\ \frac{\langle\alpha\rangle\phi \vee \langle\beta\rangle\phi}{\langle\alpha \cup \beta\rangle\phi} \qquad (\langle ? \rangle)\ \frac{H \wedge \psi}{\langle ?H\rangle\psi} \qquad (\langle ' \rangle)\ \frac{\exists t{\geq}0\, \big((\forall 0{\leq}\tilde{t}{\leq}t\, \langle x := y(\tilde{t})\rangle H) \wedge \langle x := y(t)\rangle\phi\big)}{\langle x' = \theta \,\&\, H\rangle\phi}\ \text{[1]}$$

$$([\cup])\ \frac{[\alpha]\phi \wedge [\beta]\phi}{[\alpha \cup \beta]\phi} \qquad ([?])\ \frac{H \rightarrow \psi}{[?H]\psi} \qquad ([\,'\,])\ \frac{\forall t{\geq}0\, \big((\forall 0{\leq}\tilde{t}{\leq}t\, [x := y(\tilde{t})]H) \rightarrow [x := y(t)]\phi\big)}{[x' = \theta \,\&\, H]\phi}\ \text{[1]}$$

$$(\exists r)\ \frac{\Gamma \vdash \phi(\theta), \exists x\, \phi(x), \Delta}{\Gamma \vdash \exists x\, \phi(x), \Delta}\ \text{[2]} \qquad (\forall r)\ \frac{\Gamma \vdash \phi(s(X_1, .., X_n)), \Delta}{\Gamma \vdash \forall x\, \phi(x), \Delta}\ \text{[3]}$$

$$(\forall l)\ \frac{\Gamma, \phi(\theta), \forall x\, \phi(x) \vdash \Delta}{\Gamma, \forall x\, \phi(x) \vdash \Delta}\ \text{[2]} \qquad (\exists l)\ \frac{\Gamma, \phi(s(X_1, .., X_n)) \vdash \Delta}{\Gamma, \exists x\, \phi(x) \vdash \Delta}\ \text{[3]}$$

$$(\mathrm{i}\forall)\ \frac{\Gamma \vdash \mathrm{QE}(\forall X\, (\Phi(X) \vdash \Psi(X))), \Delta}{\Gamma, \Phi(s(X_1, .., X_n)) \vdash \Psi(s(X_1, .., X_n)), \Delta}\ \text{[4]} \qquad (\mathrm{i}\exists)\ \frac{\Gamma \vdash \mathrm{QE}(\exists X\, \bigwedge_i (\Phi_i \vdash \Psi_i)), \Delta}{\Gamma, \Phi_1 \vdash \Psi_1, \Delta \ \ \ldots \ \ \Gamma, \Phi_n \vdash \Psi_n, \Delta}\ \text{[5]}$$

[1] t and $\tilde{t}$ are fresh logical variables and $\langle x := y(t)\rangle$ is the discrete assignment belonging to the solution y of the differential equation with constant symbol x as symbolic initial value.

[2] θ is an arbitrary term, often a new (existential) logical variable X.

[3] s is a new (Skolem) function and $X_1, .., X_n$ are all (existential) free logical variables of $\forall x\, \phi(x)$.

[4] X is a new logical variable. Further, QE needs to be defined for the formula in the premise.

[5] Among all open branches, free logical variable X only occurs in the branches $\Gamma, \Phi_i \vdash \Psi_i, \Delta$. Further, QE needs to be defined for the formula in the premise, especially, no Skolem dependencies on X can occur.

Figure 5: Some proof rules of the d$\mathcal{L}$ sequent calculus

[Hoa69] Charles Antony Richard Hoare. An axiomatic basis for computer programming. *Commun. ACM*, 12(10):576–580, 1969.

[HS94] Reiner Hähnle and Peter H. Schmitt. The liberalized δ-rule in free variable semantic tableaux. *J. Autom. Reasoning*, 13(2):211–221, 1994.

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

[Pla10] André Platzer. *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics*. Springer, Heidelberg, 2010. doi:10.1007/978-3-642-14509-4.

[Pla12] André Platzer. Logics of dynamical systems. In *LICS*, pages 13–24. IEEE, 2012. doi:10.1109/LICS.2012.13.