# Differential Equation Invariance Axiomatization

ANDRÉ PLATZER,  Carnegie Mellon University
YONG KIAM TAN,  Carnegie Mellon University

This article proves the completeness of an axiomatization for differential equation invariants described by Noetherian functions. First, the differential equation axioms of differential dynamic logic are shown to be complete for reasoning about analytic invariants. Completeness crucially exploits differential ghosts, which introduce additional variables that can be chosen to evolve freely along new differential equations. Cleverly chosen differential ghosts are the proof-theoretical counterpart of dark matter. They create new hypothetical state, whose relationship to the original state variables satisfies invariants that did not exist before. The reflection of these new invariants in the original system then enables its analysis.

An extended axiomatization with existence and uniqueness axioms is complete for all local progress properties, and, with a real induction axiom, is complete for all semianalytic invariants. This parsimonious axiomatization serves as the logical foundation for reasoning about invariants of differential equations. Indeed, it is precisely this logical treatment that enables the generalization of completeness to the Noetherian case.

## 1 INTRODUCTION

Classically, differential equations are studied by analyzing their solutions, which is at odds with the fact that solutions are often much more complicated than the differential equations themselves. This stark difference between the simple local description as differential equations, and the complex global behavior exhibited by their solutions is fundamental to the descriptive power of differential equations. Poincaré's qualitative study of differential equations [34] calls for the exploitation of this difference by deducing properties of solutions *directly from the differential equations*. This article completes an important step in this enterprise by identifying the *logical foundations for proving invariance properties of differential equations* described by Noetherian functions [3, 11, 12, 41].

This result exploits the differential equation axioms of differential dynamic logic (dL) [29, 32]. dL is a logic for deductive verification of hybrid systems that are modeled by hybrid programs combining discrete computation (e.g., assignments, tests and loops), and continuous dynamics specified using systems of ordinary differential equations (ODEs). By the continuous relative completeness theorem for dL [29, Theorem 1], verification of hybrid systems reduces completely to

the study of differential equations. Thus, the hybrid systems axioms of dL provide a way of lifting the findings of this article about differential equations to hybrid systems. The remaining practical challenge is to find succinct ODE invariants. The dL calculus reduces proving such an invariant to arithmetical questions, which are decidable if the invariants are in first-order real arithmetic [4].

To understand the difficulty in verifying properties of ODEs, it is useful to draw an analogy between ODEs and discrete program loops.[1] Loops also exhibit the dichotomy between global behavior and local description. Although the body of a loop may be simple, it is almost always impractical to reason about the global behavior of loops by unfolding all possible iterations. Instead, the premier reasoning technique for loops is to study their loop invariants, i.e., inductive properties that are always preserved across each execution of the loop body.

Similarly, invariants of ODEs describe subsets of the state space from which solutions of the ODEs cannot escape. The three basic dL principles for reasoning about such invariants are: (1) *differential invariants*, which enable local reasoning about local change of truth in differential form, (2) *differential cuts*, which accumulate knowledge about the evolution of an ODE from multiple proofs, and (3) *differential ghosts*, which add differential equations for new ghost variables to the existing system of differential equations enabling reasoning about the historical evolution of ODE systems in integral form. These reasoning principles relate to their discrete loop counterparts as follows: (1) corresponds to loop induction by analyzing the loop body, (2) corresponds to progressive refinement of the loop guards, and (3) corresponds to adding discrete ghost variables to remember intermediate program states. At first glance, differential ghosts seem counter-intuitive: they increase the dimension of the system, which should be adverse to analyzing it! However, just as the addition of discrete ghosts allows the expression of new relationships between variables along executions of a program [26], adding differential ghosts that suitably co-evolve with the ODEs crucially allows the expression of new relationships along solutions to the differential equations. The ramifications of these new relationships are then used to analyze the original, unaugmented ODEs.

The dL proof calculus internalizes these reasoning principles as *syntactic* axioms [32]. ODE invariance proofs in dL are syntactic derivations whose correctness relies solely on the soundness of these underlying axioms. Crucially, this obviates the need to unfold the mathematical semantics of differential equations for proving their invariance properties. This separation of syntax and axiomatics from semantics enables their sound implementation, e.g., in KeYmaera X [10] with dL's uniform substitution calculus [32], and their verification in foundational theorem provers [5].

This article extends the authors' earlier conference version [33] beyond the polynomial setting and presents a *differential equation invariance axiomatization*. For extended term languages (and ODEs) meeting three extended term conditions, this article presents the following contributions:

(1) *All* analytic invariants, i.e., finite conjunctions and disjunctions of equations between extended terms, are provable using only the three ODE axioms outlined above.
(2) With axioms internalizing the existence and uniqueness theorems for solutions of differential equations, all *local progress* properties of ODEs are provable for all semianalytic formulas, i.e., propositional combinations of inequalities between extended terms.
(3) With a real induction axiom that reduces invariance to local progress, the dL calculus is complete for proving *all* semianalytic invariants of differential equations.
(4) These are *axiomatic completeness* results: all (semi)analytic invariance and local progress questions are provably *equivalent* in dL to questions about the underlying arithmetic. This equivalence also yields disproofs when the resulting arithmetic questions are refuted.

---

[1]In fact, this analogy can be made precise: dL also has a converse relative completeness theorem [29, Theorem 2] that reduces hybrid systems and their ODEs completely to discrete Euler approximation loops.

These results are proved constructively, yielding practical and purely logical proof-producing procedures for reducing ODE invariance questions to arithmetical questions in dL. The most subtle step is the construction of suitable differential ghosts that simplify the analysis as a function of both the differential equations and desired invariant. The axiomatic approach crucially enables these contributions because the axioms internalize basic properties of ODEs and thus remain sound and complete for *all* extended term languages meeting the extended term conditions. Furthermore, the identification of a parsimonious yet complete ODE axiomatization provides the best of both worlds: *parsimony* minimizes effort required in implementation and verification of the proof calculus while *completeness* guarantees that all ODE invariance reasoning is possible using only syntactic proofs from the foundational axioms. Since the completeness results prove equivalences, these advantages continue to hold whether proving or disproving invariance properties of differential equations. This logical foundation is essential because it enables *compositional* syntactic reasoning in dL for (continuous) differential equations in isolation from other (discrete) parts of the hybrid system [29].

Since Noetherian functions from real analytic geometry [3, 11, 12, 41] generate Noetherian rings closed under (partial) derivatives, they meet all of the extended term conditions and thus provide an ideal setting for extending term languages. Noetherian functions include many functions of practical interest for modeling hybrid systems, e.g., real exponential and trigonometric functions, which are implicitly definable in dL [28, 29] but do not come with effective reasoning principles.[2] Making them first-class members of the term language enables their explicit use in hybrid systems models and proofs, especially in descriptions of ODE invariants. The study of Noetherian functions is a major new contribution of this extended version, among others:

(5) Noetherian functions are shown to meet the extended term conditions. Any such extension automatically inherits all of the aforementioned completeness results.
(6) The authors' earlier results and proofs [33] are generalized to extended term languages.
(7) A stronger proof-theoretical result is shown for algebraic (and analytic) completeness compared to the earlier result [33] using only *scalar* differential ghosts.

Just as discrete ghosts can make a program logic relatively complete [26], differential ghosts achieve completeness for algebraic (and analytic) invariants in dL. The improvement (7) is significant for conceptual, implementation, and proof purposes. All algebraic (and analytic) invariants can now be proved using only a *constant* number of scalar differential ghosts compared to the earlier result [33] which introduces a *quadratic* number of ghost variables using *vectorial* differential ghosts.

## 2 BACKGROUND: DIFFERENTIAL DYNAMIC LOGIC

This section briefly reviews (differential-form) differential dynamic logic (dL), focusing on its continuous fragment. It also establishes the notational conventions used in this article and motivates the extended term conditions. The interested reader is referred to the literature [29, 32] for a complete exposition of dL, including its discrete and hybrid fragments.

### 2.1 Syntax

*Terms* in dL are given by the following grammar, where $x \in \mathbb{V}$ is a variable from the set of all variables $\mathbb{V}$, $c \in \mathbb{Q}$ is a rational constant, and $h \in \{h_1, \ldots, h_r\}$ are $k$-ary function symbols:

$$e, \tilde{e} ::= x \mid c \mid e + \tilde{e} \mid e \cdot \tilde{e} \mid h(e_1, \ldots, e_k) \mid (e)'$$

Terms generated using only the first 4 clauses of this grammar correspond to polynomials over the variables under consideration. For this article, the term language is extended with a finite number

---

[2]The relative decidability theorem for dL [29, Theorem 11] needs either an oracle for (continuous) differential equation properties or an oracle for discrete program properties.

of new $k$-ary fixed function symbols, $h \in \{h_1, \ldots, h_r\}$, with fixed interpretations. As a running example of such an extended term language, consider the unary function symbols $\exp, \sin, \cos$ which are always interpreted as the real exponential and trigonometric functions respectively:

$$e, \tilde{e} ::= x \mid c \mid e + \tilde{e} \mid e \cdot \tilde{e} \mid \exp(e) \mid \sin(e) \mid \cos(e) \mid (e)' \qquad (1)$$

Of course, the syntactic extension cannot be completely arbitrary, e.g., adding functions $h$ whose interpretation is nowhere differentiable would fundamentally break the enterprise of studying ODEs directly by their local behavior. These unsuitable syntactic extensions are ruled out by a set of extended term conditions. These conditions are developed and motivated along the way, with a summary in Section 2.4. The class of Noetherian functions, which meets all of these extended term conditions, is introduced and studied in Section 7. The Noetherian class includes the functions in the example ($\exp, \sin, \cos$) so the completeness results also apply to the extended term language (1).

*Differentials* $(e)'$ are used in dL for sound differential equations reasoning [32]. The value of $(e)'$ relates to how the value of term $e$ changes with each of its variables as a function also of how those variables themselves change. The fundamental insight is that, along the evolution of a differential equation, the value of differential $(e)'$ coincides with the analytic time derivative of $e$ [32, Lem. 35], so that proofs about *equations of differentials* yield proofs about *differential equations*. It is crucial for soundness and compositionality that differentials have a local semantics defined in any state, so that they can be used correctly in any context to draw sound conclusions from syntactic manipulations mixing dynamic statements about differential equations and static statements about differentials. The precise semantics of differentials is elaborated in Section 2.2, while Section 2.3.1 explains how they can be used to obtain a syntactic representation of (semantic) time derivatives along solutions to differential equations. Syntactically, every variable $x \in \mathbb{V}$ is assumed to have a corresponding differential variable $x' \in \mathbb{V}$ which, like differential terms, are syntactic representations of the semantic time derivative of $x$ along solutions. Section 2.3.1 also shows that, when in the context of an ODE, differential terms (and variables) can be provably turned into terms that do not contain any differentials or differential variables. Therefore, $e, \tilde{e}$ is used exclusively in this article to refer to such differential-free terms, e.g., $(e)'$ is the differential of $e$, where $e$ is a differential-free term.

For this article, we write $x$ to refer to a vector of variables $x_1, \ldots, x_n$ and write $e(x), \tilde{e}(x)$ to emphasize that these terms depend only on variables $x$ free. When this dependency is unimportant, terms $e, \tilde{e}$ are written as usual without any dependencies. As convenient distinguishing notation, vectors of terms are written in bold $\mathbf{e}, \tilde{\mathbf{e}}$, with $\mathbf{e}_i, \tilde{\mathbf{e}}_i$ for their $i$-th components. These vectorial terms and their corresponding dimensions are always explicitly specified when used, e.g., in Section 4.1. Polynomial terms are useful as familiar illustrative examples and they also enjoy special properties not necessarily shared by extended term languages. The notation $p, q$ is reserved for polynomial terms, with dependencies $p(x), q(x)$ added when necessary.

*Formulas* of dL are given by the following grammar, where $\sim$ is a comparison operator $=, \geq, >$ and $\alpha$ is a differential equation (or, more generally, a *hybrid program* [29, 32]):

$$\phi, \psi ::= e \sim \tilde{e} \mid \phi \wedge \psi \mid \phi \vee \psi \mid \neg\phi \mid \forall x\, \phi \mid \exists x\, \phi \mid [\alpha]\phi \mid \langle\alpha\rangle\phi$$

Formulas can be normalized such that every atomic comparison $e \sim \tilde{e}$ has 0 on the right-hand side. The notation $e \succcurlyeq 0$ is used when there is a free choice between $\geq$ or $>$. Other logical connectives, e.g., $\rightarrow, \leftrightarrow$ are definable as usual. For the formula $\mathbf{e} = \tilde{\mathbf{e}}$ where both $\mathbf{e}, \tilde{\mathbf{e}}$ have dimension $n$, equality is understood *component-wise* as $\bigwedge_{i=1}^{n} \mathbf{e}_i = \tilde{\mathbf{e}}_i$ and $\mathbf{e} \neq \tilde{\mathbf{e}}$ as $\neg(\mathbf{e} = \tilde{\mathbf{e}})$. The modal formula $[\alpha]\phi$ is true iff $\phi$ is true after *all* runs of $\alpha$, and its dual $\langle\alpha\rangle\phi$ is true iff $\phi$ is true after *some* run of $\alpha$.

Formulas not containing the first-order quantifiers and modal connectives are called *semianalytic* formulas and are written as $P, Q$. The word "analytic" refers to the (semantic) real analyticity [20] of terms when extended with Noetherian functions in Section 7. As usual, the dependencies $P(x), Q(x)$

are added when necessary. Every semianalytic formula can be normalized to one that is formed from only conjunctions and disjunctions of atomic comparison formulas. Formulas $P, Q$ formed from only conjunctions and disjunctions of equalities are called *analytic* formulas. When all atomic comparisons in (semi)analytic formulas are restricted to only occur between polynomial terms $p \sim q$, the resulting formulas are also known as *(semi)algebraic* formulas [4]. The first-order theory of the reals with polynomial terms (and with quantifiers), is decidable by quantifier elimination [4]. Thus, every first-order formula of real arithmetic is equivalent to a (quantifier-free) semialgebraic formula and no expressiveness is lost by disallowing first-order quantifiers in the semialgebraic case. Unfortunately, quantifier elimination is impossible even for simple term language extensions like the exponential function [42]. Furthermore, even for the extended term language (1) with trigonometric functions, arithmetic questions are already undecidable [36]. Therefore, special care is taken in this article to distinguish first-order properties of the real closed fields, i.e., those described by (semi)algebraic formulas [4], from those properties described by (semi)analytic formulas.

The dL modalities $[\alpha]$ and $\langle \alpha \rangle$ are parameterized by a *continuous program* $\alpha$ (more general *hybrid programs* combining discrete and continuous dynamics are supported in dL but not relevant here):

$$\alpha ::= \cdots \mid x' = f(x) \,\&\, Q$$

The continuous program $x' = f(x) \,\&\, Q$ is an autonomous (vectorial) differential equation system with LHS $x' = (x'_1, \ldots, x'_n)$ and RHS term $f_i(x)$ for each $x'_i$. Following the notational convention, $f_i(x)$ is differential-free so the ODE system $x' = f(x)$ is given in explicit form [32]. Autonomous ODEs $x' = f(x)$ do not depend explicitly on time on the RHS. A standard transformation is to add a clock variable $t$ to the system with $x' = f(x,t), t' = 1$ if time dependency on the RHS is desired. The evolution domain constraint $Q$ is a semianalytic formula restricting the set of states in which the ODE is allowed to evolve continuously; the ODE is simply written as $x' = f(x)$ when the domain constraint is *true*. The following running example ODE is used in this article (see Fig. 1):

$$\alpha_e \stackrel{\text{def}}{\equiv} u' = -v + \frac{u}{4}(1 - u^2 - v^2), v' = u + \frac{v}{4}(1 - u^2 - v^2) \tag{2}$$

Following the analogy between ODEs and (discrete) program loops in Section 1, solutions of an ODE must continuously (locally) follow its RHS. This is visualized in Fig. 1 with directional arrows corresponding to the RHS of $\alpha_e$ evaluated at points on the plane. Even though the RHS of $\alpha_e$ are polynomials, its solutions, which must locally follow the arrows, already exhibit complex global behavior. Fig. 1 suggests, e.g., that all points (except the origin) globally evolve towards the unit circle.
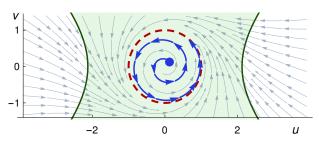


Fig. 1. The red dashed circle $u^2 + v^2 = 1$ is approached by solutions of $\alpha_e$ from all points except the origin, e.g., the blue trajectory from $(\frac{1}{8}, \frac{1}{8})$ spirals towards the circle. The red circle, green region $u^2 \le v^2 + \frac{9}{2}$, and origin are invariants of the system.

## 2.2 Semantics

A state $\omega : \mathbb{V} \to \mathbb{R}$ assigns a real value to each variable in $\mathbb{V}$; the set of all states is written $\mathbb{S}$. The semantics of term $e$ in state $\omega$ is written as $\omega[\![e]\!] \in \mathbb{R}$. It is defined as usual for the standard arithmetic operators, e.g., $\omega[\![e + \tilde{e}]\!] = \omega[\![e]\!] + \omega[\![\tilde{e}]\!]$. The semantics of each fixed function symbol $h$ is given by a corresponding real-valued function $h : \mathbb{R}^k \to \mathbb{R}$ (using the same symbol $h$ for the LHS

syntactic function symbol and its RHS semantic interpretation by a slight abuse of notation):

$$\omega[[h(e_1, \ldots, e_k)]] = h(\omega[[e_1]], \ldots, \omega[[e_k]])$$

The semantics of differentials [32] is the sum of partial derivatives $\frac{\partial \omega[[e]]}{\partial x}$ by all variables $x \in \mathbb{V}$ multiplied by the values of their associated differential variables $x'$, where $\omega(x')$ selects the direction in which $x$ evolves locally and $\frac{\partial \omega[[e]]}{\partial x}$ describes how the value of $e$ changes with a change of $x$:

$$\omega[[(e)']] = \sum_{x \in \mathbb{V}} \omega(x') \frac{\partial \omega[[e]]}{\partial x}$$

There are two subtleties to highlight. First, the real-valued functions $h$ are required to be defined on the domain $\mathbb{R}^k$ so that the term semantics are well-defined in all states. It is possible to extend dL with terms that are only defined within an open domain of definition rather than the entire real domain and this would allow, e.g., rational functions to be added to the term language. This article will not pursue such an extension, although the Noetherian functions from Section 7 and Proposition 7.4 give an implicit way of working with quotients of extended terms. Second, the semantics of differentials implicitly requires that the partial derivatives $\frac{\partial \omega[[e]]}{\partial x}$ exist. In fact, partial derivatives of any order for the semantics of any term must exist because their differentials (which provably reduce to differential-free terms by Section 2.3.1), in turn, have differentials that must also have a well-defined semantics. Following the standard interpretation of function symbols [32], it suffices to require that the fixed function symbols $h$ are interpreted as smooth $C^\infty$ functions, i.e., have partial derivatives of any order. Since the $C^\infty$ functions are closed under addition, multiplication and function composition, the resulting term semantics are also smooth [32], as required.

The semantics of differentials $(e)'$ is well-defined for isolated states $\omega$, independent of any ODEs. Their importance for differential equations reasoning in dL stems from the semantics of hybrid programs $\alpha$, which are transition relations, $[[\alpha]] \subseteq \mathbb{S} \times \mathbb{S}$, between states. The semantics of an ODE, $[[x' = f(x) \& Q]]$, is the set of all pairs of states that are connected by some solution of the ODE:

$$(\omega, \nu) \in [[x' = f(x) \& Q]] \text{ iff there is a duration } 0 \le T \in \mathbb{R} \text{ and a function } \varphi : [0, T] \to \mathbb{S}$$

$$\text{with } \varphi(0) = \omega \text{ on } \{x'\}^\complement, \varphi(T) = \nu, \text{ and } \varphi \models x' = f(x) \land Q$$

The $\varphi \models x' = f(x) \land Q$ condition checks $\varphi(\zeta) \in [[x' = f(x) \land Q]]$, $\varphi(0) = \varphi(\zeta)$ on $\{x, x'\}^\complement$ for all $0 \le \zeta \le T$, and, if $T > 0$, then $\frac{d\varphi(t)(x)}{dt}(\zeta)$ exists, and is equal to $\varphi(\zeta)(x')$ for all $0 \le \zeta \le T$. In other words, $\varphi$ is a solution of the differential equations $x' = f(x)$ that always stays in the evolution domain constraint $Q$. It is also required to hold all variables other than $x, x'$ constant. Most importantly, the values of the differential variables $x'$ are required to match the value of the RHS $f(x)$ of the differential equation along the solution. See [32, Definition 7] for further details.

The semantics of comparison operations and first-order logical connectives are defined as usual, with $[[\phi]] \subseteq \mathbb{S}$ being the set of states where formula $\phi$ is true. For example, $\omega \in [[e \le \tilde{e}]]$ iff $\omega[[e]] \le \omega[[\tilde{e}]]$, and $\omega \in [[\phi \land \psi]]$ iff $\omega \in [[\phi]]$ and $\omega \in [[\psi]]$. The semantics of modal connectives are:

$$\omega \in [[[\alpha]\phi]] \text{ iff } \nu \in [[\phi]] \text{ for all } \nu \text{ such that } (\omega, \nu) \in [[\alpha]]$$

$$\omega \in [[\langle\alpha\rangle\phi]] \text{ iff there is a state } \nu \text{ such that } (\omega, \nu) \in [[\alpha]] \text{ and } \nu \in [[\phi]]$$

Formula $\phi$ is *valid* iff it is true in all states, i.e., $[[\phi]] = \mathbb{S}$. If the formula $P \to [x' = f(x) \& Q]P$ is valid, then the formula $P$ is called an *invariant* of the ODE, $x' = f(x) \& Q$. Unfolding the semantics, this means that from any initial state $\omega \in [[P]]$, any solution $\varphi$ of $x' = f(x)$ starting in $\omega$, which does not leave the evolution domain $[[Q]]$, stays in $[[P]]$ for its *entire duration*. Fig. 1 suggests several invariants for the ODE $\alpha_e$ from (2). The unit circle, $u^2 + v^2 = 1$, is an equational invariant because

the direction of flow on the circle is always tangential to it. The open unit disk, $u^2 + v^2 < 1$, is also invariant because trajectories within the disk spiral towards the circle but never reach it. The green region described by $u^2 \leq v^2 + \frac{9}{2}$ is invariant but needs a careful proof.

## 2.3 Axiomatization

This article uses a standard, classical sequent calculus [27] with the usual rules for manipulating logical connectives and sequents, e.g., ∨L, ∧R, and cut. A summary of all base axioms and proof rules used in this article is in Appendix A.3, along with a list of the standard propositional and first-order sequent calculus proof rules. The semantics of *sequent* $\Gamma \vdash \phi$ is equivalent to the formula $(\bigwedge_{\psi \in \Gamma} \psi) \rightarrow \phi$ and the sequent is valid iff its corresponding formula is valid. Formulas $\Gamma$ are *antecedents* of the sequent, while formula $\phi$ is its *succedent*. Completed branches are marked with $*$ in a sequent proof. An axiom is *sound* iff all its instances are valid, and a proof rule is *sound* iff the validity of all its *premises* (above the rule bar) imply the validity of its *conclusion* (below rule bar). When an implicational or equivalence axiom is used, propositional sequent manipulation steps are omitted and the proof step is directly labeled with the axiom, giving the resulting premises accordingly [32]. The calculus includes ∀L, ∃R rules for the reals allowing $x$ to be instantiated (or witnessed) with a term for the sequents $\Gamma, \forall x \, \phi \vdash \psi$ and $\Gamma \vdash \exists x \, \phi$ respectively. First-order real arithmetic is decidable [4] so access to such a decision procedure is assumed; proof steps are labeled with ℝ whenever they follow as a substitution instance of a valid formula of first-order real arithmetic. Extra care must be taken when using ℝ for extended term languages, as illustrated next.

*Example 2.1 (Proving with ℝ).* Consider the following two proofs in the extended term language (1). The left sequent proves (as a substitution instance) by ℝ because the negation of a real number is its additive inverse. In contrast, the right sequent does not prove by ℝ alone (indicated by the subscript on rule ℝ$_{\exp}$) because it uses the fact that the real exponential function is strictly positive.

$$\mathbb{R} \frac{*}{\vdash \exp(x) + (-\exp(x)) = 0} \qquad\qquad \mathbb{R}_{\exp} \frac{*}{\vdash \exp(x) > 0}$$

An alternative understanding is that rule ℝ can be used to conclude valid properties that follow *only* from first-order properties of the real closed fields [4].

All of the axiom and rule (schemata) in this article can be derived from axioms in dL's uniform substitution calculus [32], an approach which minimizes the soundness-critical core in implementations of the logic [10]. This presentation is omitted as it is not the focus for this article. Readers are referred to the authors' earlier conference version [33] for details.

*2.3.1 Differentials and Lie Derivatives.* ODEs $x' = f(x)$ precisely specify time derivatives that their solutions must obey. The deduction of invariants directly from these differential equations therefore relates to the study of time derivatives of the quantities that the invariants involve. However, directly using time derivatives leads to numerous subtle sources of unsoundness because they are semantic objects that only make sense when a "time" axis even exists at all. Such a continuous time axis is furnished by the domain of definition of an ODE solution, but time derivatives are not otherwise well-defined in arbitrary contexts, e.g., in isolated states or across discrete transitions. It is of utmost importance for soundness that, unlike time derivatives, differentials have a local semantics that is well-defined in single states which enables their use in arbitrary contexts for sound syntactic manipulations [32]. The crucial differential lemma [32, Lem. 35] shows that, along a solution of the ODE $x' = f(x)$, the value of the differential term $(e)'$ coincides with the time derivative $\frac{d}{dt}$ of the value of term $e$. This relationship allows conclusions to be drawn about the differential equations directly from syntactic dL proofs involving differentials. The latter syntactic

manipulation of differentials is achieved using the *differential axioms* of dL, which are given below. In axiom DE, $x' = f(x)$ is understood vectorially, i.e., $x$ is a vector of variables $x_1, \ldots, x_n$, $x'$ the corresponding vector of differential variables $x'_1, \ldots, x'_n$, and $f(x)$ a vector of terms $f_1(x), \ldots, f_n(x)$.

THEOREM 2.2 (DIFFERENTIAL AXIOMS [32]). *The following are sound axioms of* dL:
DE  $[x' = f(x) \& Q(x)]P(x, x') \leftrightarrow [x' = f(x) \& Q(x)][x' := f(x)]P(x, x')$

$c'$ $(c)' = 0$                                    $x'$ $(x)' = x'$

$+'$ $(e + \tilde{e})' = (e)' + (\tilde{e})'$           $\cdot'$ $(e \cdot \tilde{e})' = (e)' \cdot \tilde{e} + e \cdot (\tilde{e})'$

PROOF SKETCH. The soundness proofs for these axioms [32] carry over unchanged for extended term languages since fixed function symbols $h$ are interpreted as smooth $C^\infty$ functions.                    □

The differential effect axiom (DE) says that the differential variables $x'$ take on the values of the RHS along solutions to an ODE. This is expressed on its RHS with an assignment $x' := f(x)$ to the differential variable $x'$. The syntax and semantics of this (discrete) assignment are defined elsewhere [32] but it suffices to understand it here with the assignment axiom of dL:

$$[:=] \quad [x := e]\phi(x) \leftrightarrow \phi(e) \quad (e \text{ free for } x \text{ in } \phi)$$

Intuitively, axiom $[:=]$ says that property $\phi(x)$ is true after assigning $e$ to $x$ iff $\phi(e)$ is true right now. Together, axioms DE, $[:=]$ allow replacing free occurrences of $x'$ in the postcondition $P(x, x')$ yielding postcondition $P(x, f(x))$. However, proofs usually involve working with differentials of terms $(e)'$ rather than differential variables directly. This is where the differential axioms $(c', x', +', \cdot')$ are used. Axiom $c'$ says that the differential of a constant is 0, while axiom $x'$ says the differential of a variable $(x)'$ is the corresponding differential variable $x'$. Axioms $+', \cdot'$ are the sum and product rules of differentiation respectively. Soundness of these axioms allows differential terms to be rewritten equationally in all contexts, including in the postcondition of an ODE and within sub-terms. The differential axioms enable sound syntactic differentiation because differential terms $(e)'$ can be rewritten according to these equational axioms until no further differential sub-terms occur; any remaining differential variables are substituted away using DE, $[:=]$ under an ODE. Such *exhaustive use of differential axioms* is simply labeled as $(\ )'$ in proofs. The following example shows such a derivation concretely using a polynomial from the running example:

*Example 2.3 (Syntactic differentiation).* The following dL derivation syntactically differentiates the polynomial $v^2 - u^2 + \frac{9}{2}$ along the ODE $\alpha_e$ from (2) for any comparison operator $\sim$:

$$
\begin{array}{c}
\vdash [\alpha_e]4uv + \frac{1}{2}(1 - u^2 - v^2)(v^2 - u^2) \sim 0 \\
\hline
\mathbb{R} \quad \vdash [\alpha_e]2v(u + \frac{v}{4}(1 - u^2 - v^2)) - 2u(-v + \frac{u}{4}(1 - u^2 - v^2)) \sim 0 \\
\hline
[:=] \quad \vdash [\alpha_e][u' := -v + \frac{u}{4}(1 - u^2 - v^2)][v' := u + \frac{v}{4}(1 - u^2 - v^2)]2vv' - 2uu' \sim 0 \\
\hline
(\ )' \quad \vdash [\alpha_e][u' := -v + \frac{u}{4}(1 - u^2 - v^2)][v' := u + \frac{v}{4}(1 - u^2 - v^2)](v^2 - u^2 + \frac{9}{2})' \sim 0 \\
\hline
DE \quad \vdash [\alpha_e](v^2 - u^2 + \frac{9}{2})' \sim 0
\end{array}
$$

The first DE step makes available assignments on $u', v'$. The $(\ )'$ step is then used to syntactically simplify $(v^2 - u^2 + \frac{9}{2})'$ yielding $2vv' - 2uu'$. A subsequent use of $[:=]$ replaces the resulting differential variables $u', v'$ with their respective RHSes along the ODE. Finally, rule $\mathbb{R}$ is used to rearrange the calculated derivative arithmetically, which results in a (simplified) polynomial term.

Example 2.3 suggests that differentials can always be eliminated under an ODE. This is the case for differentials of polynomial terms $(p)'$, but differential axioms are needed for the fixed function

symbols. Consider the case of a unary fixed function symbol $h$ which is semantically interpreted as the function $h : \mathbb{R} \to \mathbb{R}$. Expanding the semantics of term $(h(e))'$ and applying the chain rule:

$$\omega[\![(h(e))']\!] = \sum_{x \in \mathbb{V}} \omega(x') \frac{\partial \omega[\![h(e)]\!]}{\partial x} = \sum_{x \in \mathbb{V}} \omega(x') \frac{\partial h}{\partial y}(\omega[\![e]\!]) \frac{\partial \omega[\![e]\!]}{\partial x}$$

$$= \frac{\partial h}{\partial y}(\omega[\![e]\!]) \sum_{x \in \mathbb{V}} \omega(x') \frac{\partial \omega[\![e]\!]}{\partial x} = \frac{\partial h}{\partial y}(\omega[\![e]\!]) \omega[\![(e)']\!]$$

The RHS product between $\frac{\partial h}{\partial y}(\omega[\![e]\!])$ and $\omega[\![(e)']\!]$ can be represented syntactically provided that the partial derivative of $h$ with respect to its argument is representable as a term. Assume (suggestively) that such a term is written as $\frac{\partial h}{\partial y}(e)$. The easiest case is to think of $\frac{\partial h}{\partial y}$ as another unary fixed function symbol and $\frac{\partial h}{\partial y}(e)$ as function application, hence the suggestive notation. This is not strictly necessary, however: $\frac{\partial h}{\partial y}$ can be another term that mentions variable $y$ free, in which case $\frac{\partial h}{\partial y}(e)$ corresponds to substituting $e$ for $y$ in that term. The differential axiom $h'$ for fixed function symbol $h$ uses a product of the (syntactic) partial derivative $\frac{\partial h}{\partial y}$ and differential $(e)'$ of $e$:

$$h' \quad (h(e))' \;=\; \frac{\partial h}{\partial y}(e) \cdot (e)'$$

*Example 2.4 (Unary extended differential axioms).* For the extended term language (1), the extended terms for the partial derivatives are as usual from calculus:

$$\frac{\partial \exp(y)}{\partial y} = \exp(y) \qquad \frac{\partial \sin(y)}{\partial y} = \cos(y) \qquad \frac{\partial \cos(y)}{\partial y} = -\sin(y)$$

Following the axiom schema $h'$, the differential axioms for these fixed function symbols are:

$$exp' \; (\exp(e))' \;=\; \exp(e) \cdot (e)' \quad sin' \; (\sin(e))' \;=\; \cos(e) \cdot (e)' \quad cos' \; (\cos(e))' \;=\; -\sin(e) \cdot (e)'$$

Axioms $sin'$, $cos'$ illustrate a syntactic subtlety. Fixed function symbols must only be introduced in a syntactically complete way with respect to differentials. The unary function symbol sin for the trigonometric sine function cannot be added without also adding one for the cosine function because there would otherwise be no way to express the differential of sin syntactically.[3]

The following lemma generalizes this syntactic representation condition and gives sound differential axioms for $k$-ary fixed function symbols:

LEMMA 2.5 (EXTENDED DIFFERENTIAL AXIOMS). *Let the $k$-ary fixed function symbol $h$ be semantically interpreted as a differentiable function $h : \mathbb{R}^k \to \mathbb{R}$. Suppose its partial derivative $\frac{\partial h}{\partial y_i}(y_1, \dots, y_k)$ at $y_1, \dots, y_k$ is syntactically represented by term $\frac{\partial h}{\partial y_i}$ for each $i$ such that $\omega[\![\frac{\partial h}{\partial y_i}(y_1, \dots, y_k)]\!] = \frac{\partial h}{\partial y_i}(\omega(y_1), \dots, \omega(y_k))$ for all states $\omega$. Then the differential axiom schema $h'$ for $h$ is sound:*

$$h' \quad (h(e_1, \dots, e_k))' \;=\; \sum_{i=1}^{k} \frac{\partial h}{\partial y_i}(e_1, \dots, e_k) \cdot (e_i)'$$

PROOF. The terms $\frac{\partial h}{\partial y_i}(e_1, \dots, e_k)$ appearing on the RHS of axiom $h'$ are understood as (syntactic) function application of $\frac{\partial h}{\partial y_i}$ to the arguments $e_1, \dots, e_k$. Soundness of this axiom follows from the

---

[3]Technically, $\pi$ could be added and $\cos(x)$ encoded as $\sin(x + \pi)$ but that also requires another 0-ary function symbol $\pi$.

(multivariate) chain rule and the semantics of differential terms. For any given state $\omega$:

$$\omega[\![(h(e_1, \ldots, e_k))']\!] = \sum_{x \in \mathbb{V}} \omega(x') \frac{\partial \omega[\![h(e_1, \ldots, e_k)]\!]}{\partial x} = \sum_{x \in \mathbb{V}} \omega(x') \sum_{i=1}^{k} \frac{\partial h}{\partial y_i}(\omega[\![e_1]\!], \ldots, \omega[\![e_k]\!]) \frac{\partial \omega[\![e_i]\!]}{\partial x}$$

$$= \sum_{i=1}^{k} \frac{\partial h}{\partial y_i}(\omega[\![e_1]\!], \ldots, \omega[\![e_k]\!]) \sum_{x \in \mathbb{V}} \omega(x') \frac{\partial \omega[\![e_i]\!]}{\partial x} = \sum_{i=1}^{k} \frac{\partial h}{\partial y_i}(\omega[\![e_1]\!], \ldots, \omega[\![e_k]\!]) \omega[\![(e_i)']\!]$$

$$= \sum_{i=1}^{k} \omega[\![\frac{\partial h}{\partial y_i}(e_1, \ldots, e_k)]\!] \omega[\![(e_i)']\!] = \omega[\![\sum_{i=1}^{k} \frac{\partial h}{\partial y_i}(e_1, \ldots, e_k)(e_i)']\!]$$

The penultimate step uses the fact that all partial derivatives are syntactically represented in the term language in order to replace a semantic function application with its syntactic representation.   □

With the differential axioms of Lemma 2.5, all differential terms $(e)'$ under an ODE $x' = f(x)$ can be axiomatically rewritten to another term not mentioning differentials and differential variables. This resulting term is the *Lie derivative* of term $e$ along ODE $x' = f(x)$, succinctly written as:

$$\mathcal{L}_{f(x)}(e) \stackrel{\text{def}}{=} \sum_{i=1}^{n} \frac{\partial e}{\partial x_i} \cdot f_i(x)$$

Unlike (semantic) time derivatives, Lie derivatives can be written down syntactically in the extended term language. Like time derivatives though, Lie derivatives still depend on the ODE context in which they are used, so they do not give a compositional means of defining syntactic differentiation. The use of differentials in dL solves this problem by giving a compositional term semantics that is defined independently of any hybrid programs or formulas. Along an ODE $x' = f(x)$, however, the value of Lie derivative $\mathcal{L}_{f(x)}(e)$ coincides with that of the differential $(e)'$ and dL allows transformation between the two by proof with the differential axioms [32]. The Lie derivative $\mathcal{L}_{f(x)}(e)$ is written as $\dot{e}$ when $x' = f(x)$ is clear from the context. The $i$-th *higher Lie derivative* $\dot{e}^{(i)}$ of term $e$ along the ODE $x' = f(x)$ is defined by iterating the Lie derivation operator:

$$\dot{e}^{(0)} \stackrel{\text{def}}{=} e, \quad \dot{e}^{(i+1)} \stackrel{\text{def}}{=} \mathcal{L}_{f(x)}(\dot{e}^{(i)}), \quad \dot{e} \stackrel{\text{def}}{=} \dot{e}^{(1)}$$

*2.3.2 Differential Equation Axiomatization.* Having enabled meaningful syntactic differentiation with differentials, it suffices to give axioms for working with differential equations. The following are the dL axioms for differential equations [32, Figure 3] as highlighted in Section 1. All axioms are understood for vectorial differential equations as described in Theorem 2.2 for axiom DE.

THEOREM 2.6 (DIFFERENTIAL EQUATION AXIOMATIZATION [32]). *The following are sound axioms of* dL. *In axiom DG, the $\exists$ quantifier can be replaced with a $\forall$ quantifier.*

   DI$_=$  $[x' = f(x) \& Q](e)' = 0 \rightarrow ([x' = f(x) \& Q]e = 0 \leftrightarrow (Q \rightarrow e = 0))$

   DI$_\succcurlyeq$  $[x' = f(x) \& Q](e)' \geq 0 \rightarrow ([x' = f(x) \& Q]e \succcurlyeq 0 \leftrightarrow (Q \rightarrow e \succcurlyeq 0))$    ($\succcurlyeq$ is either $\geq$ or $>$)

   DC  $[x' = f(x) \& Q]R \rightarrow ([x' = f(x) \& Q]P \leftrightarrow [x' = f(x) \& Q \wedge R]P)$

   DG  $[x' = f(x) \& Q]P \leftrightarrow \exists y\, [x' = f(x), y' = a(x)y + b(x) \& Q]P$

PROOF SKETCH. The soundness proofs for these axioms [32] carry over unchanged for extended term languages since fixed function symbols $h$ are interpreted as smooth $C^\infty$ functions.   □

*Differential invariants* (DI) reduce questions about invariance of $e = 0, e \succcurlyeq 0$ (globally, along solutions of the ODE) to local questions about differentials. Only two instances (DI$_=$, DI$_{\succcurlyeq}$) of the more general DI axiom [32] are needed here. Axiom DI$_=$ says that the value of extended term $e$ always stays zero if its differential $(e)'$ is always zero along the solution. Similarly, axiom DI$_{\succcurlyeq}$ says that $e$ stays non-negative (or strictly positive) if its differential is non-negative. Note that axiom DI$_{\succcurlyeq}$ only requires $(e)' \geq 0$ in its premise even for the $e > 0$ case. These axioms internalize the mean value theorem (see Appendix A.2). With the differential axioms of Section 2.3.1, the differential $(e)'$ can be soundly and syntactically transformed into the Lie derivative $\dot{e}$ in proofs. *Differential cut* (DC) expresses that if the system never leaves $R$ while staying in $Q$ (the outer assumption), then $R$ may be additionally assumed in the domain constraint when proving the postcondition $P$ (the last subformula). Even if DC increases the deductive power over DI [31], the deductive power increases even further [31] with the *differential ghost* axiom (DG) which adds a *fresh* variable $y$ to the system of ODEs for the sake of the proof. Since $y$ is fresh, its initial value can be either existentially (DG) or universally (DG$_\forall$) quantified [32]. The syntactic restriction of DG is that the new ODE must be linear (or affine) in $y$, hence $a(x), b(x)$ are not allowed to mention $y$. This restriction prevents the newly added equation from unsoundly restricting the duration of existence for solutions to the differential equations [31], e.g., the (unsound) differential ghost $y' = y^2$ may cause finite-time (or early) blowup of solutions [44]. The added differential ghost variable $y$ co-evolves along solutions and crucially enables the expression of new (integral) relationships between variables along the differential equations. These new relationships are then used to deduce invariance properties of interest in the original system. The systematic construction of appropriate differential ghosts is central to this article's completeness results. For example, the equational invariance axiom DI$_=$ is only complete for invariant functions [30]. In Section 3, axiom DG is used to extend this deductive power to all Darboux (in)equalities, Section 4 extends it further to *all* analytic invariants.

To utilize axioms DI, DC, DG in proofs, the following axiom and proof rule of dL are also used [32]:

$$\text{dW} \quad \frac{Q \vdash P}{\Gamma \vdash [x' = f(x) \,\&\, Q]P} \qquad\qquad \text{K} \quad [\alpha](\phi \to \psi) \to ([\alpha]\phi \to [\alpha]\psi)$$

*Differential weakening* (dW) drops the ODEs entirely and proves postcondition $P$ directly from the evolution domain constraint $Q$. Kripke axiom K is the modal modus ponens for postconditions of the box modality. Using dW and K, the following proof rule and axiom derive:

$$\text{M}['] \quad \frac{Q, \psi \vdash \phi \qquad \Gamma \vdash [x' = f(x) \,\&\, Q]\psi}{\Gamma \vdash [x' = f(x) \,\&\, Q]\phi} \qquad [\cdot]\wedge \quad [\alpha](\phi \wedge \psi) \leftrightarrow [\alpha]\phi \wedge [\alpha]\psi$$

Monotonicity rule M['] strengthens the postcondition to $\psi$ if it implies $\phi$ within the domain constraint $Q$ of the ODE $x' = f(x) \,\&\, Q$. Axiom $[\cdot]\wedge$ proves conjunctive postconditions separately, e.g., DI$_=$ derives from DI$_{\succcurlyeq}$ using $[\cdot]\wedge$ with the real arithmetic equivalence $e = 0 \leftrightarrow e \geq 0 \wedge -e \geq 0$.

## 2.4 Extended Term Conditions

Two natural conditions on the fixed function symbols $h \in \{h_1, \ldots, h_r\}$ and their semantics have been uncovered thus far. For this article's completeness results, a third condition is needed. All three *extended term conditions* are assumed throughout this article:

(S) *Smoothness.* All fixed function symbols $h \in \{h_1, \ldots h_r\}$ in the extended term language are interpreted as smooth $C^\infty$ functions $h : \mathbb{R}^k \to \mathbb{R}$.

(P) *Syntactic partial derivatives.* Each partial derivative $\frac{\partial h}{\partial y_i}$ of $h(y_1, \ldots, y_k)$ has a syntactic representation in the extended term language in the sense of Lemma 2.5.

(R) *Computable differential radicals.* The extended term language has computable differential radicals, i.e., for each extended term $e$ and ODE $x' = f(x)$ with extended terms in its RHS $f(x)$, there must computably exist an $N \geq 1$ and $N$ extended terms $g_i$ such that the higher Lie derivatives of $e$ along $x' = f(x)$ provably satisfy the following *differential radical identity* [15]:

$$\dot{e}^{(N)} = \sum_{i=0}^{N-1} g_i \dot{e}^{(i)} \tag{3}$$

Condition (S) ensures that the semantics are well-defined, while conditions (P) and (R) enable (complete) *syntactic* analysis of differential equations invariance by their local (differential) behavior. The $C^\infty$ smoothness required by (S) is subtly weaker than *real analyticity* [20]. This article often gives brief but intuitive (semantic) explanations of results, and explicitly indicates when those arguments only apply *in the real analytic setting*. None of the actual proofs given in this article require real analyticity. Condition (R) requires an algorithm that computes and proves the identity (3). This identity is crucially used for completeness in Section 4 and Section 6, where it is also motivated logically. It yields a finiteness property on the number of Lie derivatives that need to be analyzed for any given term $e$ and ODE. From identity (3), the first $N - 1$ Lie derivatives will turn out to suffice for completely determining the local behavior of extended term $e$ along the ODE $x' = f(x)$. All three extended term conditions are met by the polynomial term language without extensions.

PROPOSITION 2.7. *Polynomial term languages satisfy the extended term conditions.*

PROOF SKETCH. A full proof is omitted because this is a corollary of a later result (Theorem 7.7). Briefly, conditions (S) and (P) are met because polynomial functions are smooth (even real analytic) and the polynomials are closed under partial derivatives. Condition (R) generalizes different flavors of results that have been proved in the literature [15, 22, 25]. The proofs rely on the fact that polynomials form a Noetherian ring [6] so that the ascending chain of ideals[4] formed by successive (polynomial) Lie derivatives stabilizes. The resulting (polynomial) identity (3) is a formula of real arithmetic and can therefore always be proved by the rule ℝ for decidable real arithmetic.  □

It is less straightforward to show that an extended term language like (1) meets these conditions. Indeed, even the simple language extension (1) already features exponential rings which are not Noetherian [40, Remark 1.4.2] and undecidable arithmetic over the trigonometric functions [36]. In the interest of a general presentation, the question of how to determine if a candidate term language extension $\{h_1, \ldots, h_r\}$ meets the extended term conditions is deferred till Section 7. Until then, the only assumption about the extended term language is that it satisfies these three conditions. This suffices for the completeness results, which the next section begins to show.

## 3  DARBOUX INVARIANTS

This section exploits differential ghosts for proving an important class of invariance properties. These are called *Darboux invariants* because they are inspired by Darboux polynomials [9]. The derived proof rule for Darboux equalities corresponds to the case $N = 1$ in the differential radical identity (3), while the subsequent rule for Darboux *ine*qualities is a crucial step for the completeness result in Section 4. Their derivations also show how analytic and geometric notions from the theory of differential equations, such as Darboux polynomials [9] and Grönwall's lemma [18, 44, §29.VI] can be internalized syntactically with differential ghost arguments without extension to any axiom.

---

[4]The *ideal* [4] generated by polynomials $p_1, \ldots, p_s \in \mathbb{R}[x]$ is the set of all their linear combination with polynomial cofactors $g_i \in \mathbb{R}[x]$, denoted by $(p_1, \ldots, p_s) \overset{\text{def}}{=} \{\sum_{i=1}^s g_i p_i \ : \ g_i \in \mathbb{R}[x]\}$.

### 3.1 Darboux Equalities

Assume that the extended term $e$ satisfies the differential radical identity (3) with $N = 1$ and extended term cofactor $g$, i.e., $\dot{e} = ge$. Taking Lie derivatives on both sides gives:

$$\dot{e}^{(2)} = \mathcal{L}_{f(x)}(\dot{e}) = \mathcal{L}_{f(x)}(ge) = \dot{g}e + g\dot{e} = (\dot{g} + g^2)e$$

By repeatedly taking Lie derivatives, *all* higher Lie derivatives of $e$ can be written as a product between $e$ and some cofactor. Now, consider an initial state $\omega$ where $e$ evaluates to $\omega[\![e]\!] = 0$, then:

$$\omega[\![\dot{e}]\!] = \omega[\![ge]\!] = \omega[\![g]\!] \cdot \omega[\![e]\!] = 0$$

Because every higher Lie derivative is a product with $e$, all of them are simultaneously 0 in state $\omega$. Thus, *in the real analytic setting*, $e = 0$ stays invariant along solutions to the ODE starting at $\omega$ because all its derivatives are 0. This motivates the following proof rule for invariance of $e = 0$:

$$\text{dbx} \quad \frac{Q \vdash \dot{e} = ge}{e = 0 \vdash [x' = f(x)\,\&\,Q]e = 0}$$

Rule dbx derives using differential ghosts and is a first hint at their deductive power for equational invariants. A special case of dbx proves invariance for *Darboux polynomials*, which are polynomials $p$ satisfying the polynomial identity $\dot{p} = gp$ for some polynomial cofactor $g$. These are of significant interest in the study of (polynomial) ODEs [9] and invariant generation for hybrid systems [37]. In Section 4, dbx is generalized vectorially to yield proofs of *all* analytic invariants with differential ghosts. Although the rule can be derived from DG directly, this article follows a detour through a proof rule for Darboux *in*equalities instead, which is crucially used for this vectorial generalization.

### 3.2 Darboux Inequalities

Assume that the extended term $e$ satisfies the Darboux *inequality* $\dot{e} \geq ge$ for some extended term cofactor $g$. Semantically, in an initial state $\omega$ where $\omega[\![e]\!] \geq 0$, Grönwall's lemma [18, 44, §29.VI] implies that $e \geq 0$ stays invariant along solutions starting at $\omega$ because the semantic value of extended term $e$ is bounded below by a (typically decaying) non-negative exponential solution of the non-autonomous linear differential equation $e' = g(t)e$ for the variable $e$. Here, $g(t)$ is the time-dependent function corresponding to the value of term $g$ evaluated along the solution to the differential equations $x' = f(x)$ from $\omega$, see Fig. 2a for an illustration. Indeed, if $e$ satisfies the Darboux equality $\dot{e} = ge$ with cofactor $g$, then it satisfies both Darboux inequalities $\dot{e} \geq ge$ and $\dot{e} \leq ge$, giving an alternative semantic argument for the invariance of $e = 0$ in rule dbx.

Differentials and Lie derivatives along differential equations $x' = f(x)$ provably coincide (Section 2.3.1), so axiomatic Darboux inequalities assume $[x' = f(x)\,\&\,Q](e)' \geq ge$ and Darboux equalities assume $[x' = f(x)\,\&\,Q](e)' = ge$ instead of $\dot{e} \geq ge$ and $\dot{e} = ge$, respectively. Darboux (in)equality invariance can be proved purely syntactically with the differential ghost axiom DG.

LEMMA 3.1 (DARBOUX (IN)EQUALITIES ARE DIFFERENTIAL GHOSTS). *The Darboux equality DBX and Darboux inequality $DBX_{\succcurlyeq}$ axioms derive from DG (and DI, DC) for any extended term cofactor $g$.*

DBX $\quad [x' = f(x)\,\&\,Q](e)' = ge \rightarrow (e = 0 \rightarrow [x' = f(x)\,\&\,Q]e = 0)$

$DBX_{\succcurlyeq}$ $\quad [x' = f(x)\,\&\,Q](e)' \geq ge \rightarrow (e \succcurlyeq 0 \rightarrow [x' = f(x)\,\&\,Q]e \succcurlyeq 0) \qquad (\succcurlyeq \text{ is either } \geq \text{ or } >)$

PROOF. Axiom $DBX_{\succcurlyeq}$ is derived first before axiom DBX is derived as a corollary. After propositional normalization, the derivation starts with a DG, DG$_\forall$ step, introducing a new ghost variable $y$ satisfying a carefully chosen differential equation $y' = -gy$. Next, $\exists$R, $\forall$L pick an initial value for $y$.

It suffices to pick any $y > 0$. The augmented ODE is abbreviated with $\alpha_y \equiv x' = f(x), y' = -gy$:

$$
\begin{array}{c}
\dfrac{[\alpha_y \,\&\, Q](e)' \geq ge, e \succcurlyeq 0, y > 0 \vdash [\alpha_y \,\&\, Q]e \succcurlyeq 0}{} \\[2pt]
{\scriptstyle \exists R, \forall L} \dfrac{\forall y\,[\alpha_y \,\&\, Q](e)' \geq ge, e \succcurlyeq 0 \vdash \exists y\,[\alpha_y \,\&\, Q]e \succcurlyeq 0}{} \\[2pt]
{\scriptstyle DG, DG_\forall} \overline{[x' = f(x) \,\&\, Q](e)' \geq ge, e \succcurlyeq 0 \vdash [x' = f(x) \,\&\, Q]e \succcurlyeq 0}
\end{array}
$$

The augmented ODE $\alpha_y$ has a new provable invariant relationship $ey \succcurlyeq 0$ (see Fig. 2 and discussion after this proof). To deduce the original property of interest ($e \succcurlyeq 0$) from this new relationship, it suffices to prove $y > 0$ invariant because the formula $ey \succcurlyeq 0 \wedge y > 0 \to e \succcurlyeq 0$ is provable by $\mathbb{R}$. Axiom DC is used to prove $y > 0$ separately (right premise abbreviated with ①) and assume it in the evolution domain constraints of the left premise. Subsequently, monotonicity rule $M[']$ and $\mathbb{R}$ strengthen the postcondition to $ey \succcurlyeq 0$ using the newly added domain constraint $y > 0$.

$$
\begin{array}{c}
{\scriptstyle M['], \mathbb{R}} \dfrac{[\alpha_y \,\&\, Q \wedge y > 0](e)' \geq ge, e \succcurlyeq 0, y > 0 \vdash [\alpha_y \,\&\, Q \wedge y > 0]ey \succcurlyeq 0}{[\alpha_y \,\&\, Q \wedge y > 0](e)' \geq ge, e \succcurlyeq 0, y > 0 \vdash [\alpha_y \,\&\, Q \wedge y > 0]e \succcurlyeq 0 \qquad ①} \\[2pt]
{\scriptstyle DC} \overline{[\alpha_y \,\&\, Q](e)' \geq ge, e \succcurlyeq 0, y > 0 \vdash [\alpha_y \,\&\, Q]e \succcurlyeq 0}
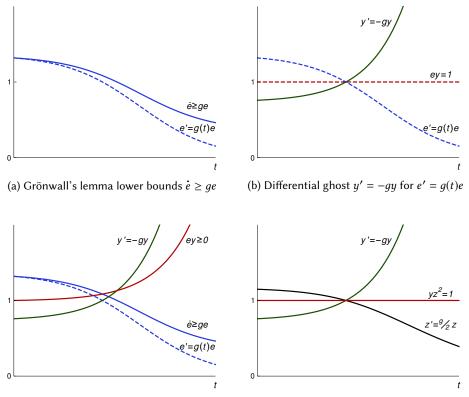\end{array}
$$

From the left premise, a cut, $\mathbb{R}$ step adds $ey \succcurlyeq 0$ to the assumptions using the provable arithmetic formula $e \succcurlyeq 0 \wedge y > 0 \to ey \succcurlyeq 0$. Axiom $DI_{\succcurlyeq}$ is used to prove the inequational invariant $ey \succcurlyeq 0$ and the resulting differential $(ey)'$ simplifies with $(\,)'$ from Section 2.3.1. An additional DE, $[:=]$ step replaces the differential variable $y'$ according to the augmented ODE $\alpha_y$, before a monotonicity $M[']$ (with a cut) and $\mathbb{R}$ step closes the derivation using the domain constraint $y > 0$. The differential ghost $y' = -gy$ is specifically crafted so that this final arithmetic step proves with $\mathbb{R}$.

$$
\begin{array}{c}
\qquad\qquad\qquad * \\
{\scriptstyle \mathbb{R}} \overline{(e)' \geq ge, y > 0 \vdash (e)'y + e(-gy) \geq 0} \\[2pt]
{\scriptstyle M[']} \overline{[\alpha_y \,\&\, Q \wedge y > 0](e)' \geq ge \vdash [\alpha_y \,\&\, Q \wedge y > 0](e)'y + e(-gy) \geq 0} \\[2pt]
{\scriptstyle DE, [:=]} \overline{[\alpha_y \,\&\, Q \wedge y > 0](e)' \geq ge \vdash [\alpha_y \,\&\, Q \wedge y > 0](e)'y + ey' \geq 0} \\[2pt]
{\scriptstyle (\,)'} \overline{[\alpha_y \,\&\, Q \wedge y > 0](e)' \geq ge \vdash [\alpha_y \,\&\, Q \wedge y > 0](ey)' \geq 0} \\[2pt]
{\scriptstyle DI_{\succcurlyeq}} \overline{[\alpha_y \,\&\, Q \wedge y > 0](e)' \geq ge, ey \succcurlyeq 0 \vdash [\alpha_y \,\&\, Q \wedge y > 0]ey \succcurlyeq 0} \\[2pt]
{\scriptstyle cut, \mathbb{R}} \overline{[\alpha_y \,\&\, Q \wedge y > 0](e)' \geq ge, e \succcurlyeq 0, y > 0 \vdash [\alpha_y \,\&\, Q \wedge y > 0]ey \succcurlyeq 0}
\end{array}
$$

The derivation continues from premise ① with a second differential ghost $z' = \frac{g}{2}z$ analogously:

$$
\begin{array}{c}
\qquad\qquad * \\
{\scriptstyle \mathbb{R}} \overline{Q \vdash (-gy)z^2 + 2yz(\frac{g}{2}z) = 0} \\[2pt]
{\scriptstyle dW} \overline{\vdash [x' = f(x), y' = -gy, z' = \frac{g}{2}z \,\&\, Q](-gy)z^2 + 2yz(\frac{g}{2}z) = 0} \\[2pt]
{\scriptstyle DE, [:=]} \overline{\vdash [x' = f(x), y' = -gy, z' = \frac{g}{2}z \,\&\, Q]y'z^2 + 2yzz' = 0} \\[2pt]
{\scriptstyle DI_=, (\,)'} \overline{yz^2 = 1 \vdash [x' = f(x), y' = -gy, z' = \frac{g}{2}z \,\&\, Q]yz^2 = 1} \\[2pt]
{\scriptstyle \exists R, M['], \mathbb{R}} \overline{y > 0 \vdash \exists z\,[x' = f(x), y' = -gy, z' = \frac{g}{2}z \,\&\, Q]y > 0} \\[2pt]
{\scriptstyle DG} \overline{y > 0 \vdash [x' = f(x), y' = -gy \,\&\, Q]y > 0}
\end{array}
$$

In the $\exists R, M['], \mathbb{R}$ step, observe that if $y > 0$ initially, then there exists $z$ such that $yz^2 = 1$. Moreover, $yz^2 = 1$ is sufficient to imply $y > 0$ in the postcondition. Rule $\mathbb{R}$ again applies here since both of these are properties of real arithmetic. The differential ghost $z' = \frac{g}{2}z$ is specifically constructed so that $yz^2 = 1$ can be proved invariant along the differential equation.

(a) Grönwall's lemma lower bounds $\dot{e} \geq ge$

(b) Differential ghost $y' = -gy$ for $e' = g(t)e$

(c) Differential ghost $y' = -gy$ for $\dot{e} \geq ge$

(d) Differential ghost $z' = \frac{g}{2}z$ for $y' = -gy$

Fig. 2. The horizontal axis tracks the evolution of time $t$ along solutions. Dashed lines indicate steps based on semantical arguments while solid lines indicate constructions used in the syntactical proof of Lemma 3.1. (a) Solutions of $\dot{e} \geq ge$ (solid blue) are bounded below by those of the non-autonomous linear differential equation $e' = g(t)e$ (dashed blue) by Grönwall's lemma. (b) The differential ghost $y' = -gy$ (solid green) balances out $e' = g(t)e$ so that the value of $ey$ (dashed red) remains constant at 1. (c) The same ghost $y' = -gy$ also balances out $\dot{e} \geq ge$, where the value of $ey$ (solid red) remains non-negative but not necessarily constant. (d) A second differential ghost $z' = \frac{g}{2}z$ (solid black) balances out $y' = -gy$ so that the value of $yz^2$ (solid red) remains constant at 1. The constant 1 in the RHS of $ey = 1$ and $yz^2 = 1$ in (b) and (d) respectively is chosen for simplicity. Any positive constant suffices with appropriate initial values of the differential ghosts.

Axiom DBX derives using the derived axiom $[\cdot]\wedge$, the equivalence $e = 0 \leftrightarrow e \geq 0 \wedge -e \geq 0$ by $\mathbb{R}$, and the equality $(-e)' = -(e)'$ provable by $(\ )'$. The ODE is abbreviated with $\alpha_x \equiv x' = f(x) \,\&\, Q$:

$$
\begin{array}{c}
\text{DBX}_{\succcurlyeq}, \wedge\text{L}, \wedge\text{R} \cfrac{\qquad\qquad\qquad *}{[\alpha_x](e)' \geq ge \wedge [\alpha_x](-e)' \geq g(-e), e \geq 0 \wedge -e \geq 0 \vdash [\alpha_x]e \geq 0 \wedge [\alpha_x]-e \geq 0} \\
[\cdot]\wedge \cfrac{}{[\alpha_x]((e)' \geq ge \wedge (-e)' \geq g(-e)), e \geq 0 \wedge -e \geq 0 \vdash [\alpha_x](e \geq 0 \wedge -e \geq 0)} \\
\text{M}[\ '], \mathbb{R} \cfrac{}{[x' = f(x) \,\&\, Q](e)' = ge, e = 0 \vdash [x' = f(x) \,\&\, Q]e = 0} \qquad\qquad \square
\end{array}
$$

The first two syntactic derivation steps in the derivation of DBX$_{\succcurlyeq}$ do not appear to have changed the sequent much, but they correspond to a significant geometric transformation of the problem, as illustrated in Fig. 2b and Fig. 2c. In the system extended with differential ghost $y$, there is now a *new*

invariant $ey \succcurlyeq 0$ which can be observed along solutions! While the value of $e$ decays (dangerously) towards 0, the chosen differential equation $y' = -gy$ yields an (integral) value for $y$ that counteracts this change, ensuring that their product still always stays non-negative along all solutions. In fact, the value of $ey$ even remains constant when the extended term $e$ satisfies the equational identity $\dot{e} = ge$. The second differential ghost $z' = \frac{g}{2}z$ in the proof is similarly constructed so that $yz^2 = 1$ can be proved invariant *along the differential equation*. The geometric transformation from this second syntactic differential ghost is illustrated in Fig. 2d. Since the first differential ghost $y$ satisfies a differential *equation*, the second ghost $z$ exactly balances it out with the value of $yz^2$ remaining (provably) constant and positive at 1 along solutions (similarly to Fig. 2b).

The derivation of $\text{DBX}_{\succcurlyeq}$ illustrates how the ODE axioms of dL (DI, DC, DG) complement each other in proofs of ODE invariance. For brevity, the same derivation is used for both $\geq$ and $>$ cases of $\text{DBX}_{\succcurlyeq}$ even though the latter only needs one ghost (using $y' = -\frac{g}{2}y$ and invariant $ey^2 > 0$ instead). Axiom DBX also derives directly (similarly to $\text{DBX}_{\succcurlyeq}$, using the invariant $ey = 0$ instead) using just two differential ghosts rather than the four incurred with $[\cdot]\wedge$.

COROLLARY 3.2 (DARBOUX (IN)EQUALITY RULES). *The Darboux equality dbx and Darboux inequality $dbx_{\succcurlyeq}$ proof rules derive from DG (and DI, DC) for any extended cofactor term g.*

$$\text{dbx} \ \frac{Q \vdash \dot{e} = ge}{e = 0 \vdash [x' = f(x) \,\&\, Q]e = 0} \qquad \text{dbx}_{\succcurlyeq} \ \frac{Q \vdash \dot{e} \geq ge}{e \succcurlyeq 0 \vdash [x' = f(x) \,\&\, Q]e \succcurlyeq 0} \quad (\succcurlyeq \text{ is either } \geq \text{ or } >)$$

PROOF. The dbx proof rule derives from axiom DBX (and rule $\text{dbx}_{\succcurlyeq}$ from axiom $\text{DBX}_{\succcurlyeq}$) using an additional $(\ )'$, DE step to turn the differential $(e)'$ into the Lie derivative followed by a dW step:

$$
\begin{array}{cc}
\begin{array}{l}
\text{dW} \quad \dfrac{Q \vdash \dot{e} = ge}{\vdash [x' = f(x) \,\&\, Q]\dot{e} = ge} \\[2pt]
(\ )', \text{DE}, [:=] \quad \dfrac{}{\vdash [x' = f(x) \,\&\, Q](e)' = ge} \\[2pt]
\text{DBX} \quad \dfrac{}{e = 0 \vdash [x' = f(x) \,\&\, Q]e = 0}
\end{array}
&
\begin{array}{l}
\text{dW} \quad \dfrac{Q \vdash \dot{e} \geq ge}{\vdash [x' = f(x) \,\&\, Q]\dot{e} \geq ge} \\[2pt]
(\ )', \text{DE}, [:=] \quad \dfrac{}{\vdash [x' = f(x) \,\&\, Q](e)' \geq ge} \\[2pt]
\text{DBX}_{\succcurlyeq} \quad \dfrac{}{e \succcurlyeq 0 \vdash [x' = f(x) \,\&\, Q]e \succcurlyeq 0}
\end{array}
\quad \square
\end{array}
$$

Axioms DBX, $\text{DBX}_{\succcurlyeq}$ yield particularly efficient proofs within dL's uniform substitution calculus [32]. They derive once-and-for-all, independently of the ODE $x' = f(x)$. Subsequently substituting [32] for specific ODE instances means that only the final Lie derivative calculation steps DE, $(\ )'$, [:=] are needed for each concrete derived instance of dbx, $\text{dbx}_{\succcurlyeq}$.

The following example shows a concrete proof utilizing the newly derived proof rules.

*Example 3.3 (Proving ODE properties in* dL*).* Judging by the plot (Fig. 1) of the ODE $\alpha_e$ from (2), trajectories from within the open (or closed) disk stay trapped within the disk. Rather than relying (informally) on a potentially incorrect plot though, this fact can be shown formally by proving that $e \succcurlyeq 0$, with $e = 1 - u^2 - v^2$, is an invariant of $\alpha_e$. By calculating the Lie derivative:

$$\mathcal{L}_{\alpha_e}(e) = -2u\left(-v + \frac{u}{4}(1 - u^2 - v^2)\right) - 2v\left(u + \frac{v}{4}(1 - u^2 - v^2)\right) = -\frac{1}{2}(u^2 + v^2)e$$

Thus, $e$ satisfies the (polynomial) inequality $\dot{e} \geq ge$ with polynomial cofactor $g = -\frac{1}{2}(u^2 + v^2)$. The following derivation with $\text{dbx}_{\succcurlyeq}$ proves invariance of $1 - u^2 - v^2 \succcurlyeq 0$:

$$
\text{dbx}_{\succcurlyeq} \ \dfrac{\mathbb{R} \ \dfrac{*}{\vdash \mathcal{L}_{\alpha_e}(1 - u^2 - v^2) \geq -\frac{1}{2}(u^2 + v^2)(1 - u^2 - v^2)}}{1 - u^2 - v^2 \succcurlyeq 0 \vdash [\alpha_e]1 - u^2 - v^2 \succcurlyeq 0}
$$

The term $e$ obeys the special case $\dot{e} = ge$ (Fig. 2b) in which the seemingly innocuous syntactic introduction of a differential ghost $y' = -gy$ even *exactly* balances out the complicated (decaying)

evolution of $e$ geometrically. Indeed, in this case, $e = 0$ can also be proved invariant for the ODE $\alpha_e$ using rule dbx. This proves the observation from Fig. 1 that the unit circle is also invariant for $\alpha_e$.

The derivations of axioms DBX, DBX$_{\succeq}$ give constructive choices of differential ghosts when the invariant is a Darboux (in)equality. The derived rule dbx$_{\succeq}$ exceeds the deductive power of DI, DC because the formula $y > 0 \rightarrow [y' = -y]y > 0$ is easily provable by dbx$_{\succeq}$ using the Darboux equality $\dot{y} = -y$, but is *not* provable with DI, DC alone [31]. The next section builds on these constructions, showing that the deductive power afforded by axiom DG extends to *all* true analytic invariants.

## 4 ANALYTIC INVARIANTS

Analytic formulas are formed from finite conjunctions and disjunctions of equalities, but, over $\mathbb{R}$, can be normalized to a single equality $e = 0$ using the provable real arithmetic equivalences: $e = 0 \land \tilde{e} = 0 \leftrightarrow e^2 + \tilde{e}^2 = 0$ and $e = 0 \lor \tilde{e} = 0 \leftrightarrow e\tilde{e} = 0$. Thus, it suffices to restrict attention to equational formulas $e = 0$ when proving completeness for analytic invariants.

The key to completeness is the differential radical identity (3) for $e$ with arbitrary rank $N \geq 1$, which analyzes *all* higher Lie derivatives simultaneously. Suppose that extended term $e$ satisfies identity (3) with rank $N$ and some cofactors $g_i$. Taking Lie derivatives on both sides of (3) yields:

$$\dot{e}^{(N+1)} = \mathcal{L}_{f(x)}(\dot{e}^{(N)}) = \mathcal{L}_{f(x)}(\sum_{i=0}^{N-1} g_i \dot{e}^{(i)}) = \sum_{i=0}^{N-1} \mathcal{L}_{f(x)}(g_i \dot{e}^{(i)}) = \sum_{i=0}^{N-1} \left(\dot{g}_i \dot{e}^{(i)} + g_i \dot{e}^{(i+1)}\right)$$

$$= \sum_{i=0}^{N-1} \left(\dot{g}_i \dot{e}^{(i)}\right) + \sum_{i=0}^{N-2} \left(g_i \dot{e}^{(i+1)}\right) + g_{N-1}\dot{e}^{(N)} = \sum_{i=0}^{N-1} \left(\dot{g}_i \dot{e}^{(i)}\right) + \sum_{i=0}^{N-2} \left(g_i \dot{e}^{(i+1)}\right) + g_{N-1}\left(\sum_{i=0}^{N-1} g_i \dot{e}^{(i)}\right)$$

The last step follows using (3) to expand $\dot{e}^{(N)}$. Observe that the resulting expression for $\dot{e}^{(N+1)}$ is again a sum over the lower Lie derivatives $\dot{e}^{(i)}$ for $i = 0, \ldots, N-1$ multiplied by appropriate cofactors. By repeatedly taking Lie derivatives on both sides, the higher Lie derivatives $\dot{e}^{(N)}, \dot{e}^{(N+1)}, \ldots$ can all be written as sums over these lower Lie derivatives with appropriate cofactors. Thus, *in the real analytic setting*, for initial states $\omega$ where $\omega[\![e]\!], \omega[\![\dot{e}]\!], \ldots, \omega[\![\dot{e}^{(N-1)}]\!]$ all simultaneously evaluate to $0$, $e = 0$ (*and similarly for all its higher Lie derivatives*) stays invariant along solutions to the ODE.

This suggests that rule dbx should be generalized by considering higher Lie derivatives. The canonical technique for generalizing to higher derivatives comes from the study of ODEs. All (explicit form) ordinary differential equations involving higher derivatives can be transformed into vectorial systems of differential equations involving only first derivatives but possibly over a vector of variables [44, §11.I]. This transformation can be done syntactically and is precisely the idea used to derive the (complete) proof rule for analytic invariants by reduction to a suitable vectorial generalization of rule dbx. This crucial vectorial generalization is derived first.

### 4.1 Vectorial Darboux Equalities

Suppose that the $m$-dimensional vector of extended terms $\mathbf{e}$ satisfies the vectorial identity $\dot{\mathbf{e}} = G\mathbf{e}$, where $G$ is an $m \times m$ matrix of extended terms and $\dot{\mathbf{e}}$ denotes component-wise Lie derivatives of vector $\mathbf{e}$ along $x' = f(x)$, just like $(\mathbf{e})'$ denotes component-wise differentials. If all components of $\mathbf{e}$ evaluate to $0$ in an initial state, then they all always stay at $0$ along $x' = f(x)$ because their component-wise Lie derivatives *all* evaluate to $0$ in that initial state.

LEMMA 4.1 (VECTORIAL DARBOUX EQUALITIES ARE DIFFRENTIAL GHOSTS). *The vectorial Darboux axiom VDBX derives from DG (and DI, DC), where $G$ is an $m \times m$ cofactor matrix of extended terms and $\mathbf{e}$ is an $m$-dimensional vector of extended terms.*

$$\text{VDBX} \quad [x' = f(x) \,\&\, Q](\mathbf{e})' = G\mathbf{e} \rightarrow (\mathbf{e} = 0 \rightarrow [x' = f(x) \,\&\, Q]\mathbf{e} = 0)$$

PROOF. First, observe that the formula $\mathbf{e} = 0$ is provably equivalent in real arithmetic to the formula $-\|\mathbf{e}\|_2^2 \geq 0$, where the term $\|\mathbf{e}\|_2^2 \overset{\text{def}}{=} \sum_{i=1}^m \mathbf{e}_i^2$ is the *squared* Euclidean norm of vector $\mathbf{e}$. The derivation starts with M['], cut and ℝ to rephrase $\mathbf{e} = 0$ using this equivalence:

$$
\begin{array}{cc}
& * \\
\hline
(\,)',\mathbb{R} & (\mathbf{e})' = G\mathbf{e} \vdash (-\|\mathbf{e}\|_2^2)' \geq g(-\|\mathbf{e}\|_2^2) \\
\hline
\text{M['']} & [x' = f(x)\,\&\,Q](\mathbf{e})' = G\mathbf{e} \vdash [x' = f(x)\,\&\,Q](-\|\mathbf{e}\|_2^2)' \geq g(-\|\mathbf{e}\|_2^2) \\
\hline
\text{DBX}_{\succcurlyeq} & [x' = f(x)\,\&\,Q](\mathbf{e})' = G\mathbf{e}, \; -\|\mathbf{e}\|_2^2 \geq 0 \vdash [x' = f(x)\,\&\,Q]-\|\mathbf{e}\|_2^2 \geq 0 \\
\hline
\text{M['], cut, }\mathbb{R} & [x' = f(x)\,\&\,Q](\mathbf{e})' = G\mathbf{e}, \; \mathbf{e} = 0 \vdash [x' = f(x)\,\&\,Q]\mathbf{e} = 0
\end{array}
$$

Thanks to this rephrasing, the sequent no longer contains vectorial quantities and the derivation is completed using a (scalar) DBX$_{\succcurlyeq}$ step with the extended term cofactor $g = \|G\|_F^2 + 1$, where the term $\|G\|_F^2 \overset{\text{def}}{=} \sum_{i=1}^m \sum_{j=1}^m G_{ij}^2$ is the squared Frobenius norm of matrix $G$. All that remains is to justify the final $(\,)', \mathbb{R}$ step after M['] by showing that the following arithmetic formula is provable:

$$(\mathbf{e})' = G\mathbf{e} \;\rightarrow\; (-\|\mathbf{e}\|_2^2)' \geq g(-\|\mathbf{e}\|_2^2) \tag{4}$$

The differential $(-\|\mathbf{e}\|_2^2)'$ is calculated (and proved via $(\,)'$ from Section 2.3.1) as follows, where $\mathbf{u} \cdot \mathbf{v}$ denotes the dot product of vectors $\mathbf{u}, \mathbf{v}$. The last step uses $(\mathbf{e})' = G\mathbf{e}$:

$$(-\|\mathbf{e}\|_2^2)' = -\Big(\sum_{i=1}^m \mathbf{e}_i^2\Big)' = -2\sum_{i=1}^m \mathbf{e}_i(\mathbf{e}_i)' = -2(\mathbf{e}\cdot(\mathbf{e})') = -2(\mathbf{e}\cdot(G\mathbf{e}))$$

Thus, it suffices to prove the validity of $-2(\mathbf{e}\cdot(G\mathbf{e})) \geq g(-\|\mathbf{e}\|_2^2)$, i.e., its truth in all states $\omega$. Validity is first shown semantically. For ease of notation, let $\omega[\![\mathbf{e}]\!]$, $\omega[\![G]\!]$ stand for the respective real vector and matrix values of $\mathbf{e}$ and $G$ evaluated component-wise in state $\omega$. The notation $\|\cdot\|_2$, $\|\cdot\|_F$ denotes the (real-valued) Euclidean and Frobenius norms for vectors and matrices respectively.

By the Cauchy-Schwarz inequality [44, §28.I], the dot product between vectors $\omega[\![\mathbf{e}]\!]$ and $\omega[\![G]\!]\omega[\![\mathbf{e}]\!]$ is bounded by the product of their norms:

$$\omega[\![\mathbf{e}]\!] \cdot (\omega[\![G]\!]\omega[\![\mathbf{e}]\!]) \leq \|\omega[\![\mathbf{e}]\!]\|_2 \, \|\omega[\![G]\!]\omega[\![\mathbf{e}]\!]\|_2$$

The norm $\|\omega[\![G]\!]\omega[\![\mathbf{e}]\!]\|_2$ of this matrix-vector product is bounded by the product of their matrix and vector norms because the Euclidean and Frobenius norms are compatible [44, §14.II]:

$$\|\omega[\![G]\!]\omega[\![\mathbf{e}]\!]\|_2 \leq \|\omega[\![G]\!]\|_F \, \|\omega[\![\mathbf{e}]\!]\|_2$$

Expanding the (square) inequality $0 \leq (\|\omega[\![G]\!]\|_F - 1)^2$ yields an upper bound on the Frobenius norm $\|\omega[\![G]\!]\|_F$ by its squared value:

$$2\|\omega[\![G]\!]\|_F \leq \|\omega[\![G]\!]\|_F^2 + 1$$

Chaining these (in)equalities yields:

$$
\begin{aligned}
\omega[\![-2(\mathbf{e}\cdot(G\mathbf{e}))]\!] &= -2(\omega[\![\mathbf{e}]\!]\cdot(\omega[\![G]\!]\omega[\![\mathbf{e}]\!])) \geq -2\|\omega[\![\mathbf{e}]\!]\|_2 \, \|\omega[\![G]\!]\omega[\![\mathbf{e}]\!]\|_2 \\
&\geq -2\|\omega[\![\mathbf{e}]\!]\|_2 \, \|\omega[\![G]\!]\|_F \, \|\omega[\![\mathbf{e}]\!]\|_2 = -2\|\omega[\![G]\!]\|_F \, \|\omega[\![\mathbf{e}]\!]\|_2^2 \\
&\geq (\|\omega[\![G]\!]\|_F^2 + 1)(-\|\omega[\![\mathbf{e}]\!]\|_2^2) = \omega[\![g(-\|\mathbf{e}\|_2^2)]\!]
\end{aligned}
$$

where $\|\omega[\![G]\!]\|_F^2 + 1$ is precisely the semantic value of cofactor $g$ in state $\omega$. Since this semantic argument for the validity of implication (4) only depends on first-order properties of the real closed fields, which is decidable [4], formula (4) is provable syntactically by $(\,)', \mathbb{R}$. □

COROLLARY 4.2 (VECTORIAL DARBOUX EQUALITY RULE). *The vectorial Darboux equality proof rule* vdbx *derives from* DG *(and* DI, DC*), where G is an $m \times m$ cofactor matrix of extended terms and* **e** *is an m-dimensional vector of extended terms.*

$$\text{vdbx} \ \frac{Q \vdash \dot{\mathbf{e}} = G\mathbf{e}}{\mathbf{e} = 0 \vdash [x' = f(x) \,\&\, Q]\mathbf{e} = 0}$$

PROOF. Rule vdbx derives from derived axiom VDBX using $(\ )'$, DE, $[:=]$ to provably transform between $(\mathbf{e})'$ and $\dot{\mathbf{e}}$, just like rule dbx derives from derived axiom DBX in Corollary 3.2. □

The use of axiom $\text{DBX}_{\succcurlyeq}$ in the derivation of axiom VDBX corresponds to Grönwall's lemma [18, 44, §29.VI], as illustrated in Fig. 2a. In case $e$ starts with value 0 initially and satisfies the Darboux inequality $\dot{e} \geq ge$, the constant zero solution of the differential equation $e' = g(t)e$ bounds it from below. In Fig. 2a, this corresponds to the case where both blue lines lie exactly on the horizontal axis. The proof uses the (squared) Euclidean and Frobenius norms to reduce a vectorial equality ($\mathbf{e} = 0$) to a scalar inequality ($-\|\mathbf{e}\|_2^2 \geq 0$), which enables further analysis using *scalar* differential ghosts. The convenient choice of compatible norms ensures that all syntactic proof steps are done within the extended term language. Since all norms are equivalent on finite-dimensional vector spaces [44, §10.III], this reduction can also be done using other norms with suitable syntactic representations. Convenient choices of norms are a common technique in the study of differential equations [44].

An alternative derivation of rule vdbx is given in the authors' earlier conference version [33] based on Liouville's formula [44, §15.III]. That alternative derivation has an alternative geometric interpretation as a continuous change of basis that is expressed purely syntactically [33] but requires the use of *vectorial* differential ghosts and a number of ghost variables that is quadratic in the dimension. The new derivation in Lemma 4.1 uses exactly 2 scalar differential ghosts in the $\text{DBX}_{\succcurlyeq}$ step independent of dimension and relies only on basic properties of real arithmetic. In fact, just like the scalar Darboux axioms, axiom VDBX for $m$-dimensional extended terms **e** derives once-and-for-all so no differential ghosts are needed for its subsequent use.

## 4.2 Completeness for Analytic Invariants

Returning to extended terms $e$ satisfying the differential radical identity (3), a proof rule for invariance of $e = 0$ based on *higher* Lie derivatives derives as a direct instance of derived rule vdbx:

THEOREM 4.3 (DIFFERENTIAL RADICAL INVARIANTS ARE VECTORIAL DARBOUX). *The differential radical invariant proof rule* dRI *derives from* vdbx *(which in turn derives from* DG*).*

$$\text{dRI} \ \frac{\Gamma, Q \vdash \bigwedge_{i=0}^{N-1} \dot{e}^{(i)} = 0 \quad Q \vdash \dot{e}^{(N)} = \sum_{i=0}^{N-1} g_i \dot{e}^{(i)}}{\Gamma \vdash [x' = f(x) \,\&\, Q]e = 0}$$

PROOF SUMMARY (APPENDIX B.3). Rule dRI derives from rule vdbx by transforming identity (3) involving higher Lie derivatives of $e$ into a vectorial Darboux equality involving only first Lie derivatives of the extended term vector. The proof uses the following choice of cofactor matrix $G$:

$$G = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \dots & 0 & 1 \\ g_0 & g_1 & \dots & g_{N-2} & g_{N-1} \end{pmatrix}, \quad \mathbf{e} = \begin{pmatrix} e \\ \dot{e}^{(1)} \\ \vdots \\ \dot{e}^{(N-2)} \\ \dot{e}^{(N-1)} \end{pmatrix}$$

The matrix $G$ has 1 on its superdiagonal and the $g_i$ cofactors in the last row. The left premise of dRI is used to show $\mathbf{e} = 0$ initially, while its right premise is used to show the premise of vdbx. □

For any extended term $e$ in the LHS of normalized equation $e = 0$, the computable differential radicals condition (R) requires that the differential radical identity (3) (computably) exists and proves with associated rank $N$ and cofactors $g_i$ for $e$. The resulting (provable) identity (3) proves the right premise of dRI.[5] The succedent in the remaining left premise of dRI thus gives a finitary characterization for when *all* Lie derivatives of $e$ evaluate to zero in the initial state. This motivates the following definition of a *finite* formula summarizing that *all* higher Lie derivatives of $e$ are zero:

*Definition 4.4 (Differential radical formula).* The *differential radical formula* $\dot{e}^{(*)} = 0$ for extended term $e$ of rank $N \geq 1$ from identity (3) with Lie derivatives along $x' = f(x)$ is defined to be:

$$\dot{e}^{(*)} = 0 \overset{\text{def}}{\equiv} \bigwedge_{i=0}^{N-1} \dot{e}^{(i)} = 0$$

The finiteness of $\dot{e}^{(*)} = 0$ depends on Lie derivatives along the particular differential equation $x' = f(x)$ of interest, because, without considering the ODE, *no* corresponding chain of higher-order differentials would stabilize. The rest of this article focuses on Lie derivatives to utilize this finiteness property, but relies under the hood on dL's axiomatic proof transformation from differentials.

The completeness of derived rule dRI can be proved semantically by extending earlier arguments [15] to extended term languages. Even better: the following equivalent characterization in arithmetic of the future truth of analytic formulas along differential equations (including analytic invariants) derives axiomatically using the extensions developed in Section 5.[6] In contrast to the semantic completeness argument, this syntactic characterization enables complete proofs and *complete disproofs* of analytic invariance within the dL calculus. In other words, *disproving* the RHS of the characterization under assumptions $\Gamma$, yields a dL proof of $\Gamma \vdash \neg[x' = f(x) \,\&\, Q]e = 0$.

THEOREM 4.5 (ANALYTIC COMPLETENESS). *The differential radical invariant axiom* DRI *derives in* dL *when $Q$ is a semianalytic formula formed from conjunctions and disjunctions of strict inequalities:*

$$\text{DRI} \quad [x' = f(x) \,\&\, Q]e = 0 \leftrightarrow \big(Q \to \dot{e}^{(*)} = 0\big)$$

PROOF SUMMARY (APPENDIX B.3). The "←" direction derives (for any $Q$) by an application of derived rule dRI, whose right premise closes by (3). The "→" direction relies on existence and uniqueness of solutions to differential equations, which are internalized as axioms in Section 5. □

For the proof of Theorem 4.5, the additional axioms are *only required* for syntactically deriving the "→" direction (completeness) of DRI. The "←" direction (soundness) derives using dRI, which, by Theorem 4.3, can be derived using only DI, DC, DG. Thus, the base dL axiomatization with differential ghosts is *complete* for proving properties of the form $[x' = f(x) \,\&\, Q]e = 0$ because dRI provably reduces all such questions to $Q \to \dot{e}^{(*)} = 0$. The validity of this resulting semianalytic formula is a purely arithmetical question. In fact, the base dL axiomatization *decides* $[x' = f(x) \,\&\, Q]p = 0$ in the case where $x' = f(x)$ is polynomial and $Q$ is semialgebraic, because the resulting RHS of DRI is semialgebraic, and hence, a formula of decidable real arithmetic [4]. The same applies for the next result, which is a corollary of Theorem 4.5 but applies beyond the continuous fragment of dL.

COROLLARY 4.6 (ANALYTIC HYBRID PROGRAM COMPLETENESS). *For analytic formulas $P$ and analytic hybrid programs $\alpha$, i.e., whose tests and domain constraints are negations of analytic formulas, it is possible to compute an extended term $e$ such that the equivalence $[\alpha]P \leftrightarrow e = 0$ is derivable in* dL, *provided that the term language is Noetherian (defined in Appendix C).*

---

[5]Theorem 4.3 shows $Q$ can be assumed when proving the right premise. A finite rank must exist either way, but assuming $Q$ may reduce the number of higher Lie derivatives of $e$ that need to be considered for the proof (as in Example 7.10).
[6]With these axiomatic extensions, the requirement in Theorem 4.5 that $Q$ is formed from strict inequalities is not necessary. A derived equivalence axiom for analytic invariance with arbitrary semianalytic domain constraint $Q$ is given in Theorem 6.10.

PROOF SUMMARY (APPENDIX C). By structural induction on $\alpha$ analogous to [29, Thm. 1], using Theorem 4.5 for the differential equations case and the Noetherian term language for loops. □

The Noetherian condition of Corollary 4.6 implies the computable differential radicals condition (R). Polynomial term languages are Noetherian so Corollary 4.6 shows that dL decides $[\alpha]P$ where $P$ and $\alpha$ are both algebraic. However, the Noetherian condition fails even for simple extended term languages such as (1). The stronger Noetherian condition is only required when the analytic hybrid program $\alpha$ contains loops. Otherwise, the weaker condition (R) suffices for Corollary 4.6.

## 5 EXTENDED AXIOMATIZATION

This section presents the axiomatic extension that is used for the rest of this article. The purpose of this axiomatic extension is to internalize standard properties of differential equations, such as existence and uniqueness [44, §10.VI] as *syntactic* reasoning principles. The extension requires that the system $x' = f(x)$ *locally evolves* $x$, i.e., it has no fixpoint at which $f(x)$ is the 0 vector. This can be ensured syntactically, e.g., by requiring that the system contains a clock variable $x_1' = 1$ that tracks the passage of time. Such a clock can always first be added using axiom DG if necessary.

### 5.1 Existence, Uniqueness, and Continuity

The differential equations of dL are smooth. Hence, the Picard-Lindelöf theorem [44, §10.VI] guarantees that for any initial state $\omega$, a *unique* solution of the system $x' = f(x)$, i.e., $\varphi : [0, T] \to \mathbb{S}$ with $\varphi(0) = \omega$, *exists* for some duration $T > 0$. The solution $\varphi$ can be extended (uniquely) to its maximal open interval of existence [44, §10.IX] and $\varphi(\zeta)$ is smooth with respect to $\zeta$.

LEMMA 5.1 (CONTINUOUS EXISTENCE, UNIQUENESS, AND DIFFERENTIAL ADJOINTS). *The following axioms are sound. In Cont and Dadj, $y$ are fresh variables (so not in $x' = f(x) \& Q(x)$ or $e$).*

Uniq $\langle x' = f(x) \& Q_1 \wedge Q_2 \rangle P \leftrightarrow \left( \langle x' = f(x) \& Q_1 \rangle P \right) \wedge \left( \langle x' = f(x) \& Q_2 \rangle P \right)$

Cont $x = y \to \left( \langle x' = f(x) \& e > 0 \rangle x \neq y \leftrightarrow e > 0 \right)$

Dadj $\langle x' = f(x) \& Q(x) \rangle x = y \leftrightarrow \langle y' = -f(y) \& Q(y) \rangle y = x$

PROOF SUMMARY (APPENDIX A.1). Uniq internalizes uniqueness, Cont internalizes continuity of the values of $e$ and existence of solutions, and Dadj internalizes differential adjoints by the group action of time on ODE solutions, which is another consequence of existence and uniqueness. □

The *uniqueness axiom* Uniq says that if a state has two solutions $\varphi_1, \varphi_2$ respectively staying in evolution domains $Q_1, Q_2$ and whose endpoints satisfy $P$, then, by uniqueness, one of $\varphi_1$ or $\varphi_2$ is a prefix of the other, and therefore, that prefix stays in both evolution domains $Q_1 \wedge Q_2$ and satisfies $P$ at its endpoint. The *continuous existence axiom* Cont expresses a notion of *local progress* for differential equations. It says that from an initial state satisfying $x = y$, the system can locally evolve to another state satisfying $x \neq y$ while still staying in the *open set* of states characterized by $e > 0$ iff the initial state is already in that open set. This uses the assumption that the system locally evolves $x$ at all. The *differential adjoints* axiom Dadj expresses that $x$ can flow forward to $y$ iff $y$ can flow backward to $x$ along the negated ODE. It is at the heart of the "there and back again" axiom that equivalently expresses properties of differential equations with evolution domains in terms of properties of forwards and backwards differential equations without evolution domains [29].

Although all three axioms are stated as (conditional[7]) equivalences to support intuition, the main properties of interest are their "←" directions. For example, the "→" direction of Uniq derives from domain constraint monotonicity for the diamond modality (derived rule dRW⟨·⟩ below). These diamond monotonicity principles are given below as they are useful for working with the newly introduced axioms. They derive by duality from the usual dL box modality principles:

Corollary 5.2 (Derived diamond modality domain rules and axioms). *The following axiom and its corollary proof rule derive in* dL:

DR⟨·⟩ $[x' = f(x) \& R]Q \rightarrow (\langle x' = f(x) \& R\rangle P \rightarrow \langle x' = f(x) \& Q\rangle P)$

dRW⟨·⟩ $\dfrac{R \vdash Q \quad \Gamma \vdash \langle x' = f(x) \& R\rangle P}{\Gamma \vdash \langle x' = f(x) \& Q\rangle P}$

Proof Summary (Appendix A.2). Axiom DR⟨·⟩ is the diamond version of dL's domain refinement axiom that underlies axiom DC; if solutions never leave $Q$ when staying in $R$ (first assumption), then any solution staying in $R$ (second assumption) must also stay in $Q$ (conclusion). The rule dRW⟨·⟩ derives from DR⟨·⟩ using rule dW on its first assumption. □

## 5.2 Real Induction

The final axiomatic extension is based on the real induction principle [7], which is briefly recalled:

*Definition 5.3 (Inductive subset [7]).* The subset $S \subseteq [a, b]$ is called an *inductive* subset of the compact interval $[a, b]$ iff for all $a \le \zeta \le b$ and $[a, \zeta) \subseteq S$,

① $\zeta \in S$.
② If $\zeta < b$ then $(\zeta, \zeta + \epsilon] \subseteq S$ for some $\epsilon > 0$.

Here, $[a, a)$ is the empty interval, hence ① requires $a \in S$.

Proposition 5.4 (Real induction [7]). *The subset $S \subseteq [a, b]$ is inductive iff $S = [a, b]$.*

Proof. In the "⟸" direction, $S = [a, b]$ is inductive by definition. For the "⟹" direction, let $S \subseteq [a, b]$ be inductive. Suppose $S \ne [a, b]$, so that the complement set $S^\complement = [a, b] \setminus S$ is nonempty. Let $\zeta$ be the infimum of $S^\complement$, then $\zeta \in [a, b]$ since $[a, b]$ is left-closed. First, note that $[a, \zeta) \subseteq S$. Otherwise, $\zeta$ is not an infimum of $S^\complement$, because there would exist $a \le \tau < \zeta$, such that $\tau \in S^\complement$. By ①, $\zeta \in S$. Next, if $\zeta = b$, then $S = [a, b]$, contradiction. Thus, $\zeta < b$, and by ②, $(\zeta, \zeta + \epsilon] \subseteq S$ for some $\epsilon > 0$. Since $\zeta \in S$, this implies that $\zeta + \epsilon$ is a greater lower bound of $S^\complement$ than $\zeta$, contradiction. □

Proposition 5.4 is based on the completeness of the reals [7] for compact intervals $[a, b]$ of $\mathbb{R}$. Applying it to the time axis of ODE solutions yields real induction *along* solutions of differential equations. For brevity, only the real induction axiom for systems without evolution domain constraints is presented here, leaving the general version to Appendix A.1, since evolution domains are definable in dL [29].

Lemma 5.5 (Real induction). *The real induction axiom RI is sound, where $y$ is fresh in $[x' = f(x)]P$.*

RI $[x' = f(x)]P \leftrightarrow \forall y\, [x' = f(x) \& P \lor x = y](x = y \rightarrow P \land \langle x' = f(x) \& P \lor x = y\rangle x \ne y)$

Proof Summary (Appendix A.1). The RI axiom follows from the real induction principle [7] and the Picard-Lindelöf theorem [44, §10.VI]. □

---

[7]Axiom Cont is sound even without the condition from assumption $x = y$. It is stated conditionally to align with the intuition of local evolution from an initial state satisfying $x = y$.

Real induction axiom RI can be understood in relation to Def. 5.3: its RHS is true in a state iff the subset of times at which the solution satisfies $P$ is inductive. First, $\forall y \, [\ldots](x = y \to \ldots)$ can be understood as quantifying over all final states ($x = y$) reached by trajectories staying within $P$ except possibly at the endpoint $x = y$. This corresponds to $[a, \zeta] \subseteq S$ in Def. 5.3. The left conjunct ($P$) under the box modality expresses that $P$ is still true at such an endpoint, corresponding to ① in Def. 5.3. The right conjunct ($\langle x' = f(x) \,\&\, P \vee x = y \rangle x \neq y$) expresses that $P$ continues to remain true locally when following the ODE for a short time, corresponding to ② in Def. 5.3.

To see the topological significance of RI, recall the ODE $\alpha_e$ from (2) and consider a set of points that is *not invariant*. Figure 3 illustrates two trajectories that leave the half-open candidate invariant disk characterized by the disjunctive formula: $u^2 + v^2 < \frac{1}{4} \vee u^2 + v^2 = \frac{1}{4} \wedge u \geq 0$.



Fig. 3. The half-open green disk is not invariant for the ODE $\alpha_e$ from (2) because the red and blue trajectories spiral out of it towards the unit circle at a closed (solid green) or open (dashed green) boundary, respectively.

Trajectories starting in the disk leave it through its boundary but only in one of two ways: either at a point which is also in the disk (red trajectory exiting right) or which is not in the disk (blue trajectory exiting left). The left conjunct of RI rules out trajectories like the blue one exiting left in Fig. 3, while the right conjunct rules out trajectories like the red trajectory exiting right.
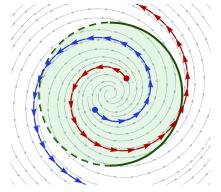
The right conjunct of axiom RI also suggests a way to use it: axiom RI reduces proofs of invariance to local progress properties under the box modality. This motivates the following syntactic modality abbreviation for *local progress* into an evolution domain $Q$:

$$\langle x' = f(x) \,\&\, Q \rangle \bigcirc \stackrel{\text{def}}{\equiv} \langle x' = f(x) \,\&\, Q \vee x = y \rangle \, x \neq y$$

All proofs in this article use the modality with an initial assumption $x = y$, where $y$ is fresh. In this case, where $\omega[\![x]\!] = \omega[\![y]\!]$, since the ODE locally evolves $x$, the $\bigcirc$ modality has this semantics:

$\omega \in [\![\langle x' = f(x) \,\&\, Q \rangle \bigcirc]\!]$ iff there is a function $\varphi : [0, T] \to \mathbb{S}$ with $T > 0$, $\varphi(0) = \omega$,

$\varphi$ solves the ODE $x' = f(x)$ and $\varphi(\zeta) \in [\![Q]\!]$ for all $\zeta$ in the half-open interval $(0, T]$

Thus, the abbreviation $\bigcirc$ is a continuous-time version of the *next* modality of temporal logic [8] for differential equations. Conventionally, such a next state operator is excluded from continuous-time generalizations of temporal logic [8] because there is no unique "next" state in the continuous setting. The local progress modality $\bigcirc$ overcomes this by instead quantifying over *some* time interval $(0, T]$, with $T > 0$, of states along the solution. Intuitively, the exclusion of time 0 is because the $\bigcirc$ modality describes what solutions will do *next* (or *locally*) rather than what it is doing *now*. A precise (topological) explanation is provided in Appendix B.2. A complete characterization of local progress for all semianalytic formulas is derived in Section 6. As a corollary this shows that, like its discrete counterpart, the $\bigcirc$ modality is self-dual for semianalytic $Q$.

The final derived rule rI shows what the added axioms and local progress provide: axiom RI reduces global invariance properties of ODEs to local progress properties. These local progress properties are provable using Cont, Uniq and the existing dL axioms, as shown in the next section.

COROLLARY 5.6 (REAL INDUCTION RULE). *The real induction proof rule* rI *derives from* RI, Dadj. *Variables $y$ are fresh in the ODE $x' = f(x)$ and formula $P$.*

$$\text{rI} \quad \frac{x{=}y, P \vdash \langle x' = f(x) \,\&\, P \rangle \bigcirc \qquad x{=}y, \neg P \vdash \langle x' = -f(x) \,\&\, \neg P \rangle \bigcirc}{P \vdash [x' = f(x)]P}$$

PROOF SUMMARY (APPENDIX A.2). Rule rI derives from axiom RI, where the left/right premises of the rule correspond respectively to the right/left conjunct of the RHS of RI. Axiom Dadj is used to syntactically flip signs in the right premise.                                                                                    □

## 6  SEMIANALYTIC INVARIANTS

From now on, assume domain constraint $Q \equiv true$ since it is definable [29] and not central to the core idea of this section. Using the generalizations of RI, rI from Appendix A, the case of semianalytic invariants for ODEs with arbitrary semianalytic evolution domain $Q$ is given in Appendix B.

The first step in invariance proofs for semianalytic $P$ is to use derived rule rI, which yields premises of the form $x{=}y, P \vdash \langle x' = f(x) \,\&\, P \rangle \bigcirc$ (modulo sign changes and negation). These premises express local progress properties of the ODE $x' = f(x)$. Analogously to the equivalent arithmetic reduction of equational properties of differential equations in Theorem 4.5 using the *finite* differential radical formula (Def. 4.4), the key insight is that local progress for any semianalytic formula is also (provably) completely characterized by a *finite* semianalytic progress formula.

### 6.1  Local Progress

The characterization of local progress was previously used implicitly for semialgebraic invariants [16, 22]. This section shows how it can be derived syntactically in dL for extended term languages and proves the completeness of this characterization. The derivation is built up systematically, starting from the base case of atomic inequalities before moving on to the full semianalytic case. Interesting properties of this characterization, e.g., self-duality, are observed along the way.

*6.1.1  Atomic Inequalities.* Consider the atomic inequality $e \succcurlyeq 0$. Intuitively, to show *local progress* into such an inequality, it is sufficient to locally consider the *first* (significant) Lie derivative of $e$ because the sign of a smooth function is locally dominated by the sign of its first non-zero derivative (if one exists). The key to its syntactic rendition is the following lemma for non-strict inequalities:

LEMMA 6.1 (LOCAL PROGRESS STEP). *The local progress step axiom* $\text{LPi}_\geq$ *derives from* Cont. *Variables $y$ are fresh in the ODE $x' = f(x)$ and extended term $e$.*

$$\text{LPi}_\geq \quad x{=}y \rightarrow \Big( e \geq 0 \wedge \big( e = 0 \rightarrow \langle x' = f(x) \,\&\, \dot e \geq 0 \rangle x{\neq}y \big) \rightarrow \langle x' = f(x) \,\&\, e \geq 0 \rangle x{\neq}y \Big)$$

PROOF. The proof starts with a ∨L case split since $e \geq 0$ is equivalent to $e > 0 \vee e = 0$ by ℝ. The resulting premises are respectively abbreviated ① for $e > 0$ and ② for $e = 0$, and continued below.

$$\text{ℝ, ∨L} \frac{\qquad\qquad\qquad\qquad\qquad\qquad ① \qquad\qquad ②\qquad\qquad\qquad\qquad}{x{=}y, e \geq 0, e = 0 \rightarrow \langle x' = f(x) \,\&\, \dot e \geq 0 \rangle x{\neq}y \vdash \langle x' = f(x) \,\&\, e \geq 0 \rangle x{\neq}y}$$

From premise ①, since the value of $e$ is already positive initially, it must *locally* stay positive. Using dRW⟨·⟩, the non-strict inequality in the domain constraint of the succedent is strengthened to a strict one, after which Cont closes the derivation.

$$\text{Cont} \frac{*}{x{=}y, e > 0 \vdash \langle x' = f(x) \,\&\, e > 0 \rangle x{\neq}y}$$
$$\text{dRW⟨·⟩} \frac{}{x{=}y, e > 0 \vdash \langle x' = f(x) \,\&\, e \geq 0 \rangle x{\neq}y}$$

From premise ②, the local sign of $e$ cannot be determined from its initial value alone. The proof looks to the Lie derivative of $e$, which is assumed to be locally non-negative (in the implication $e = 0 \rightarrow \dots$). Axiom $\text{DR}\langle \cdot \rangle$ reduces this to a box modality, after which DI finishes the proof.

$$
\dfrac{\dfrac{\dfrac{*}{e = 0 \vdash [x' = f(x) \,\&\, \dot{e} \geq 0]e \geq 0} \text{DI, ( )', DE, [:=]}}{e = 0, \langle x' = f(x) \,\&\, \dot{e} \geq 0 \rangle x{\neq}y \vdash \langle x' = f(x) \,\&\, e \geq 0 \rangle x{\neq}y} \text{DR}\langle \cdot \rangle}{e = 0, e = 0 \rightarrow \langle x' = f(x) \,\&\, \dot{e} \geq 0 \rangle x{\neq}y \vdash \langle x' = f(x) \,\&\, e \geq 0 \rangle x{\neq}y} \rightarrow\text{L}
$$

$\square$

Similar to DBX, $\text{DBX}_{\succcurlyeq}$, and VDBX, a version of $\text{LPi}_{\geq}$ derives once-and-for-all using differentials $((e)' \geq 0)$ in domain constraints. This presentation is omitted to keep with this article's syntactic convention that domain constraints are always (differential-free) semianalytic formulas (Section 2.1). Mathematically, to conclude that $e$ is locally non-negative, it is important that the Lie derivative $\dot{e}$ is assumed to be *locally* non-negative rather than just *initially* non-negative. Just as the local sign of $e$ cannot be determined (directly) when its initial value is zero, the same is true for $\dot{e}$. This difference drives the use of *higher* Lie derivatives when $\text{LPi}_{\geq}$ is generalized below. Syntactically, this difference manifests in both $\text{DR}\langle \cdot \rangle$, DI proof steps which crucially rely on the formula $\dot{e} \geq 0$ appearing in their respective domain constraints rather than simply as an initial assumption.

Observe that $\text{LPi}_{\geq}$ allows derivations to pass from reasoning about local progress[8] for $e \geq 0$ to local progress for its (first) Lie derivative $\dot{e} \geq 0$ whilst accumulating $e = 0$ in the antecedent. This is reminiscent of derivative tests from elementary calculus used for testing the local behavior around a given stationary point of a (sufficiently) smooth function. The difference is that (syntactic) Lie derivatives have to be used for soundness instead of analytic time derivatives, but these notions are provably equatable along ODEs using differentials [32, Lem. 35]. Similar to these derivative tests, if the first Lie derivative is indeterminate as well, then the derivation can look to the second higher Lie derivative, and so on. Deductively, this is done by repeated use of derived axiom $\text{LPi}_{\geq}$:

$$
\dfrac{\dfrac{\Gamma \vdash e \geq 0}{}\ \dfrac{\dfrac{\Gamma, e = 0 \vdash \dot{e} \geq 0}{}\ \dfrac{\dfrac{\Gamma, x{=}y, e = 0, \dots, \dot{e}^{(k-1)} = 0 \vdash \langle x' = f(x) \,\&\, \dot{e}^{(k)} \geq 0 \rangle x{\neq}y}{\dots} \text{LPi}_{\geq}}{\Gamma, x{=}y, e = 0 \vdash \langle x' = f(x) \,\&\, \dot{e} \geq 0 \rangle x{\neq}y}}{} \text{LPi}_{\geq}}{\Gamma, x{=}y \vdash \langle x' = f(x) \,\&\, e \geq 0 \rangle x{\neq}y} \text{LPi}_{\geq}
$$

The rightmost premise closes whenever the (strict) inequality $\dot{e}^{(k)} > 0$ can be proved from the accumulated antecedents. The local sign of $e$ (and of all its Lie derivatives below the $k$-th one) is dominated by that of $\dot{e}^{(k)}$ because all of the lower (Lie) derivatives have indeterminate sign. The use of Cont, $\text{dRW}\langle \cdot \rangle$ finishes that proof because the solution must then locally enter $\dot{e}^{(k)} > 0$:

$$
\dfrac{\Gamma, x{=}y, e = 0, \dots, \dot{e}^{(k-1)} = 0 \vdash \dot{e}^{(k)} > 0 \quad \dfrac{\dfrac{\dfrac{*}{x{=}y, \dot{e}^{(k)} > 0 \vdash \langle x' = f(x) \,\&\, \dot{e}^{(k)} > 0 \rangle x{\neq}y} \text{Cont}}{x{=}y, \dot{e}^{(k)} > 0 \vdash \langle x' = f(x) \,\&\, \dot{e}^{(k)} \geq 0 \rangle x{\neq}y} \text{dRW}\langle \cdot \rangle}{}}{\Gamma, x{=}y, e = 0, \dots, \dot{e}^{(k-1)} = 0 \vdash \langle x' = f(x) \,\&\, \dot{e}^{(k)} \geq 0 \rangle x{\neq}y} \text{cut}
$$

The extended term conditions of smoothness (S) and syntactic partial derivatives (P) guarantee that all of the (infinitely many) higher Lie derivatives of $e$ are well-defined semantically and syntactically. Derivations, on the other hand, are finite syntactic objects and can only mention *finitely many* Lie derivatives. Thus, one might suspect they are insufficient (hence incomplete)

---

[8]The local progress property used in $\text{LPi}_{\geq}$ is syntactically simpler than for the $\bigcirc$ modality (no $x = y$ in the domain constraints). For non-strict inequalities, the two are equivalent but the syntactic simplification in $\text{LPi}_{\geq}$ allows its re-use as a lemma in proving $\bigcirc$ local progress for both non-strict and strict inequalities.

when, e.g., none of the higher Lie derivatives has a definite sign or if (infinitely many) different choices of $k$ are needed in the proof depending on the initial state that satisfies assumptions $\Gamma$.

This is where the third, computable differential radicals condition (R) is crucially used. When $N$ is the rank of $e$ according to identity (3), then once the derivation has gathered $e = 0, \ldots, \dot{e}^{(N-1)} = 0$, i.e., $\dot{e}^{(*)} = 0$ in the antecedents, derived rule dRI proves the invariant $e = 0$ and ODEs always locally progress in invariants. Furthermore, this shows (mathematically) that it is unnecessary to go to higher Lie derivatives when proving local progress for $e > 0$ because none of the signs of the higher Lie derivatives of $e$ beyond $N$ will be sign-definite. Thus, the rank provides a uniform and finite bound for the number of Lie derivatives of $e$ that need to be analyzed in any state, regardless of assumptions $\Gamma$. This finiteness property motivates the following definition, which gathers the above open premises to obtain a finite formula characterizing the *first significant Lie derivative* of $e$:

*Definition 6.2 (First significant Lie derivative).* The *progress formula* $\dot{e}^{(*)} > 0$ for extended term $e$ of rank $N \geq 1$ from identity (3) with Lie derivatives along $x' = f(x)$ is defined to be:

$$\dot{e}^{(*)} > 0 \stackrel{\text{def}}{\equiv} e \geq 0 \wedge \left(e = 0 \to \dot{e} \geq 0\right) \wedge \left(e = 0 \wedge \dot{e} = 0 \to \dot{e}^{(2)} \geq 0\right)$$

$$\wedge \cdots \wedge \left(e = 0 \wedge \dot{e} = 0 \wedge \cdots \wedge \dot{e}^{(N-3)} = 0 \to \dot{e}^{(N-2)} \geq 0\right)$$

$$\wedge \left(e = 0 \wedge \dot{e} = 0 \wedge \cdots \wedge \dot{e}^{(N-2)} = 0 \to \dot{e}^{(N-1)} > 0\right)$$

The *progress formula* $\dot{e}^{(*)} \geq 0$ is defined to be $\dot{e}^{(*)} > 0 \vee \dot{e}^{(*)} = 0$. The formulas $\dot{e}^{-(*)} > 0$ (or $\dot{e}^{-(*)} \geq 0$) are identical except their Lie derivatives are along ODE $x' = -f(x)$ instead.

LEMMA 6.3 (LOCAL PROGRESS $\succcurlyeq$). *The local progress inequality axioms* $LP_{\geq *}$, $LP_{>*}$ *derive from* $LPi_{\geq}$ *and thus from* Cont. *Variables $y$ are fresh in the ODE $x' = f(x)$ and extended term $e$.*

$LP_{\geq *}$　$x{=}y \to \left(\dot{e}^{(*)} \geq 0 \to \langle x' = f(x) \,\&\, e \geq 0\rangle \bigcirc\right)$

$LP_{>*}$　$x{=}y \to \left(\dot{e}^{(*)} > 0 \to \langle x' = f(x) \,\&\, e > 0\rangle \bigcirc\right)$

PROOF SUMMARY (APPENDIX B.2). Both axioms derive after unfolding the syntactic abbreviation of the $\bigcirc$ modality. Axiom $LP_{\geq *}$ derives by the preceding discussion with iterated use of derived axioms $LPi_{\geq}$ and dRI. Axiom $LP_{>*}$ derives similarly, but with an additional tweak to weaken the strict inequality $e > 0$ so that axiom $LPi_{\geq}$ can be used. □

The difference between the derivations of $LP_{\geq *}$ and $LP_{>*}$ is mainly technical and boils down to the handling of the assumptions about the initial state, and in particular, $x{=}y$ (see Appendix A.2 and B.2). Intuitively, the difference arises from the fact that the formula $e \geq 0$ characterizes a topologically closed set while $e > 0$ characterizes an open set. To locally progress into a set from initial state $\omega$, the state $\omega$ must already be in the topological closure of that set. Closed sets are equal to their closure so, e.g., $\omega$ must already satisfy $e \geq 0$ in order to locally progress into it. Sets that are not closed (e.g., open sets) are not equal to their closure as they lack points on their topological boundary. An example of this is the half-open disk illustrated in Fig. 3. Thus, it is possible to locally progress into such sets from their topological boundary without $\omega$ already starting in the set.

*6.1.2 Semianalytic Formulas.* Semianalytic formulas $P$ normalize propositionally to the following disjunctive normal form with extended terms $e_{ij}, \tilde{e}_{ij}$:

$$P \equiv \bigvee_{i=0}^{M} \left(\bigwedge_{j=0}^{m(i)} e_{ij} \geq 0 \wedge \bigwedge_{j=0}^{n(i)} \tilde{e}_{ij} > 0\right) \tag{5}$$

Progress formulas lift homomorphically to semianalytic formulas in normal form:

*Definition 6.4 (Semianalytic progress formula).* The *semianalytic progress formula* $\dot{P}^{(*)}$ for a semi-analytic formula $P$ in normal form (5) and Lie derivatives along $x' = f(x)$ is defined to be:

$$\dot{P}^{(*)} \overset{\text{def}}{\equiv} \bigvee_{i=0}^{M} \Big( \bigwedge_{j=0}^{m(i)} \dot{e_{ij}}^{(*)} \geq 0 \wedge \bigwedge_{j=0}^{n(i)} \dot{\tilde{e}_{ij}}^{(*)} > 0 \Big)$$

The formula $\dot{P}^{-(*)}$ takes Lie derivatives along ODE $x' = -f(x)$ instead.

A mention of the notation $\dot{P}^{(*)}$ is understood as the progress formula for semianalytic formula $P$ after it is rewritten propositionally to any equivalent normal form (5).

LEMMA 6.5 (SEMIANALYTIC LOCAL PROGRESS). *The local progress formula axiom* LP$_\mathbb{R}$ *derives from* Cont, Uniq. *Variables $y$ are fresh in the ODE $x' = f(x)$ and semianalytic formula $P$.*

$$\text{LP}_\mathbb{R} \quad x=y \rightarrow \big( \dot{P}^{(*)} \rightarrow \langle x' = f(x) \,\&\, P \rangle \bigcirc \big)$$

PROOF SUMMARY (APPENDIX B.2). The shape of the semianalytic progress formula $\dot{P}^{(*)}$ guides the proof. The derivation is sketched at a high level here for the representative example formula:

$$P \equiv (e_1 \geq 0 \wedge \tilde{e}_1 > 0) \vee (e_2 \geq 0 \wedge \tilde{e}_2 > 0)$$

$$\dot{P}^{(*)} \equiv (\dot{e_1}^{(*)} \geq 0 \wedge \dot{\tilde{e}_1}^{(*)} > 0) \vee (\dot{e_2}^{(*)} \geq 0 \wedge \dot{\tilde{e}_2}^{(*)} > 0)$$

To show local progress into a *disjunction*, it suffices to show local progress into either disjunct. The derivation starts by decomposing $\dot{P}^{(*)}$ according to its (outermost) disjunction and accordingly decomposing $P$ in the local progress succedent with dRW$\langle \cdot \rangle$. The premise for the second disjunct resulting from the $\vee$L step is symmetric and omitted here.

$$\frac{\dfrac{x=y, \dot{e_1}^{(*)} \geq 0 \wedge \dot{\tilde{e}_1}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, e_1 \geq 0 \wedge \tilde{e}_1 > 0 \rangle \bigcirc}{x=y, \dot{e_1}^{(*)} \geq 0 \wedge \dot{\tilde{e}_1}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, P \rangle \bigcirc} \text{dRW}\langle \cdot \rangle}{x=y, \dot{P}^{(*)} \vdash \langle x' = f(x) \,\&\, P \rangle \bigcirc} \;\vee\text{L}$$

To show local progress into a *conjunction*, by Uniq, it suffices to show local progress into both conjuncts separately. The derivation continues using Uniq, $\wedge$R to split the conjunctive local progress succedent before the derived axioms LP$_{\geq*}$, LP$_{>*}$ are used to finish the proofs of the atomic cases:

$$\frac{\dfrac{*}{x=y, \dot{e_1}^{(*)} \geq 0 \vdash \langle x' = f(x) \,\&\, e_1 \geq 0 \rangle \bigcirc} \text{LP}_{\geq*} \qquad \dfrac{*}{x=y, \dot{\tilde{e}_1}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, \tilde{e}_1 > 0 \rangle \bigcirc} \text{LP}_{>*}}{x=y, \dot{e_1}^{(*)} \geq 0, \dot{\tilde{e}_1}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, e_1 \geq 0 \wedge \tilde{e}_1 > 0 \rangle \bigcirc} \;\text{Uniq}, \wedge\text{R} \qquad \square$$

Completeness could potentially be lost in several steps of the proof of Lemma 6.5, e.g., the use of $\vee$L at the start of the derivation, or the implicational axioms LP$_{\geq*}$, LP$_{>*}$. The converse (completeness) direction of axiom LP$_\mathbb{R}$ therefore does not follow immediately from Lemma 6.5. Instead, the axiom LP$_\mathbb{R}$ can be re-used to derive its own strengthening to an equivalence. This equivalence justifies the syntactic abbreviation $\bigcirc$, recalling that the $\bigcirc$ modality of temporal logic is self-dual. It also shows that the progress formulas are congruent over equivalences.

THEOREM 6.6 (LOCAL PROGRESS COMPLETENESS). *The local progress axiom* LP *derives from* Cont, Uniq. *Variables $y$ are fresh in the ODE $x' = f(x)$ and semianalytic formula $P$.*

$$\text{LP} \quad x=y \rightarrow \big( \langle x' = f(x) \,\&\, P \rangle \bigcirc \leftrightarrow \dot{P}^{(*)} \big)$$

COROLLARY 6.7 (DUALITY AND CONGRUENCE). *The duality axiom $\neg\bigcirc$ and congruence proof rule for progress formulas CLP derive from LP and thus from Cont, Uniq. Variables y are fresh in the ODE $x' = f(x)$ and semianalytic formulas $P, R$.*

$$\neg\bigcirc \quad x=y \rightarrow \left(\langle x' = f(x) \,\&\, P\rangle\bigcirc \leftrightarrow \neg\langle x' = f(x) \,\&\, \neg P\rangle\bigcirc\right)$$

$$\text{CLP} \quad \frac{P \leftrightarrow R}{\dot{P}^{(*)} \leftrightarrow \dot{R}^{(*)}}$$

PROOF SUMMARY FOR THEOREM 6.6 AND COROLLARY 6.7 (APPENDIX B.2). The axioms (and proof rule) follow from the homomorphic definition of semianalytic progress formulas which implies that any semianalytic formula $P$ in normal form (5) has a corresponding normal form for $\neg P$ such that the equivalence $\neg(\dot{P}^{(*)}) \leftrightarrow (\neg P)^{(*)}$ is provable. Classically, in any state, either formula $\dot{P}^{(*)}$ or $\neg(\dot{P}^{(*)})$ is true. Therefore, by LP$_\mathbb{R}$, the ODE must (exclusively, by uniqueness) either locally progress into $P$ or $\neg P$ from this state. Both axioms LP, $\neg\bigcirc$ are derivable consequences of this fact, as shown syntactically in Appendix B.2. Rule CLP follows from LP by congruential equivalence [32].    □

Congruence rule CLP shows that *any* equivalent choice of normal form (5) for semianalytic formula $P$ gives a local progress formula that is (provably) equivalent to $\dot{P}^{(*)}$. Note that the rule works for all (semianalytic) equivalences, including arithmetical ones, e.g., $\exp(x) = 1 \leftrightarrow x = 0$ from (1), so CLP does not follow immediately from the homomorphic definition of progress formulas.

## 6.2 Completeness for Semianalytic Invariants

Combining derived axiom LP and derived rule rI yields an effective proof rule which reduces a semianalytic invariance question to questions involving purely arithmetic formulas:

THEOREM 6.8 (SEMIANALYTIC INVARIANTS). *The semianalytic invariant proof rule sAI derives from RI, Dadj, Cont, Uniq for semianalytic formula $P$.*

$$\text{sAI} \quad \frac{P \vdash \dot{P}^{(*)} \qquad \neg P \vdash (\dot{\neg P})^{-(*)}}{P \vdash [x' = f(x)]P}$$

PROOF. This follows immediately by rewriting the premises of rule rI with the equivalence LP.    □

Completeness of sAI was first proved semantically for polynomial terms languages [22], making crucial use of semialgebraic sets and real analytic solutions to polynomial ODE systems. The proof rule sAI *derives* syntactically in dL and generalizes to semianalytic invariants for extended term languages. Its completeness derives syntactically too, which yields dL disproofs of semianalytic invariance when arithmetic counterexamples can be found.

THEOREM 6.9 (SEMIANALYTIC INVARIANT COMPLETENESS). *The semianalytic invariant axiom SAI derives from RI, Dadj, Cont, Uniq for semianalytic formula $P$.*

$$\text{SAI} \quad \forall x\,(P \rightarrow [x' = f(x)]P) \leftrightarrow \forall x\,\left(P \rightarrow \dot{P}^{(*)}\right) \wedge \forall x\,\left(\neg P \rightarrow (\dot{\neg P})^{-(*)}\right)$$

In Appendix B, a generalization of Theorem 6.9 is proven that handles semianalytic evolution domains $Q$ using LP and a corresponding generalization of axiom RI. The same appendix also proves the following generalization of Theorem 4.5 for semianalytic evolution domains:

THEOREM 6.10 (ANALYTIC COMPLETENESS WITH SEMIANALYTIC DOMAINS). *The differential radical invariant axiom DRI& derives from Cont, Uniq for semianalytic formula $Q$.*

$$\text{DRI\&} \quad [x' = f(x) \,\&\, Q]e = 0 \leftrightarrow \left(Q \rightarrow e = 0 \wedge (\dot{Q}^{(*)} \rightarrow \dot{e}^{(*)} = 0)\right)$$

Thus, dL is complete for proving invariance of *all* (semi)analytic $P$ of differential equations because it reduces all such questions equivalently to first-order formulas, e.g., on the RHS of derived axiom SAI. In addition, dL decides invariance properties for all first-order real arithmetic formulas $P$, because quantifier elimination [4] can equivalently rewrite $P$ to (semialgebraic) normal form (5) first. Unlike for Theorem 4.5 and its generalization Theorem 6.10, which equivalently reduce the future truth of analytic postconditions directly, Theorem 6.9 and its generalized version in Appendix B are only equivalences for invariants $P$, the search of which is the only remaining challenge.

Of course, the complete proof rule sAI can be used to prove all of the suggested invariants for the ODE $\alpha_e$ from (2). However, Example 3.3 gives a significantly simpler proof for the invariance of $1 - u^2 - v^2 \succcurlyeq 0$ with dbx$_{\succcurlyeq}$. This has implications for implementations of sAI: simpler proofs help minimize dependence on real arithmetic decision procedures. For semianalytic formulas (that are not semialgebraic), proof rules resulting in simpler arithmetic premises might even be preferable because validity of these arithmetic premises is undecidable in general [36]. Logically, when $P$ is formed from only strict (resp. non-strict) inequalities then the left (resp. right) premise of sAI closes trivially. This logical fact corresponds to the topological fact that the set $P$ characterizes is topologically open (resp. closed) so only one of the two exit trajectories in Section 5.2 can occur.

## 7 NOETHERIAN FUNCTIONS

This section studies the class of Noetherian functions which meets all of the extended term conditions required in Section 2.4 and therefore inherits all soundness and completeness results of the preceding sections, including Theorem 4.5 and Theorem 6.9.

### 7.1 Mathematical Preliminaries

The following definition of Noetherian functions is standard, although the parameters that are used for studying the complexity of these functions [3, 11, 12] have been omitted. The notation $h : H \subseteq \mathbb{R}^k \to \mathbb{R}$ is used for real-valued functions with domain $H$, i.e., an open, connected subset of $\mathbb{R}^k$. With a slight abuse of notation, polynomials $p \in \mathbb{R}[x]$ over indeterminates $x = (x_1, \ldots, x_n)$ and their corresponding polynomial functions $p(x_1, \ldots, x_n)$ in $\mathbb{R}^n \to \mathbb{R}$ are used interchangeably.

*Definition 7.1 (Noetherian chain and Noetherian function).* A *Noetherian chain* is a sequence of real analytic functions $h_1, \ldots, h_r : H \subseteq \mathbb{R}^k \to \mathbb{R}$ such that all partial derivatives in $H$ for all $i = 1, \ldots, k$ and $j = 1, \ldots, r$ have the following form, where each $q_{ij} \in \mathbb{R}[y, z]$ is a polynomial in $k + r$ indeterminates with $y = (y_1, \ldots, y_k), z = (z_1, \ldots, z_r)$:

$$\frac{\partial h_j}{\partial y_i}(y) = q_{ij}(y, h_1(y), \ldots, h_r(y)) \tag{6}$$

The function $h : H \subseteq \mathbb{R}^k \to \mathbb{R}$ is *Noetherian* iff it can be written as $h(y) = p(y, h_1(y), \ldots, h_r(y))$, where $p \in \mathbb{R}[y, z]$ is a polynomial in $k + r$ indeterminates and $h_1, \ldots, h_r$ is a Noetherian chain. In that case, $h$ is said to be *generated* by this polynomial and Noetherian chain respectively but the choice of generating chain and polynomial for $h$ is not unique.

For the term language extension (1), exp is a 1-element Noetherian chain because $\frac{\partial \exp(y)}{\partial y} = \exp(y)$, while sin, cos form a 2-element Noetherian chain. All three functions together form a 3-element Noetherian chain. More generally, the union of any (finite) number of Noetherian chains is a Noetherian chain. By definition, any element of a Noetherian chain is itself a Noetherian function so exp, sin, cos are also Noetherian functions. It is often useful to consider Noetherian functions over a larger domain than the generating chain, e.g., $h(x, y) = \exp(y) + \sin(x)$ with $h : \mathbb{R}^2 \to \mathbb{R}$. In this case, the domain of definition of the generating chain is implicitly extended by treating them

as functions over the dimensionally larger domain, e.g., with $\exp(x, y), \sin(x, y) : \mathbb{R}^2 \to \mathbb{R}$ which ignore their first and second argument respectively. This is compatible with Def. 7.1 because the partial derivatives with respect to the ignored arguments is trivially zero.

Proposition 7.2 gives important closure properties of the Noetherian functions generated by the same Noetherian chain, which are crucial later and explain the name *Noetherian* function [12, 41].

PROPOSITION 7.2 ([3, 11, 12]). *The set $R$ of Noetherian functions generated by a given Noetherian chain $h_1, \ldots, h_r : H \subseteq \mathbb{R}^k \to \mathbb{R}$ is a Noetherian ring that is closed under partial derivatives.*

PROOF. Let $y = (y_1, \ldots, y_k), z = (z_1, \ldots, z_r)$ abbreviate indeterminates as in Def. 7.1. The set $R$ is a ring under the usual addition and multiplication of real-valued functions because the corresponding generating polynomials form a ring. Now, $R$ is Noetherian because it is a finitely generated algebra [6, §2.11, Corollary 3] over the Noetherian polynomial ring $\mathbb{R}[y]$. The following constructive proof yields a computational method that is used later.

Consider an ascending chain of ideals $I_0 \subseteq I_1 \subseteq \cdots$ in $R$. For each $I_i$, associate the set of generating polynomials $J_i \stackrel{\text{def}}{=} \{p \mid p(y, h_1(y), \ldots, h_r(y)) \in I_i\} \subseteq \mathbb{R}[y, z]$ with respect to the generating Noetherian chain. Each $J_i$ is an ideal in $\mathbb{R}[y, z]$ because the corresponding $I_i$ are themselves ideals. By construction, $J_i \subseteq J_{i+1}$ because $I_i \subseteq I_{i+1}$ for all $i$. Since $J_0 \subseteq J_1 \subseteq \cdots$ is an ascending chain of ideals in $\mathbb{R}[y, z]$, which is a Noetherian polynomial ring, it must stabilize at some $N$ with $J_N = J_{N+1} = \cdots$. Correspondingly, the chain of ideals $I_i$ stabilizes (at the latest) at $N$ so $R$ is Noetherian. The chain $I_0 \subseteq I_1 \subseteq \cdots$ may stabilize earlier than the corresponding $J_i$ chain but that is not important here.

To show that $R$ is closed under partial derivatives, let $h(y) = p(y, h_1(y), \ldots, h_r(y)) \in R$ with $p \in \mathbb{R}[y, z]$. For the partial derivative of $h$ with respect to $y_i$, applying the chain rule yields:

$$\frac{\partial h}{\partial y_i}(y) = \frac{\partial p(y, h_1(y), \ldots, h_r(y))}{\partial y_i} = \frac{\partial p}{\partial y_i}(y, h_1(y), \ldots, h_r(y)) + \sum_{j=1}^{r} \frac{\partial p}{\partial z_j}(y, h_1(y), \ldots, h_r(y)) \frac{\partial h_j}{\partial y_i}(y)$$

By definition, $\frac{\partial p}{\partial y_i}(y, h_1(y), \ldots, h_r(y)) \in R$ since $\frac{\partial p}{\partial y_i}$ is a polynomial in $\mathbb{R}[y, z]$. Each summand $\frac{\partial p}{\partial z_j}(y, h_1(y), \ldots, h_r(y)) \in R$ since $\frac{\partial p}{\partial z_j}$ is a polynomial in $\mathbb{R}[y, z]$, and $\frac{\partial h_j}{\partial y_i}(y) \in R$ by definition because $h_1, \ldots, h_r$ is a Noetherian chain. Hence, all RHS sub-terms are in $R$, and so $\frac{\partial h}{\partial y_i}(y) \in R$. □

Proposition 7.2 implies that adding Noetherian functions to their generating chains yields another Noetherian chain generating the same Noetherian ring $R$ of Noetherian functions because $R$ is closed under ring addition and multiplication. Beyond closure properties for a single Noetherian chain, the class of all Noetherian functions is also closed under other mathematical operations, including function composition, multiplicative inverses, and function inverses (with appropriate assumptions) [3]. Closure under function composition is proved constructively as it is used later.

PROPOSITION 7.3 ([3]). *If $h : H \subseteq \mathbb{R}^k \to \mathbb{R}$ is Noetherian and $v : \Upsilon \subseteq \mathbb{R}^l \to \mathbb{R}^k$ has a compatible image $v(\Upsilon) \subseteq H$ where each component $v_i : \Upsilon \subseteq \mathbb{R}^l \to \mathbb{R}$ for $i = 1, \ldots, k$ is Noetherian, then the function composition $f = h(v_1, \ldots, v_k) : \Upsilon \subseteq \mathbb{R}^l \to \mathbb{R}$ is Noetherian.*

PROOF. Let $y = (y_1, \ldots, y_k), z = (z_1, \ldots, z_r), \gamma = (\gamma_1, \ldots, \gamma_l)$ abbreviate indeterminates. The composed function $f$ is well-defined on $\Upsilon$ since $v(\Upsilon) \subseteq H$. By assumption, $h(y) = p(y, h_1(y), \ldots, h_r(y))$ for some generating Noetherian chain $h_1, \ldots, h_r : H \subseteq \mathbb{R}^k \to \mathbb{R}$ and polynomial $p \in [y, z]$. Since the union of Noetherian chains is Noetherian and by Proposition 7.2, assume without loss of generality, that the Noetherian functions $v_i$ for $i = 1, \ldots, k$ are members of the same generating Noetherian chain $v_1, \ldots, v_s : \Upsilon \subseteq \mathbb{R}^l \to \mathbb{R}$ with $k \leq s$. Putting these together, $f$ can be written as:

$$f = p(v, f_1, \ldots, f_r)$$

where $v = (v_1, \dots, v_k)$ and the function compositions $f_i \stackrel{\text{def}}{=} h_i(v_1, \dots, v_k)$ for $i = 1, \dots, r$. From this representation, $f$ is generated by polynomial $p$ over the sequence:

$$v_1, \dots, v_s, f_1, \dots, f_r \tag{7}$$

In order to show that (7) is a Noetherian chain, it suffices to check that the $f_1 \dots, f_r$ obey the condition on partial derivatives (6) because $v_1, \dots, v_s$ is already a Noetherian chain. For each $f_i(\gamma) : \Upsilon \subseteq \mathbb{R}^l \to \mathbb{R}$, taking the partial derivative with respect to $\gamma_j$ and applying the chain rule:

$$\frac{\partial f_i}{\partial \gamma_j}(\gamma) = \frac{\partial h_i(v_1(\gamma), \dots, v_k(\gamma))}{\partial \gamma_j} = \sum_{l=1}^{k} \frac{\partial h_i}{\partial y_l}(v_1(\gamma), \dots, v_k(\gamma))\frac{\partial v_l}{\partial \gamma_j}(\gamma)$$

It suffices to check that each sub-term appearing on the RHS sum are generated as polynomials over the sequence (7). The case for each $\frac{\partial v_l}{\partial \gamma_j}(\gamma)$ follows immediately because $v_1, \dots, v_s$ is a Noetherian chain. Since $h_1, \dots, h_r$ is a Noetherian chain, each $\frac{\partial h_i}{\partial y_l}$ is a polynomial combination $\frac{\partial h_i}{\partial y_l} = t_{il}(y, h_1, \dots, h_r)$ for some polynomial $t_{il} \in \mathbb{R}[y, z]$ and, thus, $\frac{\partial h_i}{\partial y_l}$ is generated by chain (7):

$$\frac{\partial h_i}{\partial y_l}(v_1, \dots, v_k) = t_{il}(v, h_1(v), \dots, h_r(v)) = t_{il}(v, f_1, \dots, f_r) \qquad \square$$

Before turning to the study of Noetherian functions in dL, it is helpful to first understand how they help with its differential equations reasoning. Polynomial ODEs are very expressive and earlier results [17, 23, 28] make use of polynomial ODEs to implicitly characterize (and thus, eliminate) real analytic functions appearing in initial value problems (IVPs). IVPs are specified by a system of ODEs, $x' = f(x)$, defined over domain $D$ with RHS $f(x) : D \subseteq \mathbb{R}^n \to \mathbb{R}^n$ and real initial value $X_0 \in D \subseteq \mathbb{R}^n$. The IVP is called Noetherian (resp. polynomial) when all components of the RHS $f(x)$ are Noetherian functions (resp. polynomials). Both Noetherian and polynomial functions are analytic and therefore continuously differentiable. Under the assumption of continuously differentiable RHS, the Picard-Lindelöf theorem [44, §10.VI] guarantees that the IVP has a unique maximal solution $\varphi(t) : (\alpha, \beta) \to \mathbb{R}^n$ with $-\infty \le \alpha < 0 < \beta \le \infty$ such that $\varphi(0) = X_0$ and $\frac{d\varphi(t)}{dt} = f(\varphi(t))$. Uniqueness and maximality here means that every solution of the IVP is a truncation of $\varphi$ to a smaller existence interval. The following generalizes aforementioned results [17, 23, 28] to the Noetherian setting:

PROPOSITION 7.4. *Function $\varphi : (\alpha, \beta) \to \mathbb{R}^n$ with $-\infty \le \alpha < 0 < \beta \le \infty$ is the (coordinate-projected) solution of a Noetherian IVP iff it is the (coordinate-projected) solution of a polynomial IVP.*

PROOF. In the (trivial) converse "$\Leftarrow$" direction, suppose function $\varphi$ solves the polynomial IVP $x' = p(x, y), y' = q(x, y)$ with initial values $X_0 \in \mathbb{R}^n, Y_0 \in \mathbb{R}^r$. Let $\varphi_x, \varphi_y$ denote the projection onto the $x$ and $y$ coordinates of $\varphi$ respectively. Every solution of polynomial ODEs is a univariate Noetherian function [12]. Therefore, the Noetherian IVP given by $x' = p(\varphi_x(\tau), \varphi_y(\tau)), \tau' = 1$ with the same initial value for $x$ and 0 for $\tau$ trivially has the (unique) solution $(\varphi_x(t), t) : (\alpha, \beta) \to \mathbb{R}^n \times \mathbb{R}$.

In the (nontrivial) "$\Rightarrow$" direction, suppose that $\varphi$ is the solution to the Noetherian IVP $x' = f(x)$ where each $f_i(x) : D \subseteq \mathbb{R}^n \to \mathbb{R}$ is Noetherian, and with initial value $X_0 \in D$. By uniqueness of solutions, it suffices to construct a polynomial IVP so that $\varphi(t)$ solves it in the $x$ coordinates.

Since the union of Noetherian chains is itself a Noetherian chain, assume without loss of generality that the functions $f_1, \dots, f_n$ are generated by the same Noetherian chain $h_1, \dots, h_r$ and that $f_i = p_i(x, h_1(x), \dots, h_r(x))$ for some polynomials $p_i \in \mathbb{R}[x, y]$ in $n+r$ indeterminates for $i = 1, \dots, n$. Introduce new variables $y_j$ for $j = 1, \dots, r$ which are meant to take on the respective value of $h_j$ along solutions to the ODE. Accordingly, the RHS of the Noetherian ODE is rewritten by replacing each $f_i$ with $p_i(x, y)$, i.e., the desired polynomial ODEs for $x$ is $x' = p(x, y)$.

It remains to ensure that each of these newly introduced variables $y_j$ take on their intended values $h_j(\varphi(t))$ along the solution $\varphi$. By (6), the partial derivatives for each $h_j$ can be written as polynomials $q_{ij} \in \mathbb{R}[x, y]$ over the generating Noetherian chain. By the chain rule:

$$\frac{dh_j(\varphi(t))}{dt} = \sum_{i=1}^{n} \frac{\partial h_j(x)}{\partial x_i}(\varphi(t))\frac{d\varphi_i(t)}{dt} = \sum_{i=1}^{n} q_{ij}(\varphi(t), h_1(\varphi(t)), \ldots, h_r(\varphi(t)))\frac{d\varphi_i(t)}{dt}$$

Back-substituting into the RHS of this equation using the intended values for $y_j$ and the new ODEs for $x$, yields the following additional ODEs for $y$:

$$y'_j = \sum_{i=1}^{n} q_{ij}(x, y)p_i(x, y)$$

The RHS of these additional ODEs are polynomials in $\mathbb{R}[x, y]$, which completes the desired polynomial IVP with the initial values $Y_0 \overset{\text{def}}{=} (h_1(x_0), \ldots, h_r(x_0)) \in \mathbb{R}^r$ for $y$. The construction of this polynomial IVP is correct-by-construction because of the mechanical chain rule computation. A solution to this IVP is given by the pair $(\varphi(t), y(t)) : (\alpha, \beta) \to \mathbb{R}^n \times \mathbb{R}^r$ where $y_j(t) \overset{\text{def}}{=} h_j(\varphi(t))$ : $(\alpha, \beta) \to \mathbb{R}$. By uniqueness of solutions, this completes the proof of the "$\Rightarrow$" direction.                □

In the "$\Rightarrow$" direction of Proposition 7.4, the constructed polynomial IVP may involve additional ODEs over the variables $y$ (with their respective initial values). The number of additional equations required in this construction is the length of the shortest Noetherian chain that generates the RHS of the input Noetherian ODE. The polynomial IVP may have a larger maximal interval of existence than the input Noetherian IVP if it leaves the domain $D$ of the input RHS. In the "$\Leftarrow$" direction, only one additional time variable $\tau$ is required. Consequently, the solution of *any* $n$-dimensional IVP that is the coordinate projection of the solution of a polynomial IVP (of potentially much larger dimension) is the coordinate projection of the solution of an $(n + 1)$-dimensional Noetherian IVP.

The constructive proof of the "$\Rightarrow$" direction in Proposition 7.4 yields an approach for transforming input Noetherian IVPs to polynomial IVPs assuming that the Noetherian functions can be effectively associated with generating Noetherian chains and polynomials.

*Example 7.5 (Flight dynamics [28, Equation 1]).* A simple planar model of curved aircraft motion is given by the following ODE system, where $(x, y)$ are the aircraft's planar coordinates, $\theta$ its angular orientation, and $v, \omega$ its linear and angular velocity respectively [28, Equation 1]:

$$x' = v\cos(\theta), \quad y' = v\sin(\theta), \quad \theta' = \omega$$

Consider an IVP for this ODE with initial values $x = X_0, y = Y_0, \theta = \Theta_0 \in \mathbb{R}$. The linear and angular velocities $v, \omega$ are left as symbolic constants in this model.

The RHS of the ODE is generated by the Noetherian chain: $\sin(\theta), \cos(\theta)$. Introducing additional variables $z_1, z_2$ for the elements of this chain, and replacing the RHS for $x', y'$ according to their generating polynomials with respect to the chain gives:

$$x' = vz_1, \quad y' = vz_2, \quad \theta' = \omega$$

A symbolic calculation (see Proposition 7.4) yields the following ODEs that $z_1, z_2$ must obey:

$$z'_1 = \omega z_2, \quad z'_2 = -\omega z_1$$

To finish constructing the polynomial IVP, set the initial values $z_1 = \sin(\Theta_0), z_2 = \cos(\Theta_0)$. The resulting ODE has higher dimension but a polynomial RHS.

The utility of adding Noetherian functions to dL is *not* an increase in expressiveness of the differential equations. Rather, it allows Noetherian ODEs to be written down naturally instead of relying on implicit polynomial characterization such as in Example 7.5. More importantly, they make it possible to use formulas as ODE invariants that are *not* semialgebraic. By Theorem 4.5 and Theorem 6.9, the dL ODE axiomatization provides an effective and complete calculus for (dis)proving the resulting semianalytic ODE invariants involving Noetherian functions. This requires Noetherian functions to meet the extended term conditions from Section 2.4, which is shown next.

### 7.2 Extended Term Conditions for Noetherian Functions

Assume from now on that the fixed $k$-ary function symbols $h_1, \ldots, h_r$ are interpreted semantically as members of a Noetherian chain $h_1, \ldots, h_r : \mathbb{R}^k \to \mathbb{R}$ respectively. Recall that extended dL terms are formed syntactically from these function symbols according to the grammar (Section 2.1). As discussed in Section 2.2, the choice of domain $\mathbb{R}^k$ for these functions ensures that the term semantics is well-defined in all states. The first two extended term conditions are straightforward to check:

(S) All Noetherian functions are, by definition, $C^\infty$ smooth (even real analytic) so the semantics of differentials are well-defined.

(P) The partial derivative of each $h_j(y_1, \ldots, y_k) : \mathbb{R}^k \to \mathbb{R}$ with respect to $y_i$ satisfies (6) for some polynomial $q_{ij} \in \mathbb{R}[y, z]$. Since polynomials are generated by addition and multiplication, these partial derivatives $\frac{\partial h}{\partial y_i}(y_1, \ldots, y_k)$ are syntactically represented by the extended term:

$$q_{ij}\big(y_1, \ldots, y_k, h_1(y_1, \ldots, y_k), \ldots, h_r(y_1, \ldots, y_k)\big)$$

Thus, Lemma 2.5 adds the (sound) differential axioms for each fixed function symbol $h_j$ and therefore, all Lie derivatives are representable in the extended term language.

The final condition (R) is more involved and relies crucially on closure properties of Noetherian functions. A syntactic subtlety arises for extended terms with nested function applications such as $\exp(\exp(x))$. Its semantics is the iterated real exponential function generated by the 2-element Noetherian chain $\exp(x), \exp(\exp(x))$. Thus, even though the fixed function symbols $h_1, \ldots, h_r$ form a Noetherian chain, the extended term grammar could produce extended terms that *do not* correspond to Noetherian functions generated by that chain. The following lemma resolves this issue by computing another (syntactic) Noetherian chain that generates it instead:

LEMMA 7.6. *The semantics of every extended term $e$ over Noetherian functions is a Noetherian function and $e$ can be effectively associated with a (syntactic) Noetherian chain that generates it.*

PROOF. By structural induction on extended dL term $e$. The cases for variables and constants are obvious, while the cases for addition and multiplication follow inductively from closure under ring operations (Proposition 7.2) and the fact that finite unions of Noetherian chains are Noetherian chains. The only difficult case is when $e$ is a function composition $h(e_1, \ldots, e_k)$, where $e_1, \ldots, e_k$ are extended terms. Inductively, each $e_1, \ldots, e_k$ semantically is a Noetherian function. Moreover, $h$ is (semantically) a Noetherian function by the assumption that the interpretation of all fixed function symbols is an element of some Noetherian chain. Thus, Proposition 7.3 implies that the semantics of their composition is also a Noetherian function. Let $v_1, \ldots, v_s$ be the union of Noetherian chains obtained inductively for $e_1, \ldots, e_k$. The (constructive) proof of Proposition 7.3 shows that the Noetherian chain (7) given by $v_1, \ldots, v_s, f_1, \ldots, f_r$ generates $h(e_1, \ldots, e_k)$, where $v_1, \ldots, v_s$ are syntactically represented by extended terms using the induction hypothesis on $e_1, \ldots, e_k$ and each $f_i \stackrel{\text{def}}{=} h_i(e_1, \ldots, e_k)$ is an extended term by construction. □

Lemma 7.6 makes it possible to unambiguously refer to "the" generating Noetherian chain and polynomial for any extended term $e$ by giving an effective procedure for finding their syntactic representations in the extended term language. Together with Proposition 7.2, this suffices to prove that the extended term language has the computable differential radicals condition (R).

THEOREM 7.7. *Term languages with Noetherian functions satisfy the extended term conditions.*

PROOF. Conditions (S) and (P) have already been shown above. It remains to show condition (R), i.e., any ODE $x' = f(x)$ and extended term $e$ has a computable (and provable) differential radical identity (3). By Lemma 7.6, the terms $f(x), e$ are (semantically) Noetherian and so, by taking the union of Noetherian chains, are defined by the same generating Noetherian chain $v_1, \ldots, v_s$. The ring $R$ generated by this chain is Noetherian by Proposition 7.2 and is closed under partial derivatives. Recall that the Lie derivative of $e$ along $x' = f(x)$ is given by:

$$\mathcal{L}_{f(x)}(e) \stackrel{\text{def}}{=} \sum_{i=1}^{n} \frac{\partial e}{\partial x_i} \cdot f_i(x)$$

Every sub-term on the RHS of its Lie derivative is contained in the ring $R$ because it already contains the RHS of the ODEs, $f(x)$, and is closed under the partial derivatives of $e$. Inductively, all higher Lie derivatives $\dot{e}^{(i)}$ for $i = 0, 1, \ldots$ are contained in $R$ and are therefore generated by the chain $v_1, \ldots, v_s$ with $\dot{e}^{(i)} = p_i(x, v_1, \ldots, v_s)$ for polynomials $p_i \in \mathbb{R}[x, y]$ and $y = (y_1, \ldots, y_s)$.

Following the proof of Proposition 7.2, consider this ascending chain of polynomial ideals:

$$(p_0) \subseteq (p_0, p_1) \subseteq (p_0, p_1, p_2) \subseteq \cdots$$

This chain stabilizes with the provable polynomial identity $p_N = \sum_{i=0}^{N-1} q_i p_i$ for some polynomial cofactors $q_i \in \mathbb{R}[x, y]$ and $N \geq 1$. The rank $N$ and the polynomial cofactors $q_i$ are computable by successive ideal membership checks [15, 16, 22]. Mapping this back into elements of $R$ gives the required provable identity for the Lie derivatives of $e$ by choosing $g_i \stackrel{\text{def}}{=} q_i(x, v_1, \ldots, v_s)$:

$$\dot{e}^{(N)} = \sum_{i=0}^{N-1} g_i \dot{e}^{(i)} \qquad \qquad \square$$

An immediate corollary is that term language extensions with Noetherian functions inherit all earlier soundness and completeness results, e.g., from Section 4.2 and Section 6.2.

COROLLARY 7.8 (NOETHERIAN INVARIANT COMPLETENESS). *The* dL *proof calculus is complete for (semi)analytic invariants of ODEs for term languages extended with Noetherian functions.*

PROOF. This follows from the extended term conditions for Noetherian functions (Theorem 7.7) and the completeness theorems Theorem 4.5 and Theorem 6.9.                                        $\square$

## 7.3 Extended Term Language Example

This section illustrates constructions from Section 7.1 and Section 7.2 using the extended term language (1). The first example shows the computations from Lemma 7.6 and Theorem 7.7:

*Example 7.9 (Syntactic manipulation of Noetherian functions).* Consider the ODE $x' = \exp(\sin(x))$ and the term $e = x + x^2$. The Noetherian chain for $e$ is empty because it is already a polynomial while the Noetherian chain associated with $\exp(\sin(x))$ is $v_1 = \sin(x), v_2 = \cos(x), v_3 = \exp(\sin(x))$. The higher Lie derivatives of $e$ are all extended terms generated by the chain $v_1, v_2, v_3$:

$$\dot{e}^{(1)} = v_3 + 2v_3 x \quad \dot{e}^{(2)} = v_3^2 v_2 + 2(v_3^2 v_2 x + v_3^2) = (2v_3 + v_2 v_3 + 2v_2 v_3 x)((1 + 2x)\dot{e}^{(1)} - 4v_3 e)$$

The (polynomial) identity for $\dot{e}^{(2)}$ in terms of $\dot{e}^{(1)}$, $e$ and their cofactors is obtained computationally by ideal membership checks for the polynomial ring $\mathbb{R}[x, y_1, y_2, y_3]$ (the indeterminate $y_i$ corresponds to $v_i$ for $i = 1, 2, 3$), following Proposition 7.2.

The next example illustrates how the extended term language allows effective proofs of more invariants than possible with polynomial term languages.

*Example 7.10 (Expressivity of Noetherian invariants).* The polynomial invariant $1 - u^2 - v^2 = 0$ was proved for the ODE $\alpha_e$ from (2) in Example 3.3. With respect to Fig. 1, this means that a trajectory starting at the point $(1, 0)$ stays on the circle. However, this invariant yields no information about how fast the trajectory loops around the circle or whether it revolves clockwise or anti-clockwise. In the extended term language, the most precise invariant can be proved, namely the solution to the ODEs from this initial point. The solution is a trigonometric function of time (given below), and so cannot be expressed as a polynomial (or semialgebraic) invariant [4]. The precise solution also shows that the motion is anti-clockwise, as suggested by Fig. 1.

The following derivation uses a DC to add the known polynomial invariant $1 - u^2 - v^2 = 0$ which proves by dbx as in Example 3.3. The right premise after the differential cut assumes $1 - u^2 - v^2 = 0$ in the ODE's evolution domain constraint. It is abbreviated ① and continued below.

$$
\text{DC} \cfrac{\text{dbx, }\mathbb{R}\cfrac{*}{u = 1, v = 0, t = 0 \vdash [\alpha_e, t' = 1]1 - u^2 - v^2 = 0} \qquad ①}{u = 1, v = 0, t = 0 \vdash [\alpha_e, t' = 1](u - \cos(t) = 0 \land v - \sin(t) = 0)}
$$

From ①, first calculate the Lie derivatives, abbreviating $c = u - \cos(t)$, $s = v - \sin(t)$:

$$
\mathcal{L}_{\alpha_e, t'=1}(c) = \mathcal{L}_{\alpha_e, t'=1}(u - \cos(t)) = -v + \frac{u}{4}(1 - u^2 - v^2) + \sin(t) = -s + \frac{u}{4}(1 - u^2 - v^2)
$$

$$
\mathcal{L}_{\alpha_e, t'=1}(s) = \mathcal{L}_{\alpha_e, t'=1}(v - \sin(t)) = u + \frac{v}{4}(1 - u^2 - v^2) - \cos(t) = c + \frac{u}{4}(1 - u^2 - v^2)
$$

Under the domain constraint assumption $1 - u^2 - v^2 = 0$, the additional $\frac{u}{4}(1 - u^2 - v^2)$ term in both Lie derivatives simplifies to 0. The derivation starts with a cut of the postcondition $c = 0 \land s = 0$. This arithmetic premise, abbreviated ②, is discussed afterwards. Continuing on the right premise, the vdbx step closes successfully using real arithmetic manipulations only:

$$
\text{cut} \cfrac{② \qquad \text{vdbx}\cfrac{\mathbb{R}\cfrac{*}{1 - u^2 - v^2 = 0 \vdash \begin{pmatrix} \dot{c} \\ \dot{s} \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} c \\ s \end{pmatrix}}}{c = 0 \land s = 0 \vdash [\alpha_e, t' = 1 \,\&\, 1 - u^2 - v^2 = 0](c = 0 \land s = 0)}}{u = 1, v = 0, t = 0 \vdash [\alpha_e, t' = 1 \,\&\, 1 - u^2 - v^2 = 0](c = 0 \land s = 0)}
$$

The premise ② is valid, but involves properties of trigonometric functions ($\cos(0) = 1, \sin(0) = 0$) so it cannot be proved using $\mathbb{R}$. Instead, extended arithmetic $\mathbb{R}_{\exp, \sin, \cos}$ is needed:

$$
\mathbb{R}_{\exp, \sin, \cos}\cfrac{*}{u = 1, v = 0, t = 0 \vdash u - \cos(t) = 0 \land v - \sin(t) = 0}
$$

The extended arithmetic theory is undecidable in general [36] and so, unlike $\mathbb{R}$, rule $\mathbb{R}_{\exp, \sin, \cos}$ cannot be implemented via an underlying decision procedure. Yet, simple arithmetic questions such as ② which just involve the evaluation of trigonometric functions can be easily checked.

The above derivation takes advantage of a known Darboux equality for $1 - u^2 - v^2$ to simplify the proof using vdbx. The proof could have instead directly made use of Theorem 4.5 by encoding $c = 0 \land s = 0$ as $c^2 + s^2 = 0$ and then calculating the rank of $c^2 + s^2$ (which involve trigonometric

functions) according to Theorem 7.7. This also works, but $c^2 + s^2$ has rank 3, and the resulting cofactors are too large to even fit on this page.

The final example highlights an important insight from Proposition 7.4. Even though this article only considers extended term languages with terms that are defined everywhere, it is possible to use logical formulas to implicitly characterize more terms, making use of closure properties of the Noetherian functions [3]. The following example illustrates implicit characterization of quotients which are defined everywhere in the domain of interest:

*Example 7.11 (Implicit characterization of quotients).* The trigonometric tangent function $\tan(x)$ is Noetherian and defined on the interval $(-\frac{\pi}{2}, \frac{\pi}{2})$. Consider the following "formula" where $x$ is restricted in the domain constraint to never reach a point where the RHS $\tan(x)$ is undefined:

$$x = \frac{1}{2} \rightarrow [x' = \tan(x) \,\&\, {-1} \leq x \leq 1]x \geq \frac{1}{2}$$

This "formula" is not formally in the syntax of dL formulas because tan is not defined everywhere. However, Proposition 7.4 can be used to ask an equivalent question in dL. Recall from calculus:

$$\tan(x) = \frac{\sin(x)}{\cos(x)} \qquad \frac{\partial \frac{1}{\cos(x)}}{\partial x} = \frac{\sin(x)}{(\cos(x))^2}$$

Thus, $\sin(x), \cos(x), \frac{1}{\cos x}$ forms a 3-element Noetherian chain that generates $\tan(x)$. For brevity, by partially following the IVP construction of Proposition 7.4, the "formula" is rephrased as an actual dL formula with $y$ representing $\frac{1}{\cos x}$ along the ODE. After replacing $x' = \sin(x)y$, the required differential equation for $y$ is calculated symbolically with $y' = \sin(x)y^2(\sin(x)y) = \sin^2(x)y^3$.

$$x = \frac{1}{2} \wedge \cos(x)y - 1 = 0 \rightarrow [x' = \sin(x)y, y' = \sin^2(x)y^3 \,\&\, {-1} \leq x \leq 1]x \geq \frac{1}{2}$$

For non-zero denominator, the initial value $\frac{1}{\cos(x)}$ of $y$ is logically characterized by the formula $\cos(x)y - 1 = 0$. The following Lie derivative calculation shows that $\cos(x)y - 1$ satisfies a Darboux equality and so $\cos(x)y - 1 = 0$ can be proven invariant along the ODE (abbreviated as $\alpha$) by dbx.

$$\mathcal{L}_\alpha(\cos(x)y - 1) = {-\sin(x)(\sin(x)y)y} + \cos(x)(\sin^2(x)y^3) = \sin^2(x)y^2(\cos(x)y - 1)$$

The rephrased formula proves after a DC with this Darboux invariant for $y$ using the ODE invariant $x \geq \frac{1}{2}$ and rule sAI (or its generalization with domain constraints from Appendix B). Briefly, the invariance of $x \geq \frac{1}{2}$ provably reduces to the following arithmetic premise which is valid and falls within a *decidable* fragment of arithmetic with trigonometric functions [24]:

$$-1 \leq x \leq 1, \cos(x)y - 1 = 0, x = \frac{1}{2} \vdash \sin(x)y > 0$$

## 8  RELATED WORK

This related work discussion focuses on deductive verification of hybrid systems. An overview of approaches to hybrid systems verification is available elsewhere [8]. Readers interested in ODEs [44], real analysis [20, 44], algebra [6], and real algebraic geometry [4] are referred to the cited textbooks. The orthogonal task of efficiently generating invariants is investigated elsewhere [15, 22, 37].

*Proof Rules for ODE Invariants.* Numerous useful but incomplete proof rules for ODE invariants [31, 35, 37, 39] are surveyed elsewhere [16]. The soundness and completeness theorems for dRI and sAI were previously proved semantically [15, 22]. These earlier results are limited to (semi)algebraic invariants as they depend on specific semantic properties limited to polynomials.

The extended term conditions (Section 2.4) and Noetherian functions (Section 7) generalize these results, showing that all (semi)analytic invariance questions reduce completely to arithmetic.

In their original presentation [15, 22], dRI and sAI are *algorithmic procedures* for checking invariance of semialgebraic sets, requiring e.g., checking ideal membership for all polynomials in the semialgebraic decomposition. This makes them difficult to implement soundly within a small, trusted axiomatic core [10]. This article shows that, by relying on the logic dL, these rules can be *derived* from a small set of axiomatic principles. Although these derivations also leverage ideal computations, they are only used in *derived rules*. With the aid of a theorem prover, derived rules can be implemented as tactics that crucially remain *outside* its soundness-critical axiomatic core.

*Deductive Power and Proof Theory.* The derivations shown in this article are fully general, which is necessary for completeness of the resulting derived rules. The number of conjuncts in the progress and differential radical formula for an extended term $e$ is equal to the rank of $e$. Known upper bounds for the rank, even in the case of polynomials in $n$ variables, are doubly exponential in $n^2 \ln n$ [25]. Many simpler classes of invariants can be proved using simpler derivations, as exemplified by Examples 3.3 and 7.10. This is where a study of the deductive power of sound, but incomplete, proof rules [16] is essential. For ODE invariants of a simpler class, it suffices to use a proof rule that is complete for just that class. This intuition is echoed in an earlier study [31] of the relative deductive power of differential invariants (DI), differential cuts (DC), and differential ghosts (DG). The first completeness result (Theorem 4.5) shows that dL with DG is complete for algebraic and analytic invariants. Other proof-theoretical studies of dL [29] reveal surprising correspondences between its hybrid, continuous, and discrete aspects in the sense that each aspect can be axiomatized completely and effectively relative to any other aspect. Corollary 4.6 constructively exploits their combination.

*Noetherian Functions.* This article only touched on basic properties of Noetherian functions. The model-theoretic study of Noetherian functions and the related Pfaffian functions is fascinating in its own right [3, 11, 12]. Pfaffian functions are generated by chains satisfying (6) except with triangular dependencies in their partial derivatives [12], and notably, the expansion of the real field with Pfaffian functions is o-minimal [38, 43, 45]. Such o-minimal expansions have been studied in reachability analysis for *o-minimal hybrid systems* [19, 21] because they admit the construction of finite bisimulations for reachability analysis algorithms. In contrast, expansions with (more general) Noetherian functions, e.g., (unrestricted) trigonometric sine and cosine, are not o-minimal because they can be used to characterize the natural numbers. This is a barrier to the construction of finite bisimulations [21] but not for deductive approaches, as long as the relevant arithmetic is provable.

Undecidability of arithmetic is a delicate issue [36], but this article's completeness results show that ODE invariance verification *completely* reduces to arithmetic! Many (necessarily incomplete) approaches and tools for handling special functions are available, e.g., resolution with upper and lower bounds as implemented in MetiTarski [1], $\delta$-decidability as implemented in dReal [13, 14], or heuristic inference-based approaches as implemented in Polya [2]. Specialized decision procedures may also be applicable for restricted fragments of arithmetic [24], as in Examples 7.9 and 7.11. Even in settings where all of these automated tools fail to verify an arithmetic question, the system designer can provide further mathematical intuition with an interactive proof in KeYmaera X [10].

The findings of this article identify Noetherian functions as a more general unifying theme behind earlier results in continuous/hybrid systems verification. Besides the completeness results for invariants, Proposition 7.4 also generalizes earlier results [17, 23, 28] to the Noetherian setting. This idea is called *differential axiomatization* [28] because it axiomatizes ODEs involving special functions that have undecidable arithmetic using polynomial ODEs. Similarly, [23, Proposition 1]

gives an algorithm for replacing a fixed set of functions appearing in IVPs with polynomials ones. The result from [17, Theorem 4] only applies in the case of univariate Noetherian functions.

## 9 CONCLUSION

This article demonstrates the impressive deductive power of differential ghosts: they prove *all* Darboux invariants and, as a consequence, *all* analytic invariants for extended term languages with the extended term conditions. Even *scalar* differential ghosts suffice for this result, but the question of whether their deductive power extends to even larger classes of invariants is left open.

The article then introduces extensions to the dL axiomatization and shows how they can be used to extend completeness to semianalytic invariance. The case of (semi)algebraic invariants is even decidable, but the results prove completeness for much larger classes of (semi)analytic invariants. Table 1 gives an instructive overview of the key mathematical properties of solutions and terms that the soundness of each differential equation axiom rests on. With these axioms, mathematical reasoning for differential equations can be carried out *syntactically* and *axiomatically* within the dL proof calculus. This concise and foundational axiomatization of mathematical properties is precisely what enables generalizations of the authors' earlier results [33] to the (semi)analytic setting with Noetherian functions. A subtle question is left open: the extended term conditions in Section 2.4 do not require that the fixed function symbols $h$ be real analytic even if Noetherian functions are always real analytic. This suggests that there may still be a gap between the extended term conditions and Noetherian functions. Are there $C^\infty$ smooth (or even real analytic) functions that meet the extended term conditions but are *not* Noetherian functions? In other words, are Noetherian functions exactly the class of functions for which completeness results are possible? Certainly, this article's completeness results continue to hold for any functions meeting those conditions, which would make both positive and negative results interesting.

Table 1. Properties of ODE solutions underlying the differential equation axioms of dL.

| ODE Axiom | Mathematical Property |
| --- | --- |
| DI | Mean value theorem |
| DC | Prefix-closure of solutions |
| DG | Picard-Lindelöf theorem |
| Cont | Existence of solutions |
| Uniq | Uniqueness of solutions |
| Dadj | Group action on solutions |
| RI | Completeness of field $\mathbb{R}$ |

## REFERENCES

[1] Behzad Akbarpour and Lawrence C. Paulson. 2010. MetiTarski: An Automatic Theorem Prover for Real-Valued Special Functions. *J. Autom. Reasoning* 44, 3 (2010), 175–205. https://doi.org/10.1007/s10817-009-9149-2

[2] Jeremy Avigad, Robert Y. Lewis, and Cody Roux. 2016. A Heuristic Prover for Real Inequalities. *J. Autom. Reasoning* 56, 3 (2016), 367–386. https://doi.org/10.1007/s10817-015-9356-y

[3] Gal Binyamini. 2019. Density of Algebraic Points on Noetherian Varieties. *Geom. Funct. Anal.* 29, 1 (2019), 72–118. https://doi.org/10.1007/s00039-019-00475-7

[4] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. 1998. *Real Algebraic Geometry*. Springer, Heidelberg. https://doi.org/10.1007/978-3-662-03718-8

[5] Brandon Bohrer, Vincent Rahli, Ivana Vukotic, Marcus Völp, and André Platzer. 2017. Formally Verified Differential Dynamic Logic. In *CPP*, Yves Bertot and Viktor Vafeiadis (Eds.). ACM, New York, 208–221. https://doi.org/10.1145/3018610.3018616

[6] Nicolas Bourbaki. 1998. *Commutative Algebra. Chapters 1–7*. Springer, Berlin.

[7] Pete L. Clark. 2019. The Instructor's Guide to Real Induction. *Math. Mag.* 92, 2 (2019), 136–150. https://doi.org/10.1080/0025570X.2019.1549902

[8] Edmund M. Clarke, Thomas A. Henzinger, Helmut Veith, and Roderick Bloem (Eds.). 2018. *Handbook of Model Checking*. Springer, Cham. https://doi.org/10.1007/978-3-319-10575-8

[9] Jean-Gaston Darboux. 1878. Mémoire sur les équations différentielles algébriques du premier ordre et du premier degré. *Bull. Sci. Math.* 2, 1 (1878), 151–200.

[10] Nathan Fulton, Stefan Mitsch, Jan-David Quesel, Marcus Völp, and André Platzer. 2015. KeYmaera X: An Axiomatic Tactical Theorem Prover for Hybrid Systems. In *CADE (LNCS)*, Amy P. Felty and Aart Middeldorp (Eds.), Vol. 9195. Springer, Cham, 527–538. https://doi.org/10.1007/978-3-319-21401-6_36

[11] Andrei Gabrielov and Askold Khovanskii. 1998. Multiplicity of a Noetherian Intersection. In *Geometry of Differential Equations*. Amer. Math. Soc., Providence, 119–130. https://doi.org/10.1090/trans2/186/03

[12] Andrei Gabrielov and Nicolai Vorobjov. 2004. Complexity of Computations with Pfaffian and Noetherian Functions. In *Normal Forms, Bifurcations and Finiteness Problems in Differential Equations*. Kluwer Acad. Publ., Netherlands, 211–250.

[13] Sicun Gao, Jeremy Avigad, and Edmund M. Clarke. 2012. Delta-Decidability over the Reals. In *LICS*. IEEE Computer Society, 305–314. https://doi.org/10.1109/LICS.2012.41

[14] Sicun Gao, Soonho Kong, and Edmund M. Clarke. 2013. dReal: An SMT Solver for Nonlinear Theories over the Reals. In *CADE (LNCS)*, Maria Paola Bonacina (Ed.), Vol. 7898. Springer, Heidelberg, 208–214. https://doi.org/10.1007/978-3-642-38574-2_14

[15] Khalil Ghorbal and André Platzer. 2014. Characterizing Algebraic Invariants by Differential Radical Invariants. In *TACAS (LNCS)*, Erika Ábrahám and Klaus Havelund (Eds.), Vol. 8413. Springer, Heidelberg, 279–294. https://doi.org/10.1007/978-3-642-54862-8_19

[16] Khalil Ghorbal, Andrew Sogokon, and André Platzer. 2017. A Hierarchy of Proof Rules for Checking Positive Invariance of Algebraic and Semi-Algebraic Sets. *Comput. Lang. Syst. Str.* 47, 1 (2017), 19–43. https://doi.org/10.1016/j.cl.2015.11.003

[17] Daniel S. Graça, Manuel L. Campagnolo, and Jorge Buescu. 2008. Computability with Polynomial Differential Equations. *Adv. Appl. Math.* 40, 3 (2008), 330 – 349. https://doi.org/10.1016/j.aam.2007.02.003

[18] Thomas H. Grönwall. 1919. Note on the Derivatives with Respect to a Parameter of the Solutions of a System of Differential Equations. *Ann. Math.* 20, 4 (1919), 292–296. https://doi.org/10.2307/1967124

[19] Margarita V. Korovina and Nicolai Vorobjov. 2004. Pfaffian Hybrid Systems. In *CSL (LNCS)*, Jerzy Marcinkowski and Andrzej Tarlecki (Eds.), Vol. 3210. Springer, Heidelberg, 430–441. https://doi.org/10.1007/978-3-540-30124-0_33

[20] Steven G. Krantz and Harold R. Parks. 2002. *A Primer of Real Analytic Functions* (second ed.). Birkhäuser, Boston. https://doi.org/10.1007/978-0-8176-8134-0

[21] Gerardo Lafferriere, George J. Pappas, and Shankar Sastry. 2000. O-Minimal Hybrid Systems. *Math. Control Signals Systems* 13, 1 (2000), 1–21. https://doi.org/10.1007/PL00009858

[22] Jiang Liu, Naijun Zhan, and Hengjun Zhao. 2011. Computing Semi-Algebraic Invariants for Polynomial Dynamical Systems. In *EMSOFT*, Samarjit Chakraborty, Ahmed Jerraya, Sanjoy K. Baruah, and Sebastian Fischmeister (Eds.). ACM, New York, 97–106. https://doi.org/10.1145/2038642.2038659

[23] Jiang Liu, Naijun Zhan, Hengjun Zhao, and Liang Zou. 2015. Abstraction of Elementary Hybrid Systems by Variable Transformation. In *FM (LNCS)*, Nikolaj Bjørner and Frank S. de Boer (Eds.), Vol. 9109. Springer, Cham, 360–377. https://doi.org/10.1007/978-3-319-19249-9_23

[24] Scott McCallum and Volker Weispfenning. 2012. Deciding Polynomial-Transcendental Problems. *J. Symb. Comput.* 47, 1 (2012), 16–31. https://doi.org/10.1016/j.jsc.2011.08.004

[25] Dimitri Novikov and Sergei Yakovenko. 1999. Trajectories of Polynomial Vector Fields and Ascending Chains of Polynomial Ideals. *Ann. I. Fourier* 49, 2 (1999), 563–609. https://doi.org/10.5802/aif.1683

[26] Susan S. Owicki and David Gries. 1976. Verifying Properties of Parallel Programs: An Axiomatic Approach. *Commun. ACM* 19, 5 (1976), 279–285. https://doi.org/10.1145/360051.360224

[27] André Platzer. 2008. Differential Dynamic Logic for Hybrid Systems. *J. Autom. Reasoning* 41, 2 (2008), 143–189. https://doi.org/10.1007/s10817-008-9103-8

[28] André Platzer. 2010. Differential-Algebraic Dynamic Logic for Differential-Algebraic Programs. *J. Log. Comput.* 20, 1 (2010), 309–352. https://doi.org/10.1093/logcom/exn070

[29] André Platzer. 2012. The Complete Proof Theory of Hybrid Systems. In *LICS*. IEEE Computer Society, 541–550. https://doi.org/10.1109/LICS.2012.64

[30] André Platzer. 2012. A Differential Operator Approach to Equational Differential Invariants. In *ITP (LNCS)*, Lennart Beringer and Amy P. Felty (Eds.), Vol. 7406. Springer, Heidelberg, 28–48. https://doi.org/10.1007/978-3-642-32347-8_3

[31] André Platzer. 2012. The Structure of Differential Invariants and Differential Cut Elimination. *Log. Meth. Comput. Sci.* 8, 4 (2012), 1–38. https://doi.org/10.2168/LMCS-8(4:16)2012

[32] André Platzer. 2017. A Complete Uniform Substitution Calculus for Differential Dynamic Logic. *J. Autom. Reasoning* 59, 2 (2017), 219–265. https://doi.org/10.1007/s10817-016-9385-1

[33] André Platzer and Yong Kiam Tan. 2018. Differential Equation Axiomatization: The Impressive Power of Differential Ghosts. In *LICS*, Anuj Dawar and Erich Grädel (Eds.). ACM, New York, 819–828. https://doi.org/10.1145/3209108.3209147

[34] Henri Poincaré. 1881. Mémoire sur les courbes définies par une équation différentielle. *J. Math. Pures Appl.* (1881).

[35] Stephen Prajna and Ali Jadbabaie. 2004. Safety Verification of Hybrid Systems Using Barrier Certificates. In *HSCC (LNCS)*, Rajeev Alur and George J. Pappas (Eds.), Vol. 2993. Springer, Heidelberg, 477–492. https://doi.org/10.1007/978-3-540-24743-2_32

[36] Daniel Richardson. 1968. Some Undecidable Problems Involving Elementary Functions of a Real Variable. *J. Symb. Log.* 33, 4 (1968), 514–520. https://doi.org/10.2307/2271358

[37] Sriram Sankaranarayanan, Henny B. Sipma, and Zohar Manna. 2008. Constructing Invariants for Hybrid Systems. *Form. Methods Syst. Des.* 32, 1 (2008), 25–55. https://doi.org/10.1007/s10703-007-0046-1

[38] Patrick Speissegger. 1999. The Pfaffian Closure of an O-Minimal Structure. *J. Reine Angew. Math.* 508 (1999), 189–211. https://doi.org/10.1515/crll.1999.026

[39] Ankur Taly and Ashish Tiwari. 2009. Deductive Verification of Continuous Dynamical Systems. In *FSTTCS (LIPIcs)*, Ravi Kannan and K. Narayan Kumar (Eds.), Vol. 4. Schloss Dagstuhl, Dagstuhl, 383–394. https://doi.org/10.4230/LIPIcs.FSTTCS.2009.2334

[40] Giuseppina Terzo. 2007. *Consequences of Schanuel's Conjecture in Exponential Algebra*. Ph.D. Dissertation. University of Naples Federico II.

[41] Jean-Claude Tougeron. 1991. Algèbres analytiques topologiquement noethériennes. Théorie de Khovanskiĭ. *Ann. I. Fourier* 41, 4 (1991), 823–840. https://doi.org/10.5802/aif.1275

[42] Lou van den Dries. 1984. Remarks on Tarski's Problem Concerning (R, +, *, exp). In *Logic Colloquium '82*, Gabriele Lolli, Giuseppe Longo, and Annalisa Marcja (Eds.). Vol. 112. North-Holland, Amsterdam, 97–121. https://doi.org/10.1016/S0049-237X(08)71811-1

[43] Lou van den Dries. 1998. *Tame Topology and O-Minimal Structures*. Cambridge University Press, Cambridge. https://doi.org/10.1017/CBO9780511525919

[44] Wolfgang Walter. 1998. *Ordinary Differential Equations*. Springer, New York. https://doi.org/10.1007/978-1-4612-0601-9

[45] Alex J. Wilkie. 1999. A Theorem of the Complement and Some New O-Minimal Structures. *Sel. Math. New Ser.* 5, 4 (1999), 397–421. https://doi.org/10.1007/s000290050052

# A  DIFFERENTIAL DYNAMIC LOGIC AXIOMATIZATION

## A.1  Extended Axiomatization Soundness

This section proves the soundness of the axiomatic extension from Section 5. For the solution $\varphi : [0, T] \to \mathbb{S}$, its truncation to the interval $[0, t]$ for some $0 \le t \le T$ is denoted $\varphi|_t : [0, t] \to \mathbb{S}$, with $\varphi|_t(\zeta) = \varphi(\zeta)$ for $\zeta \in [0, t]$. The shorthand notation $\varphi([a, b]) \in [\![P]\!]$ means $\varphi(\zeta) \in [\![P]\!]$ for all $a \le \zeta \le b$, where the interval $[a, b]$ is required to be a closed subinterval of the interval $[0, T]$. Analogously, $\varphi((a, b))$ is used when the interval is open, and similarly for the half-open cases.

As explained in Section 5, the soundness of the extended axioms requires that the ODE system $x' = f(x)$ always locally evolves $x$. An easy syntactic check ensuring this condition is if the system already contains an equation $x_1' = 1$ that tracks the passage of time, which can be added using axiom DG if necessary before using the axioms. However, the soundness proofs are more general and only use the assumption that the ODE system locally evolves $x$, whether by $x_1' = 1$ or otherwise.

The soundness proofs make use of dL's coincidence lemmas [32, Lemmas 10,11]:

LEMMA A.1 (COINCIDENCE FOR TERMS AND FORMULAS [32]). *The following coincidence properties hold for* dL, *where free variables FV(e), FV(φ) are defined as expected [32, Sections 2.3 and 2.4].*

- *If the states $\omega$, $\nu$ agree on the free variables of term e (FV(e)), then $\omega[\![e]\!] = \nu[\![e]\!]$.*
- *If the states $\omega$, $\nu$ agree on the free variables of formula $\phi$ (FV(φ)), then $\omega \in [\![\phi]\!]$ iff $\nu \in [\![\phi]\!]$.*

*A.1.1  Existence, Uniqueness, and Continuity.* First, the axioms from Lemma 5.1 internalizing basic existence and uniqueness properties of solutions of differential equations are proved sound.

PROOF OF LEMMA 5.1. Let $\omega$ be an arbitrary initial state. When interpreted as a function of the variables $x$, the RHS $f(x)$ of the ODE system $x' = f(x)$ is continuously differentiable. Therefore, by the Picard-Lindelöf theorem [44, §10.VI], from $\omega$, there is an interval $[0, \tau), \tau > 0$ on which there is a unique, continuous solution $\varphi : [0, \tau) \to \mathbb{S}$ with $\varphi(0) = \omega$ on $\{x'\}^\complement$. The solution may be uniquely extended in time (to the right), up to its maximal open interval of existence [44, §10.IX].

**Uniq**  The "$\to$" direction follows directly from monotonicity of domain constraints because of the propositional tautology $Q_1 \wedge Q_2 \to Q_1$ (and similarly for $Q_2$). For the "$\leftarrow$" direction, suppose that initial state $\omega$ satisfies both conjuncts with $\omega \in [\![\langle x' = f(x) \& Q_1 \rangle P]\!]$ and $\omega \in [\![\langle x' = f(x) \& Q_2 \rangle P]\!]$. Expanding the definition of the diamond modality, there exist two solutions $\varphi_1 : [0, T_1] \to \mathbb{S}$, $\varphi_2 : [0, T_2] \to \mathbb{S}$ from $\omega$ such that $\varphi_1 \models x' = f(x) \wedge Q_1$ and $\varphi_2 \models x' = f(x) \wedge Q_2$, with both $\varphi_1(T_1) \in [\![P]\!]$ and $\varphi_2(T_2) \in [\![P]\!]$. Suppose $T_1 \leq T_2$. Since $\varphi_2([0, T_2]) \in [\![Q_2]\!]$ and, by uniqueness, $\varphi_1$ is a truncation of $\varphi_2$ to a smaller existence interval, $\varphi_1 \models x' = f(x) \wedge (Q_1 \wedge Q_2)$. At time $T_1$, the solution satisfies $\varphi_1(T_1) \in [\![P]\!]$, so $\omega \in [\![\langle x' = f(x) \& Q_1 \wedge Q_2 \rangle P]\!]$, as required. The case for $T_2 < T_1$ is similar, except with $\varphi_2 \models x' = f(x) \wedge (Q_1 \wedge Q_2)$ and satisfying $\varphi_2(T_2) \in [\![P]\!]$ at time $T_2$ instead.

**Cont**  Assume that $\omega$ satisfies the outermost implication, i.e., $\omega \in [\![x = y]\!]$. The (inner) "$\to$" direction follows by definition because in order for there to be a solution staying in $e > 0$ at all, the initial state $\omega$ must already satisfy $e > 0$ (evolution domains are differential-free). For the (inner) "$\leftarrow$" direction, suppose further that $\omega \in [\![e > 0]\!]$. Since $x' \notin e$ as $e$ is differential-free (Section 2.1), coincidence (Lemma A.1) implies $\varphi(0) \in [\![e > 0]\!]$. As a composition of continuous evaluation [32, Definition 5] with the continuous solution $\varphi$, $\varphi(t)[\![e]\!]$ is a continuous function of time $t$. Thus, $\varphi(0) \in [\![e > 0]\!]$ implies $\varphi([0, T]) \in [\![e > 0]\!]$ for some $0 < T \leq \tau$ and the truncated solution $\varphi|_T$ satisfies $\varphi|_T \models x' = f(x) \wedge e > 0$. Since $y$ is constant for the ODE but $x' = f(x)$ was assumed to locally evolve (for example with $x_1' = 1$), there is a time $0 < \epsilon \leq T$ at which $\varphi(\epsilon) \in [\![x \neq y]\!]$. The truncation $\varphi|_\epsilon$ witnesses $\omega \in [\![\langle x' = f(x) \& e > 0 \rangle x \neq y]\!]$.

**Dadj**  The "$\leftarrow$" direction follows immediately from the "$\to$" direction by swapping the names $x, y$, because $-(-f(x)) = f(x)$. Therefore, it suffices to prove the "$\to$" direction. Suppose $\omega \in [\![\langle x' = f(x) \& Q(x) \rangle x = y]\!]$. Unfolding the semantics, there is a solution $\varphi : [0, T] \to \mathbb{S}$, of the system $x' = f(x)$, with $\varphi(0) = \omega$ on $\{x'\}^\complement$, with $\varphi([0, T]) \in [\![Q(x)]\!]$ and $\varphi(T) \in [\![x = y]\!]$. Since the variables $y$ do not appear in the differential equations $x' = f(x)$, their values are constant along the solution $\varphi$. Consider the time- and variable-reversal $\psi : [0, T] \to \mathbb{S}$, where:

$$\psi(\tau)(z) \stackrel{\text{def}}{=} \begin{cases} \varphi(T - \tau)(x_i) & z = y_i \\ -\varphi(T - \tau)(x_i') & z = y_i' \\ \omega(z) & \text{otherwise} \end{cases}$$

By construction, $\psi(0)$ agrees with $\omega$ on $\{y'\}^\complement$ because $\varphi(T) \in [\![x = y]\!]$. The signs of the differential variables $y_i'$ are negated along $\psi$. By uniqueness, the solutions of $x' = -f(x)$ are the time-reversed solutions of $x' = f(x)$. As constructed, $\psi$ is the time-reversed solution for

$x' = f(x)$ except the $x$ were replaced by $y$ instead. Moreover, since $\varphi([0, T]) \in [\![Q(x)]\!]$, by construction and coincidence (Lemma A.1), $\psi([0, T]) \in [\![Q(y)]\!]$. Therefore, $\psi \models y' = -f(y) \wedge Q(y)$. Finally, observe that $\psi(T)(y) = \varphi(0)(x)$, but $\psi$ holds the values of $x$ constant, thus $\psi(T)(x) = \omega(x) = \varphi(0)(x)$ and so $\psi(T) \in [\![y = x]\!]$ and $\psi$ witnesses $\omega \in [\![\langle y' = -f(y) \& Q(y)\rangle y = x]\!]$    □

*A.1.2   Real Induction.* The following real induction axiom with domain constraints is proved sound. Axiom RI from Lemma 5.5 follows as an instance with no domain constraint, i.e., $Q \equiv true$.

RI&  $[x' = f(x) \& Q]P \leftrightarrow \forall y\, [x' = f(x) \& Q \wedge (P \vee x = y)]\Big( x = y \rightarrow$

$$\underbrace{P}_{\textcircled{a}} \wedge \underbrace{\left( \langle x' = f(x) \& Q \vee x = y\rangle x \neq y \rightarrow \langle x' = f(x) \& P \vee x = y\rangle x \neq y \right)}_{\textcircled{b}} \Big)$$

Similar to axiom RI, the axiom RI& is based on the real induction principle [7] but also accounts for an arbitrary domain constraint $Q$. Its RHS conjuncts labeled ⓐ and ⓑ correspond to ① and ② in Def. 5.3 respectively. The quantification $\forall y\, [\ldots \& Q](x = y \rightarrow \ldots)$ now only considers final states ($x = y$) reachable by trajectories that *always* stay within $Q$, and within $P$ except possibly at the endpoint $x = y$. The conjunct ⓐ expresses that $P$ is still true at such an endpoint. The conjunct ⓑ expresses that $P$ continues to remain true locally but only when $Q$ itself remains true locally. This added assumption for $Q$ corresponds to the "If $\zeta < b$ then . . . " assumption in ② of Def. 5.3. The conjunct ⓑ can be rewritten succinctly with the local progress ◯ modality as:

$$\langle x' = f(x) \& Q\rangle \bigcirc \rightarrow \langle x' = f(x) \& P\rangle \bigcirc$$

With completeness for local progress (Theorem 6.6), this gives a first hint at how RI& will be used to obtain a complete proof rule for semianalytic invariants with domain constraints in Appendix B.

LEMMA A.2 (REAL INDUCTION WITH DOMAIN CONSTRAINTS). *The real induction axiom RI& is sound, where $y$ is fresh in $[x' = f(x) \& Q]P$.*

PROOF (IMPLIES LEMMA 5.5). The conjuncts on the RHS of RI& are labeled as ⓐ and ⓑ respectively, as shown above. Consider an initial state $\omega$, both directions of the axiom are proved separately.

"$\rightarrow$" Assume the LHS of RI& is true initially with ⍟ $\omega \in [\![[x' = f(x) \& Q]P]\!]$. Unfolding the quantification and box modality on the RHS, let $\omega_y$ be identical to $\omega$ except where the values for $y$ are replaced with any arbitrary values $d \in \mathbb{R}^n$. Consider any solution $\varphi_y : [0, T] \rightarrow \mathbb{S}$ where $\varphi_y \models x' = f(x) \wedge (Q \wedge (P \vee x = y))$, $\varphi_y(0) = \omega_y$ on $\{x'\}^{\complement}$, and $\varphi_y(T) \in [\![x = y]\!]$. The following similar solution $\varphi : [0, T] \rightarrow \mathbb{S}$ keeps $y$ constant at their initial values in $\omega$:

$$\varphi(t)(z) \stackrel{\text{def}}{=} \begin{cases} \varphi_y(t)(z) & z \in \{y\}^{\complement} \\ \omega(z) & z \in \{y\} \end{cases}$$

By construction, $\varphi(0)$ is identical to $\omega$ on $\{x'\}^{\complement}$ and $\varphi$ is identical to $\varphi_y$ on $\{y\}^{\complement}$. Since $y$ is fresh in $x' = f(x) \& Q$, by coincidence (Lemma A.1) the latter implies that $\varphi \models x' = f(x) \wedge Q$. By assumption ⍟, $\varphi(T) \in [\![P]\!]$, which implies that $\varphi_y(T) \in [\![P]\!]$ by coincidence (Lemma A.1) since $y$ is fresh in $P$. This proves conjunct ⓐ. Unfolding the implication and diamond modality of conjunct ⓑ, assume there is another solution $\psi_y : [0, \tau] \rightarrow \mathbb{S}$ from $\varphi_y(T)$ with $\psi_y \models x' = f(x) \wedge (Q \vee x = y)$ and $\psi_y(\tau) \in [\![x \neq y]\!]$. Note that $\psi_y(0) = \varphi_y(T)$ *exactly* rather than just on $\{x'\}^{\complement}$, because both states have the same values for the differential variables. To show the RHS of the implication in ⓑ, i.e., that $\varphi_y(T) \in [\![\langle x' = f(x) \& P \vee x = y\rangle x \neq y]\!]$, it suffices to show: $\psi_y \models x' = f(x) \wedge P$, because $P$ propositionally implies $P \vee x = y$. In particular, since $\psi_y$ already satisfies the requisite differential equations and $\psi_y(\tau) \in [\![x \neq y]\!]$, it remains

to show that $\psi_y$ stays in the evolution domain $P$ for its entire duration, i.e., $\psi_y([0, \tau]) \in [\![P]\!]$. Let $0 \leq \zeta \leq \tau$ and consider the concatenated solution $\Phi : [0, T + \zeta] \to \mathbb{S}$ defined by:

$$\Phi(t)(z) \stackrel{\text{def}}{=} \begin{cases} \varphi_y(t)(z) & t \leq T, z \in \{y\}^{\complement} \\ \psi_y(t - T)(z) & t > T, z \in \{y\}^{\complement} \\ \omega(z) & z \in \{y\} \end{cases}$$

As with $\varphi$, the solution $\Phi$ is constructed to keep $y$ constant at their initial values in $\omega$. Since $\psi_y$ must uniquely extend $\varphi_y$ [44, §10.IX], the concatenated solution $\Phi$ is a solution starting from $\omega$, solving the system $x' = f(x)$. It stays in $Q$ for its entire duration by coincidence (Lemma A.1) because $\varphi_y(T) \in [\![Q]\!]$ and all states satisfying $x = y$ agree with $\varphi_y(T)$ on the free variables of formula $Q$. In other words, $\Phi \models x' = f(x) \wedge Q$. By ⊛, $\Phi(T + \zeta) \in [\![P]\!]$, which implies $\psi(\zeta) \in [\![P]\!]$ by coincidence (Lemma A.1) and so $\psi_y([0, \zeta]) \in [\![P]\!]$, as required.

"←" Assume the RHS of RI& is true in initial state $\omega$ and show the LHS. Consider an arbitrary solution $\varphi : [0, T] \to \mathbb{S}$ starting from $\omega$ such that $\varphi \models x' = f(x) \wedge Q$. To show $\varphi([0, T]) \in [\![P]\!]$, using the real induction principle (Proposition 5.4), it suffices to show that the set of times $S \stackrel{\text{def}}{=} \{\zeta : \varphi(\zeta) \in [\![P]\!]\}$ is an inductive subset of $[0, T]$, i.e., it satisfies properties ① and ② in Def. 5.3. So, assume that $[0, \zeta) \subseteq S$ for some time $0 \leq \zeta \leq T$.

The proof instantiates quantified variables $y$ on the RHS of RI& to match the values of $x$ at $\varphi(\zeta)$. Since $y$ is constant for the ODE, this allows properties of $\varphi(\zeta)$ to be deduced using the RHS (namely ⓐ, ⓑ) by mediating between $\varphi$ and its augmentation $\varphi_y$ below. More precisely, consider the state $\omega_y$ identical to $\omega$, except where the values for variables $y$ are replaced with the corresponding values of $x$ in $\varphi(\zeta)$. Correspondingly, consider the solution $\varphi_y : [0, \zeta] \to \mathbb{S}$ identical to $\varphi$ but which keeps $y$ constant at those initial values in $\omega_y$ rather than in $\omega$:

$$\omega_y(z) \stackrel{\text{def}}{=} \begin{cases} \omega(z) & z \in \{y\}^{\complement} \\ \varphi(\zeta)(x_i) & z = y_i \end{cases} \qquad \varphi_y(t)(z) \stackrel{\text{def}}{=} \begin{cases} \varphi(t)(z) & z \in \{y\}^{\complement} \\ \omega_y(z) & z \in \{y\} \end{cases}$$

By construction and coincidence (Lemma A.1), $\varphi_y$ is a solution from initial state $\omega_y$, solving $\varphi_y \models x' = f(x) \wedge Q$ and $\varphi_y(\zeta) \in [\![x = y]\!]$. By assumption and coincidence (Lemma A.1), $\varphi_y([0, \zeta)) \in [\![P]\!]$. Therefore, $\varphi_y([0, \zeta]) \in [\![Q \wedge (P \vee x = y)]\!]$. Unfolding the quantification, box modality and implication on the RHS yields $\varphi_y(\zeta) \in [\![ⓐ \wedge ⓑ]\!]$.

① By ⓐ, $\varphi_y(\zeta) \in [\![P]\!]$ so by coincidence (Lemma A.1), $\varphi(\zeta) \in [\![P]\!]$ as required for ①.

② Further assume that $\zeta < T$ and show $\varphi((\zeta, \zeta + \epsilon]) \in [\![P]\!]$ for some $\epsilon > 0$. Observe that since $\zeta < T$, there is a solution that extends from state $\varphi(\zeta)$, i.e., $\psi : [0, T - \zeta] \to \mathbb{S}$, where $\psi(\tau) \stackrel{\text{def}}{=} \varphi(\tau + \zeta)$ and with $\psi \models x' = f(x) \wedge Q$. Construct the corresponding solution $\psi_y : [0, T - \zeta] \to \mathbb{S}$ that extends from state $\varphi_y(\zeta)$ and still keeps $y$ constant at $\omega_y$:

$$\psi_y(t)(z) \stackrel{\text{def}}{=} \begin{cases} \psi(t)(z) & z \in \{y\}^{\complement} \\ \varphi_y(\zeta)(z) & z \in \{y\} \end{cases}$$

By coincidence (Lemma A.1), $\psi_y \models x' = f(x) \wedge Q$, so by weakening the domain constraint, $\psi_y \models x' = f(x) \wedge (Q \vee x = y)$. Since $\varphi_y(\zeta) \in [\![x = y]\!]$ by construction and the differential equation is assumed to always locally evolve (for example with $x'_1 = 1$), there must be some duration $0 < \delta < T - \zeta$ (recall $T - \zeta > 0$) after which the value of $x$ has changed from its initial value held constant in $y$, i.e., $\psi_y(\delta) \in [\![x \neq y]\!]$. The truncation $\psi_y|_\delta$ witnesses the LHS of the implication in ⓑ with: $\varphi_y(\zeta) \in [\![\langle x' = f(x) \& Q \vee x = y \rangle x \neq y]\!]$. Using this with the implication in ⓑ yields $\varphi_y(\zeta) \in [\![\langle x' = f(x) \& P \vee x = y \rangle x \neq y]\!]$. Unfolding the semantics, this gives a solution which, by uniqueness, is a truncation $\psi_y|_\epsilon$ of $\psi_y$, for some $\epsilon > 0$,

that satisfies $\psi_y|_\epsilon([0,\epsilon)) \in [\![P \vee x = y]\!]$. From ⓐ and coincidence (Lemma A.1), all states satisfying $x = y$ agree with $\varphi(\zeta)$ on the free variables of formula $P$ thus $\psi_y|_\epsilon([0,\epsilon)) \in [\![P]\!]$. By construction, $\psi_y|_\epsilon(\tau)$ coincides with $\varphi(\tau + \zeta)$ on $x$ for all $0 \leq \tau \leq \epsilon$, which implies $\varphi((\zeta, \zeta + \epsilon)) \in [\![P]\!]$ by Lemma A.1. □

Conjunct ⓑ of RI& can also be written as $\langle x' = f(x) \& Q\rangle x \neq y \rightarrow \langle x' = f(x) \& P\rangle x \neq y$ because $Q$ and $P$ can be assumed true in the context where the conjunct appears. This flexibility can be seen from its soundness proof above and will be made explicit syntactically in Corollary A.5.

## A.2 Derived Rules and Axioms

This section derives additional dL axioms and proof rules that are used in subsequent derivations in the appendices. Most of these are already derived elsewhere [29, 32] so their proofs are omitted.

*A.2.1 Basic Rules and Axioms.* This section presents basic dL axioms and proof rules and derived versions that do not rely on the axiomatic extension of Section 5 but are used in the appendices.

THEOREM A.3 (BASE AXIOMS AND PROOF RULES [29, 32]). *The following are sound axioms and proof rules of* dL.

$\langle\cdot\rangle \quad \langle\alpha\rangle\phi \leftrightarrow \neg[\alpha]\neg\phi \qquad\qquad\qquad G \quad \dfrac{\vdash \phi}{\Gamma \vdash [\alpha]\phi}$

$K \quad [\alpha](\phi \rightarrow \psi) \rightarrow ([\alpha]\phi \rightarrow [\alpha]\psi) \qquad V \quad \phi \rightarrow [\alpha]\phi \quad$ (no free variable of $\phi$ is bound by $\alpha$)

$B' \quad \langle x' = f(x) \& Q(x)\rangle \exists y P(x,y) \leftrightarrow \exists y \langle x' = f(x) \& Q(x)\rangle P(x,y) \quad (y \notin x)$

$DW \quad [x' = f(x) \& Q]Q$

$DX \quad [x' = f(x) \& Q]P \leftrightarrow (Q \rightarrow P \wedge [x' = f(x) \& Q]P) \qquad\qquad (x' \notin P, Q)$

$DMP \quad [x' = f(x) \& Q](Q \rightarrow R) \rightarrow ([x' = f(x) \& R]P \rightarrow [x' = f(x) \& Q]P)$

The first three axioms $\langle\cdot\rangle$, K, V and proof rule G are standard reasoning principles for dynamic logics [29]. They apply generally for any hybrid program $\alpha$. Axiom $\langle\cdot\rangle$ expresses the duality between the diamond and box modalities, allowing conversion between the two with a double negation. Kripke axiom K is the modal modus ponens for postconditions of the box modality. Vacuous axiom V says if no free variable of $\phi$ is changed by hybrid program $\alpha$, then the truth value of $\phi$ is also unchanged. The Gödel generalization rule G reduces proofs of $[\alpha]\phi$ to validity of $\phi$ but must discard all assumptions in antecedent $\Gamma$ for soundness.

The ODE Barcan axiom $B'$ specializes the Barcan axiom [29] to ODEs in the diamond modality, allowing an existential quantifier $\exists y$ to be commuted with the diamond modality. The quantified variables $y$ are required to be fresh in the ODE $x' = f(x)$ (i.e., $y \notin x$). The *differential weakening* axiom DW expresses that domain constraints are always obeyed along ODE solutions. It underlies the derived proof rules dW, M['], which ease manipulation of domain constraints. The *differential skip* axiom DX expresses a reflexivity property of differential equation solutions. If domain constraint $Q$ is false in an initial state $\omega$, then the formula $[x' = f(x) \& Q]P$ is trivially true in $\omega$ because no solution of the ODE starting from $\omega$ stays in the domain constraint. Conversely, if $Q$ is true in $\omega$, then the postcondition $P$ must already be true in $\omega$ because of the trivial solution of duration zero. The condition $x' \notin P, Q$ of axiom DX is met as $P, Q$ are differential-free (Section 2.1). Axiom DMP is the modus ponens principle for domain constraints of ODEs which underlies differential cuts DC [32].

PROOF OF THEOREM A.3. The soundness of all axioms and proof rules in Theorem A.3 are proved elsewhere [32], except DX, DMP, which are proved here since they are written differently elsewhere.

**DX** Let $\omega$ be an initial state. Classically, either $\omega \in [\![Q]\!]$ or not. If $\omega \in [\![Q]\!]$, then, propositionally, it suffices to assume $\omega \in [\![[x' = f(x) \& Q]P]\!]$ and show $\omega \in [\![P]\!]$. Since $\omega \in [\![Q]\!]$, there is a trivial solution $\varphi : [0, 0] \to \mathbb{S}$ where $\varphi \models x' = f(x) \wedge Q$ and $\varphi(0) = \omega$ on $\{x'\}^\complement$. By assumption, $\varphi(0) \in [\![P]\!]$. Since $x' \notin P$, coincidence (Lemma A.1) implies $\omega \in [\![P]\!]$. Conversely, if $\omega \in [\![\neg Q]\!]$, then, propositionally, it suffices to show $\omega \in [\![[x' = f(x) \& Q]P]\!]$. The box modality is vacuous because, by definition, no solution $\varphi : [0, T] \to \mathbb{S}$ can exist for any $T \geq 0$ with $\varphi \models x' = f(x) \wedge Q$. Any such solution would require $\varphi(0) \in [\![Q]\!]$ by definition. However, because $x' \notin Q$, coincidence (Lemma A.1) with state $\omega$ gives $\omega \in [\![Q]\!]$, contradiction.

**DMP** Let $\omega$ be an initial state satisfying both formulas on the left of the implications in DMP, i.e., ① $\omega \in [\![[x' = f(x) \& Q](Q \to R)]\!]$ and ② $\omega \in [\![[x' = f(x) \& R]P]\!]$. Consider any solution $\varphi : [0, T] \to \mathbb{S}$ where $\varphi(0) = \omega$ on $\{x'\}^\complement$, and $\varphi \models x' = f(x) \wedge Q$. By definition, $\varphi(\zeta) \in [\![Q]\!]$ for all $\zeta \in [0, T]$, and so by ①, $\varphi(\zeta) \in [\![Q \to R]\!]$ for all $\zeta \in [0, T]$. Therefore, $\varphi(\zeta) \in [\![R]\!]$ for all $\zeta \in [0, T]$, and thus $\varphi \models x' = f(x) \wedge R$. By ②, $\varphi(T) \in [\![P]\!]$ as required. □

The axioms and proof rules of Theorem A.3 combine to derive further useful axioms and proof rules. Diamond Kripke axiom K⟨·⟩ derives from K by dualizing its inner implication with ⟨·⟩ [29].

$$\text{K}\langle\cdot\rangle \quad [\alpha](\phi \to \psi) \to (\langle\alpha\rangle\phi \to \langle\alpha\rangle\psi)$$

Axiom ⟨·⟩ also yields dual readings for the ODE axioms and proof rules. For example, the $\text{DI}_\geqslant$ axiom internalizes the mean value theorem [44, Appendix B.I].

COROLLARY A.4 (MEAN VALUE THEOREM). *The mean value theorem axiom MVT derives from $DI_\geqslant$:*

$$\text{MVT} \quad e \geq 0 \wedge \langle x' = f(x) \& Q\rangle e < 0 \to \langle x' = f(x) \& Q\rangle(e)' < 0$$

PROOF. The derivation takes contrapositives (dualizing with ⟨·⟩) before $\text{DI}_\geqslant$ finishes it.

$$\frac{\begin{array}{c}*\\ \hline e \geq 0, [x' = f(x) \& Q](e)' \geq 0 \vdash [x' = f(x) \& Q]e \geq 0\end{array}}{e \geq 0, \langle x' = f(x) \& Q\rangle e < 0 \vdash \langle x' = f(x) \& Q\rangle(e)' < 0} \begin{array}{l}\text{DI}_\geqslant\\ \langle\cdot\rangle, \neg\text{L}, \neg\text{R}\end{array}$$

□

Axiom V is particularly useful when working with *constant assumptions*. If formula $R(y)$ is true initially and $y$ has no differential equation in $x' = f(x)$, then it continues to be true along solutions to the differential equations from the initial state because $y$ remains constant along these solutions and the truth value of $R(y)$ depends only on the value of its free variables $y$ [32]. Axiom V proves this for box modalities in succedents and, by duality, for diamond modalities in antecedents, e.g.:

$$\frac{\begin{array}{c}*\\ \hline R(y) \vdash [x' = f(x) \& Q]R(y)\end{array} \qquad \Gamma \vdash [x' = f(x) \& Q \wedge R(y)]P}{\Gamma, R(y) \vdash [x' = f(x) \& Q]P} \begin{array}{l}\text{V}\\ \text{DC}\end{array}$$

Conversely, if a constant assumption $R(y)$ is true in a final state reachable by an ODE $x' = f(x)$, then it must already be true initially. This is shown formally by the derivation below which uses a classical case split with a cut on whether the formula $R(y)$ is already true initially:

$$\frac{\frac{\begin{array}{c}*\\ \hline \Gamma, R(y), \langle x' = f(x) \& Q\rangle(P \wedge R(y)) \vdash R(y)\end{array} \qquad \Gamma, \neg R(y), \langle x' = f(x) \& Q\rangle(P \wedge R(y)) \vdash R(y)}{\Gamma, R(y) \vee \neg R(y), \langle x' = f(x) \& Q\rangle(P \wedge R(y)) \vdash R(y)}}{\Gamma, \langle x' = f(x) \& Q\rangle(P \wedge R(y)) \vdash R(y)} \begin{array}{l}\vee\text{L}\\ \text{cut}\end{array}$$

The left premise closes trivially. For the right premise, a contradiction is derived with $\langle \cdot \rangle$ as follows, where the V, M['] step uses the propositional tautology $\neg R(y) \rightarrow \neg(P \wedge R(y))$:

$$
\begin{array}{c}
\text{V, M[']} \dfrac{*}{\neg R(y) \vdash [x' = f(x) \& Q]\neg(P \wedge R(y))} \\[4pt]
\langle \cdot \rangle, \neg\text{L} \dfrac{}{\neg R(y), \langle x' = f(x) \& Q \rangle(P \wedge R(y)) \vdash \mathit{false}}
\end{array}
$$

In the sequel, these routine steps are omitted and proof steps manipulating constant assumptions are simply labeled with V directly.

Axiom DMP derives the diamond refinement axiom DR$\langle \cdot \rangle$ and its corollary dRW$\langle \cdot \rangle$ from Corollary 5.2, which provide tools for working with ODE domain constraints in the diamond modality:

Proof of Corollary 5.2. Axiom DR$\langle \cdot \rangle$ derives from DMP (the roles of $Q$ and $R$ are flipped) by dualizing with the $\langle \cdot \rangle$ axiom. The last K, dW step uses the propositional tautology $Q \rightarrow (R \rightarrow Q)$.

$$
\begin{array}{c}
\text{K, dW} \dfrac{*}{[x' = f(x) \& R]Q \vdash [x' = f(x) \& R](R \rightarrow Q)} \\[4pt]
\text{DMP} \dfrac{[x' = f(x) \& R]Q, [x' = f(x) \& Q]\neg P \vdash [x' = f(x) \& R]\neg P}{} \\[4pt]
\langle \cdot \rangle, \neg\text{R}, \neg\text{L} \dfrac{}{[x' = f(x) \& R]Q, \langle x' = f(x) \& R \rangle P \vdash \langle x' = f(x) \& Q \rangle P}
\end{array}
$$

Rule dRW$\langle \cdot \rangle$ derives from DR$\langle \cdot \rangle$ by simplifying its left premise with rule dW.                    □

*A.2.2 Extended Derived Rules and Axioms.* This section derives additional rules and axioms that make use of the axiomatic extensions from Section 5.

*Local Progress Properties.* The local progress modality $\bigcirc$ excludes the initial state $(x = y)$ in the domain constraint when expressing local progress for formula $Q$. Recall:

$$
\langle x' = f(x) \& Q \rangle \bigcirc \; \overset{\text{def}}{\equiv} \; \langle x' = f(x) \& Q \vee x = y \rangle \, x \neq y
$$

The disjunct $x = y$ in the domain constraint makes local progress an interesting question for formulas characterizing sets that are not topologically closed (e.g., open sets as characterized by the formula $e > 0$). As axiom Cont shows, the formula $\langle x' = f(x) \& e > 0 \rangle x \neq y$ which *does not* exclude $x = y$ in the evolution domain constraint is already *equivalent* to $e > 0$. A precise syntactic characterization of this difference is shown by the following derived axiom:

Corollary A.5 (Initial state inclusion). *The following axiom derives in* dL. *Variables $y$ are fresh in the ODE $x' = f(x)$ and formula $Q$.*

$$
\text{Init} \quad x{=}y \rightarrow \big( \langle x' = f(x) \& Q \rangle x \neq y \leftrightarrow Q \wedge \langle x' = f(x) \& Q \rangle \bigcirc \big)
$$

Proof. First, by dualizing via $\langle \cdot \rangle$ both sides of axiom DX, the following equivalence is derived:

$$
\langle x' = f(x) \& Q \rangle P \leftrightarrow (Q \wedge (P \vee \langle x' = f(x) \& Q \rangle P))
$$

The derivation of Init starts by using this derived equivalence (DX, $\langle \cdot \rangle$), followed by a series of equivalent propositional rewrites that simplify the logical structure of the succedent. The propositional steps are shown below, first removing the disjunct $x \neq y$ using the assumption $x{=}y$, and then pulling out the common conjunct $Q$ as an antecedent assumption.

$$
\begin{array}{c}
\dfrac{x{=}y, Q \vdash \langle x' = f(x) \& Q \rangle x \neq y \leftrightarrow \langle x' = f(x) \& Q \rangle \bigcirc}{} \\[4pt]
\dfrac{x{=}y \vdash Q \wedge \langle x' = f(x) \& Q \rangle x \neq y \leftrightarrow Q \wedge \langle x' = f(x) \& Q \rangle \bigcirc}{} \\[4pt]
\dfrac{x{=}y \vdash Q \wedge (x \neq y \vee \langle x' = f(x) \& Q \rangle x \neq y) \leftrightarrow Q \wedge \langle x' = f(x) \& Q \rangle \bigcirc}{} \\[4pt]
\text{DX}, \langle \cdot \rangle \dfrac{}{x{=}y \vdash \langle x' = f(x) \& Q \rangle x \neq y \leftrightarrow Q \wedge \langle x' = f(x) \& Q \rangle \bigcirc}
\end{array}
$$

Both directions of the resulting equivalence are proved separately by unfolding the abbreviation ◯. In the "→" direction, a dRW⟨·⟩ step suffices, because $Q → Q ∨ x{=}y$ is a propositional tautology:

$$
\text{dRW}⟨·⟩\frac{*}{x{=}y, Q, ⟨x' = f(x) \& Q⟩x ≠ y ⊢ ⟨x' = f(x) \& Q ∨ x{=}y⟩x ≠ y}
$$

In the "←" direction, the derivation starts with a DR⟨·⟩ step which reduces to the box modality. Since the formulas $x = y$ and $Q$ are true initially, a V, DC step introduces the constant assumption $Q(y)$ into the domain constraint, which is $Q$ with $y$ in place of $x$. The derivation closes with dW.

$$
\begin{array}{l}
\text{dW}\dfrac{*}{⊢ [x' = f(x) \& (Q ∨ x{=}y) ∧ Q(y)]Q} \\[2pt]
\text{V, DC}\dfrac{}{x{=}y, Q ⊢ [x' = f(x) \& Q ∨ x{=}y]Q} \\[2pt]
\text{DR}⟨·⟩\dfrac{}{x{=}y, Q, ⟨x' = f(x) \& Q ∨ x{=}y⟩x ≠ y ⊢ ⟨x' = f(x) \& Q⟩x ≠ y} \qquad \square
\end{array}
$$

It is not possible to locally progress into both formula $P$ and its negation $¬P$ simultaneously, by uniqueness. This is the "→" direction of the duality axiom $¬◯$ for local progress from Corollary 6.7. The converse "←" is more involved and relies on the characterization axiom LP later.

COROLLARY A.6 (LOCAL PROGRESS DUALITY "→"). *The following axiom derives from* Uniq. *Variables* $y$ *are fresh in the ODE* $x' = f(x)$ *and formula* $P$.

$$
¬◯_→ \quad x{=}y → \big(⟨x' = f(x) \& P⟩◯ → ¬⟨x' = f(x) \& ¬P⟩◯\big)
$$

PROOF. The derivation starts with $¬R$, after which the resulting local progress antecedents are combined by Uniq, giving a conjunction of their domain constraints because $(P ∨ x{=}y) ∧ (¬P ∨ x{=}y)$ is propositionally equivalent to $(P ∧ ¬P) ∨ x{=}y$. The conjunction $P ∧ ¬P$ in the domain constraint is propositionally equivalent to *false* and no local progress is possible into an empty set of states.

$$
\begin{array}{l}
\text{Uniq}\dfrac{⟨x' = f(x) \& P ∧ ¬P⟩◯ ⊢ \textit{false}}{⟨x' = f(x) \& P⟩◯, ⟨x' = f(x) \& ¬P⟩◯ ⊢ \textit{false}} \\[4pt]
\text{¬R}\dfrac{}{⟨x' = f(x) \& P⟩◯ ⊢ ¬⟨x' = f(x) \& ¬P⟩◯}
\end{array}
$$

The derivation is completed by unfolding the ◯ syntactic abbreviation, and shifting to the box modality by ⟨·⟩ duality. The final step after using dW is a propositional tautology:

$$
\begin{array}{l}
\text{dW}\dfrac{\dfrac{*}{(P ∧ ¬P) ∨ x = y ⊢ x = y}}{⊢ [x' = f(x) \& (P ∧ ¬P) ∨ x = y]x = y} \\[8pt]
⟨·⟩, \text{¬L}\dfrac{⟨x' = f(x) \& (P ∧ ¬P) ∨ x = y⟩x ≠ y ⊢ \textit{false}}{⟨x' = f(x) \& P ∧ ¬P⟩◯ ⊢ \textit{false}} \qquad \square
\end{array}
$$

*Reflection.* The next two derived axioms rfl⟨·⟩ and rfl internalize a mathematical property of ODE invariants. Namely, the formula $P$ is invariant for the forwards ODE $x' = f(x)$ iff its negation $¬P$ is invariant for the backwards ODE $x' = -f(x)$. This invariant reflection principle is used in Appendix B for proving completeness for semianalytic invariants, and to flip the signs in the second premise of rule rI. It is useful in its own right as it allows freely switching between proving invariance for either the forwards or backwards ODEs, e.g., if one direction yields simpler arithmetic.

COROLLARY A.7 (REFLECTION). *The reflection axioms* rfl⟨·⟩, rfl *derive from* Dadj:

rfl⟨·⟩ $\exists x \big(P(x) ∧ ⟨x' = f(x) \& Q(x)⟩R(x)\big) ↔ \exists x \big(R(x) ∧ ⟨x' = -f(x) \& Q(x)⟩P(x)\big)$

rfl $\forall x \big(P(x) → [x' = f(x) \& Q(x)]P(x)\big) ↔ \forall x \big(¬P(x) → [x' = -f(x) \& Q(x)]¬P(x)\big)$

Proof. Axiom rfl derives from rfl⟨·⟩ by instantiating with $R(x) \stackrel{\text{def}}{\equiv} \neg P(x)$ and negating both sides of the equivalence with ⟨·⟩. The diamond reflection axiom rfl⟨·⟩ is derived from Dadj. Both implications are proved separately and the "←" direction follows by instantiating the proof of the "→" direction, since $-(-f(x)) = f(x)$. The "→" direction is proved below.

In the derivation below, the formulas are bound renamed [32] for clarity. After Skolemizing, the first K⟨·⟩, dW step introduces an existentially quantified $y$ under the diamond modality in the antecedent by monotonicity using the provable first-order formula $R(x) \rightarrow \exists y\,(x = y \wedge R(y))$.

$$
\begin{array}{ll}
\text{K}\langle\cdot\rangle,\text{dW} & \dfrac{P(x), \langle x' = f(x) \,\&\, Q(x)\rangle \exists y\,(x = y \wedge R(y)) \vdash \exists y\,(R(y) \wedge \langle y' = -f(y) \,\&\, Q(y)\rangle P(y))}{\dfrac{P(x), \langle x' = f(x) \,\&\, Q(x)\rangle R(x) \vdash \exists y\,(R(y) \wedge \langle y' = -f(y) \,\&\, Q(y)\rangle P(y))}{\exists x\,(P(x) \wedge \langle x' = f(x) \,\&\, Q(x)\rangle R(x)) \vdash \exists y\,(R(y) \wedge \langle y' = -f(y) \,\&\, Q(y)\rangle P(y))}} \\
\exists\text{L}, \wedge\text{L} &
\end{array}
$$

The ODE Barcan B′ axiom moves the existentially quantified $y$ out of the diamond modality since $y$ is not in $x' = f(x)$. A subsequent V step also moves the postcondition $R(y)$ out from the diamond modality into the antecedents.

$$
\begin{array}{ll}
\text{V} & \dfrac{P(x), R(y), \langle x' = f(x) \,\&\, Q(x)\rangle x = y \vdash \exists y\,(R(y) \wedge \langle y' = -f(y) \,\&\, Q(y)\rangle P(y))}{\dfrac{P(x), \langle x' = f(x) \,\&\, Q(x)\rangle(x = y \wedge R(y)) \vdash \exists y\,(R(y) \wedge \langle y' = -f(y) \,\&\, Q(y)\rangle P(y))}{\dfrac{P(x), \exists y\,\langle x' = f(x) \,\&\, Q(x)\rangle(x = y \wedge R(y)) \vdash \exists y\,(R(y) \wedge \langle y' = -f(y) \,\&\, Q(y)\rangle P(y))}{P(x), \langle x' = f(x) \,\&\, Q(x)\rangle \exists y\,(x = y \wedge R(y)) \vdash \exists y\,(R(y) \wedge \langle y' = -f(y) \,\&\, Q(y)\rangle P(y))}}}
\end{array}
$$
$\exists$L , B′

The derivation continues using differential adjoints Dadj to syntactically flip the antecedent differential equations from evolving $x$ forwards to evolving $y$ backwards. The V, K⟨·⟩ step then strengthens the postcondition to $P(y)$ exploiting that the (negated) ODE does not modify $x$ so that $P(x)$ remains true along the ODE. This completes the proof using $y$ as a witness for $\exists y$.

$$
\begin{array}{ll}
\exists\text{R} & \dfrac{*}{\dfrac{R(y), \langle y' = -f(y) \,\&\, Q(y)\rangle P(y) \vdash \exists y\,(R(y) \wedge \langle y' = -f(y) \,\&\, Q(y)\rangle P(y))}{\dfrac{P(x), R(y), \langle y' = -f(y) \,\&\, Q(y)\rangle y = x \vdash \exists y\,(R(y) \wedge \langle y' = -f(y) \,\&\, Q(y)\rangle P(y))}{P(x), R(y), \langle x' = f(x) \,\&\, Q(x)\rangle x = y \vdash \exists y\,(R(y) \wedge \langle y' = -f(y) \,\&\, Q(y)\rangle P(y))}}} \\
\text{V, K}\langle\cdot\rangle & \\
\text{Dadj} & \hspace{9cm} \square
\end{array}
$$

*Real Induction Rule.* The real induction rule with domain constraints corresponding to axiom RI& is derived next. It is stated with the ◯ modality from Section 5. The real induction rule rI from Corollary 5.6 derives as an instance with domain constraint $Q \equiv true$.

Corollary A.8 (Real induction rule with domain constraints). *The real induction proof rule rI& (with two stacked premises) derives from RI&, Dadj, Uniq. Variables $y$ are fresh in the ODE $x' = f(x)$ and formulas $P, Q$.*

$$
\text{rI\&}\ \dfrac{\begin{array}{c} x=y, P, Q, \langle x' = f(x) \,\&\, Q\rangle\bigcirc \vdash \langle x' = f(x) \,\&\, P\rangle\bigcirc \\ x=y, \neg P, Q, \langle x' = -f(x) \,\&\, Q\rangle\bigcirc \vdash \langle x' = -f(x) \,\&\, \neg P\rangle\bigcirc \end{array}}{P \vdash [x' = f(x) \,\&\, Q]P}
$$

Proof (implies Corollary 5.6). The derivation starts by rewriting the succedent with RI&, the resulting right conjunct is abbreviated with $R \stackrel{\text{def}}{\equiv} \langle x' = f(x) \,\&\, Q\rangle\bigcirc \rightarrow \langle x' = f(x) \,\&\, P\rangle\bigcirc$. The M[′] step rewrites the postcondition equivalently using the propositional tautology $P \wedge R \leftrightarrow P \wedge (P \rightarrow R)$ which allows the left conjunct $P$ to be assumed when proving the right conjunct $R$ (the implication $x=y$ is also distributed over the conjunction). The two conjuncts are then split by [·]∧, ∧R, with

the resulting two premises labeled ① and ② respectively. These are shown and proved below.

$$\dfrac{\dfrac{\dfrac{\dfrac{\overset{①}{P \vdash [x' = f(x) \& Q \wedge (P \vee x=y)]\big((x=y \to P) \wedge (x=y \wedge P \to R)\big)}}{P \vdash [x' = f(x) \& Q \wedge (P \vee x=y)](x=y \to P \wedge R)}\ \text{M}[']}{P \vdash \forall y\,[x' = f(x) \& Q \wedge (P \vee x=y)](x=y \to P \wedge R)}\ {\vee}\text{R}}{P \vdash [x' = f(x) \& Q]P}\ \text{RI\&}}{}$$

where the leftmost label on the top line is $[\cdot]\wedge,\,\wedge\text{R}$.

The premise ② yields the top premise of rule rI& directly (unfolding the abbreviation for $R$):

$$\dfrac{\dfrac{\overset{}{x=y, P, Q, \langle x' = f(x) \& Q\rangle\bigcirc \vdash \langle x' = f(x) \& P\rangle\bigcirc}}{Q \vdash (x=y \wedge P \to R)}\ {\to}\text{R},\,\wedge\text{L}}{P \vdash [x' = f(x) \& Q \wedge (P \vee x=y)](x=y \wedge P \to R)}\ \text{dW}$$

Continuing from premise ①, the derivation splits classically on whether $x=y$ is true initially, yielding two further premises labeled ③ when $x=y$ and ④ when $x \neq y$.

$$\dfrac{\dfrac{\overset{③\qquad ④}{x=y \vee x \neq y, P \vdash [x' = f(x) \& Q \wedge (P \vee x=y)](x=y \to P)}}{}\ {\vee}\text{L}}{P \vdash [x' = f(x) \& Q \wedge (P \vee x=y)](x=y \to P)}\ \text{cut}$$

From ③, the antecedents $x=y$ and $P$ imply that $P(y)$ is true initially by a cut. Since $y$ is held constant by the ODE $x' = f(x)$, a monotonicity step M['] followed by V completes the proof:

$$\dfrac{\dfrac{*}{P(y) \vdash [x' = f(x) \& Q \wedge (P \vee x=y)]P(y)}\ \text{V}}{x=y, P \vdash [x' = f(x) \& Q \wedge (P \vee x=y)](x=y \to P)}\ \text{cut, M[']}$$

From ④, the derivation continues by dualizing to the diamond modality, and using rfl⟨·⟩ to syntactically reverse the direction of the ODE. The dRW⟨·⟩ step weakens the resulting postcondition of the diamond modality with the propositional tautology $x{\neq}y \wedge P \to x{\neq}y$.

$$\dfrac{\dfrac{\dfrac{\overset{}{x=y, \neg P, \langle x' = -f(x) \& Q \wedge (P \vee x=y)\rangle x{\neq}y \vdash \mathit{false}}}{x=y, \neg P, \langle x' = -f(x) \& Q \wedge (P \vee x=y)\rangle(x{\neq}y \wedge P) \vdash \mathit{false}}\ \text{dRW}\langle\cdot\rangle}{x{\neq}y, P, \langle x' = f(x) \& Q \wedge (P \vee x=y)\rangle(x=y \wedge \neg P) \vdash \mathit{false}}\ \text{rfl}\langle\cdot\rangle}{x{\neq}y, P \vdash [x' = f(x) \& Q \wedge (P \vee x=y)](x=y \to P)}\ \langle\cdot\rangle,\,\neg\text{R}$$

The diamond modality in the antecedent splits by axiom Uniq into two assumptions with domain constraints $Q$ and $P \vee x=y$ respectively. With a use of derived axiom Init, all the antecedents of the bottom premise of rule rI& are gathered, leaving only its succedent.

$$\dfrac{\dfrac{\overset{}{x=y, \neg P, Q, \langle x' = -f(x) \& Q\rangle\bigcirc, \langle x' = -f(x) \& P\rangle\bigcirc \vdash \mathit{false}}}{x=y, \neg P, \langle x' = -f(x) \& Q\rangle x \neq y, \langle x' = -f(x) \& P \vee x=y\rangle x \neq y \vdash \mathit{false}}\ \text{Init}}{x=y, \neg P, \langle x' = -f(x) \& Q \wedge (P \vee x=y)\rangle x \neq y \vdash \mathit{false}}\ \text{Uniq}$$

Continuing with the derived implication $\neg\bigcirc_{\to}$ results in the bottom premise of rule rI&:

$$\dfrac{\dfrac{\overset{}{x=y, \neg P, Q, \langle x' = -f(x) \& Q\rangle\bigcirc \vdash \langle x' = -f(x) \& \neg P\rangle\bigcirc}}{x=y, \neg P, Q, \langle x' = -f(x) \& Q\rangle\bigcirc, \neg\langle x' = -f(x) \& \neg P\rangle\bigcirc \vdash \mathit{false}}\ \neg\text{L}}{x=y, \neg P, Q, \langle x' = -f(x) \& Q\rangle\bigcirc, \langle x' = -f(x) \& P\rangle\bigcirc \vdash \mathit{false}}\ \neg\bigcirc_{\to} \qquad \square$$

The rule rI& discards any additional context in the antecedents of its premises. This is due to the use of RI& which focuses on particular states along trajectories of the ODE $x' = f(x)$. It would be unsound to keep any assumptions about the initial state that depend on $x$ because the state being examined may not be the initial state! On the other hand, assumptions that do not depend on $x$

remain true along the ODE. These constant assumptions can be kept with uses of V throughout the derivation above or added into $Q$ before using rI& by a DC that proves with V. Such additional steps are elided and rule rI& is used directly while keeping these *constant* assumptions around.

### A.3 Axioms and Proof Rules Summary

For the sake of a self-contained presentation, this section presents all the propositional and first-order sequent calculus proof rules used in this article. Propositional and first-order logic is not the focus of this article so a simplified treatment is used. A full treatment of these rules can be found elsewhere [27]. For ease of reference, this section also compactly references all base (and extended) dL axioms and proof rules but does not repeat them explicitly because of space considerations. All other (derived) axioms and proof rules in this article derive from this dL axiomatization.

*Propositional and First-Order Proof Rules.* Rule ℝ for first-order real arithmetic is explained in Section 2.3. The following are sound propositional and first-order sequent calculus proof rules. In rules ∀L, ∃R, an arbitrary (extended) term $e$ can be used to instantiate the respective quantifiers. In rules ∃L, ∀R, the Skolem variable $y$ is fresh, i.e., does not occur free, in the conclusion:

$$\neg L \; \frac{\Gamma \vdash \phi}{\Gamma, \neg\phi \vdash false} \qquad \neg R \; \frac{\Gamma, \phi \vdash false}{\Gamma \vdash \neg\phi} \qquad \rightarrow L \; \frac{\Gamma \vdash \phi_1 \quad \Gamma, \phi_2 \vdash \psi}{\Gamma, \phi_1 \rightarrow \phi_2 \vdash \psi} \qquad \rightarrow R \; \frac{\Gamma, \phi_1 \vdash \phi_2}{\Gamma \vdash \phi_1 \rightarrow \phi_2}$$

$$\wedge L \; \frac{\Gamma, \phi_1, \phi_2 \vdash \psi}{\Gamma, \phi_1 \wedge \phi_2 \vdash \psi} \qquad \wedge R \; \frac{\Gamma \vdash \phi_1 \quad \Gamma \vdash \phi_2}{\Gamma \vdash \phi_1 \wedge \phi_2} \qquad \forall L \; \frac{\Gamma, \phi(e) \vdash \psi}{\Gamma, \forall x \, \phi(x) \vdash \psi} \qquad \forall R \; \frac{\Gamma \vdash \phi(y)}{\Gamma \vdash \forall x \, \phi(x)}$$

$$\vee L \; \frac{\Gamma, \phi_1 \vdash \psi \quad \Gamma, \phi_2 \vdash \psi}{\Gamma, \phi_1 \vee \phi_2 \vdash \psi} \qquad \text{cut} \; \frac{\Gamma \vdash \psi \quad \Gamma, \psi \vdash \phi}{\Gamma \vdash \phi} \qquad \exists L \; \frac{\Gamma, \phi(y) \vdash \psi}{\Gamma, \exists x \, \phi(x) \vdash \psi} \qquad \exists R \; \frac{\Gamma \vdash \phi(e)}{\Gamma \vdash \exists x \, \phi(x)}$$

*Base Axioms and Proof Rules.* All base axioms and proof rules of dL are in Theorem A.3. The base differential axioms are in Theorem 2.2, while Lemma 2.5 provides differential axioms for extended terms. The base differential equation axioms DI, DC, DG are in Theorem 2.6.

*Extended Axiomatization.* The extended axioms Uniq, Cont, Dadj are in Lemma 5.1. The extended real induction axiom RI and its generalization RI& are in Lemmas 5.5 and A.2 respectively.

*Hybrid Program Axioms.* These are presented in Theorem C.1 for use only in Appendix C.

## B COMPLETENESS

This appendix gives completeness proofs for the derived rules dRI, sAI and the derived local progress characterization LP. Completeness of dRI is proved by showing that DRI is a derived axiom. A similar approach is taken for completeness of sAI by showing SAI is a derived axiom.

This syntactic approach to proving completeness of dRI and sAI demonstrates the versatility of the dL calculus. It also enables complete *dis*proofs of invariance properties as opposed to just failing to apply a complete proof rule. To conclude that invariance is *disproved* after applying an algorithmic procedure (like the presentations of (semi)algebraic dRI and sAI [15, 22]), one would need to trust, in addition to soundness, that no completeness errors are present in the implementation.

Recall that axioms Cont, RI& have an additional syntactic requirement, e.g., the presence of $x_1' = 1$, which is assumed to be met throughout this appendix, using axiom DG if necessary.

### B.1 Progress Formulas

The following are useful logical rearrangements of the progress formulas for extended term $e$:

PROPOSITION B.1 (ATOMIC PROGRESS FORMULA EQUIVALENCES). *Let $N$ be the rank of extended term $e$. The following are provable equivalences on the progress and differential radical formulas for $e$:*

$$\dot{e}^{(*)} > 0 \leftrightarrow e > 0 \vee (e = 0 \wedge \dot{e} > 0) \vee \ldots \tag{8}$$
$$\vee \left( e = 0 \wedge \dot{e} = 0 \wedge \cdots \wedge \dot{e}^{(N-3)} = 0 \wedge \dot{e}^{(N-2)} > 0 \right)$$
$$\vee \left( e = 0 \wedge \dot{e} = 0 \wedge \cdots \wedge \dot{e}^{(N-2)} = 0 \wedge \dot{e}^{(N-1)} > 0 \right)$$
$$\dot{e}^{(*)} \geq 0 \leftrightarrow e \geq 0 \wedge \left( e = 0 \rightarrow \dot{e} \geq 0 \right) \wedge \ldots \tag{9}$$
$$\wedge \left( e = 0 \wedge \dot{e} = 0 \wedge \cdots \wedge \dot{e}^{(N-3)} = 0 \rightarrow \dot{e}^{(N-2)} \geq 0 \right)$$
$$\wedge \left( e = 0 \wedge \dot{e} = 0 \wedge \cdots \wedge \dot{e}^{(N-2)} = 0 \rightarrow \dot{e}^{(N-1)} \geq 0 \right)$$
$$\neg(\dot{e}^{(*)} > 0) \leftrightarrow (\dot{-e})^{(*)} \geq 0 \qquad \neg(\dot{e}^{(*)} \geq 0) \leftrightarrow (\dot{-e})^{(*)} > 0 \tag{10}$$
$$\neg(\dot{e}^{(*)} = 0) \leftrightarrow \dot{e}^{(*)} > 0 \vee (\dot{-e})^{(*)} > 0 \tag{11}$$

PROOF. The equivalences are proved one at a time. By linearity of Lie derivatives, $(\dot{-e})^{(i)} = -(\dot{e}^{(i)})$ proves in real arithmetic for any $i$. The proof also uses these provable real arithmetic equivalences:

$$e \geq 0 \leftrightarrow e = 0 \vee e > 0 \qquad -e \geq 0 \wedge e \geq 0 \leftrightarrow e = 0 \qquad \neg(e > 0) \leftrightarrow -e \geq 0$$

(8) This equivalence follows by real arithmetic, and simplifying with propositional rearrangement as follows (here, the remaining conjuncts of $\dot{e}^{(*)} > 0$ are abbreviated to ... ):

$$e \geq 0 \wedge \left( (e = 0 \rightarrow \dot{e} \geq 0) \wedge \ldots \right) \leftrightarrow e > 0 \wedge \left( (e = 0 \rightarrow \dot{e} \geq 0) \wedge \ldots \right)$$
$$\vee e = 0 \wedge \left( (e = 0 \rightarrow \dot{e} \geq 0) \wedge \ldots \right)$$

The first disjunct on the RHS simplifies by real arithmetic to $e > 0$ since all of its implicational conjuncts contain $e = 0$ on the left of an implication. The latter disjunct simplifies to $e = 0 \wedge \left( \dot{e} \geq 0 \wedge \ldots \right)$, yielding the provable equivalence:

$$\dot{e}^{(*)} > 0 \leftrightarrow e > 0 \vee e = 0 \wedge \left( \dot{e} \geq 0 \wedge \ldots \right)$$

The equivalence (8) proves by iterating this expansion on the RHS of this equivalence for its nested conjuncts with higher Lie derivatives.

(9) This equivalence proves by expanding the formula $\dot{e}^{(*)} \geq 0$ which yields a disjunction between $\dot{e}^{(*)} > 0$ and $\dot{e}^{(*)} = 0$. The latter formula is used to relax the strict inequality in the last conjunct of $\dot{e}^{(*)} > 0$ to a non-strict inequality.

(10) The equivalence for $\neg(\dot{e}^{(*)} > 0)$ follows by negating both sides of equivalence (8) and moving negations on the RHS inwards propositionally, yielding the provable equivalence:

$$\neg(\dot{e}^{(*)} > 0) \leftrightarrow \Big( \neg(e > 0) \wedge (e = 0 \rightarrow \neg(\dot{e} > 0)) \wedge \ldots$$
$$\wedge \left( e=0 \wedge \dot{e}=0 \wedge \cdots \wedge \dot{e}^{(N-2)}=0 \rightarrow \neg(\dot{e}^{(N-1)} > 0) \right) \Big)$$

The desired equivalence derives by negating the inequalities and by equivalence (9) for $(\dot{-e})^{(*)} \geq 0$. The equivalence for $\neg(\dot{e}^{(*)} \geq 0)$ derives by negating both sides of the equivalence for $\neg(\dot{e}^{(*)} > 0)$, since $-(-e) = e$.

(11) By (10), the following equivalence is provable:

$$\neg(\dot{e}^{(*)} > 0) \wedge \neg((\dot{-e})^{(*)} > 0) \leftrightarrow ((\dot{-e})^{(*)} \geq 0) \wedge (\dot{e}^{(*)} \geq 0)$$

By rewriting with (9), the RHS of this equivalence is provably equivalent to the formula $\dot{e}^{(*)} = 0$ in real arithmetic. Negating both sides yields the provable equivalence (11). □

The provable equivalences (10) are particularly important, because they underlie the next proposition, from which the complete characterization of local progress follows:

PROPOSITION B.2 (NEGATED SEMIANALYTIC PROGRESS FORMULA). *Let the semianalytic formula $P$ be in normal form* (5). *Then $\neg P$ can be put into normal form such that $\neg(\dot{P}^{(*)}) \leftrightarrow (\dot{\neg P})^{(*)}$ is provable:*

$$\neg P \equiv \bigvee_{i=0}^{N} \Big( \bigwedge_{j=0}^{a(i)} d_{ij} \geq 0 \wedge \bigwedge_{j=0}^{b(i)} \tilde{d}_{ij} > 0 \Big)$$

PROOF. The proof uses propositional tautologies $\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$ and $\neg(A \vee B) \leftrightarrow \neg A \wedge \neg B$. Formula $P$ is negated (in normal form (5)) and all sub-terms are negated so the inequalities have 0 on the RHS, yielding the following provable equivalence. The resulting RHS is abbreviated by $\phi$:

$$\neg P \leftrightarrow \underbrace{\bigwedge_{i=0}^{M} \Big( \bigvee_{j=0}^{m(i)} -e_{ij} > 0 \vee \bigvee_{j=0}^{n(i)} -\tilde{e}_{ij} \geq 0 \Big)}_{\phi}$$

Negating both sides of the progress formula for $P$ and simplifying propositionally proves:

$$\neg(\dot{P}^{(*)}) \leftrightarrow \bigwedge_{i=0}^{M} \Big( \bigvee_{j=0}^{m(i)} \neg(\dot{e}_{ij}^{(*)} \geq 0) \vee \bigvee_{j=0}^{n(i)} \neg(\dot{\tilde{e}}_{ij}^{(*)} > 0) \Big)$$

Rewriting the RHS with equivalences (10) from Proposition B.1 yields the following provable equivalence. The resulting RHS is abbreviated by $\psi$:

$$\neg(\dot{P}^{(*)}) \leftrightarrow \underbrace{\bigwedge_{i=0}^{M} \Big( \bigvee_{j=0}^{m(i)} (-\dot{e}_{ij})^{(*)} > 0 \vee \bigvee_{j=0}^{n(i)} (-\dot{\tilde{e}}_{ij})^{(*)} \geq 0 \Big)}_{\psi}$$

Observe that $\phi, \psi$ have the same conjunctive normal form shape. Distribute the outer conjunction over the inner disjunctions in $\phi$ to obtain the following provable equivalence, whose RHS is a normal form for $\neg P$ (for some indices $N, a(i), b(i)$ and extended terms $d_{ij}, \tilde{d}_{ij}$):

$$\neg P \leftrightarrow \bigvee_{i=0}^{N} \Big( \bigwedge_{j=0}^{a(i)} d_{ij} \geq 0 \vee \bigwedge_{j=0}^{b(i)} \tilde{d}_{ij} > 0 \Big)$$

Distribute the disjunction in $\psi$ following the same syntactic steps taken for $\phi$ to obtain the following provable equivalence:

$$\psi \leftrightarrow \bigvee_{i=0}^{N} \Big( \bigwedge_{j=0}^{a(i)} \dot{d}_{ij}^{(*)} \geq 0 \vee \bigwedge_{j=0}^{b(i)} \dot{\tilde{d}}_{ij}^{(*)} > 0 \Big)$$

Rewriting with the equivalences derived so far, and using the above normal form for $\neg P$, yields the required, provable equivalence:

$$\neg(\dot{P}^{(*)}) \leftrightarrow (\dot{\neg P})^{(*)}$$                                              □

## B.2 Local Progress

This section derives the characterizations of local progress from Section 6.1. These characterizations are used in the completeness proofs for both analytic and semianalytic invariants.

*B.2.1 Atomic Inequalities.* The proof of Lemma 6.3 was outlined in Section 6.1. The case where $\succcurlyeq$ is $\geq$ is proved first, while the more technical case where $\succcurlyeq$ is $>$ is proved subsequently.

PROOF OF LEMMA 6.3 ($\text{LP}_{\geq*}$). Let $N$ be the rank of extended term $e$ with respect to $x' = f(x)$ from (3). For the derivation of $\text{LP}_{\geq*}$, the additional flexibility of the $\bigcirc$ modality with a disjunct $x = y$ in the domain constraint is not needed. This disjunction is removed after unfolding the $\bigcirc$ abbreviation using a $\text{dRW}\langle\cdot\rangle$ monotonicity step. The definition of $\dot{e}^{(*)} \geq 0$ is also unfolded, with both disjuncts handled separately. The premises are labeled ① and ② respectively.

$$
\begin{array}{c}
\dfrac{x{=}y, \dot{e}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, e \geq 0\rangle x \neq y \qquad x{=}y, \dot{e}^{(*)} = 0 \vdash \langle x' = f(x) \,\&\, e \geq 0\rangle x \neq y}{\begin{array}{c}
\dfrac{x{=}y, \dot{e}^{(*)} > 0 \vee \dot{e}^{(*)} = 0 \vdash \langle x' = f(x) \,\&\, e \geq 0\rangle x \neq y}{\dfrac{x{=}y, \dot{e}^{(*)} > 0 \vee \dot{e}^{(*)} = 0 \vdash \langle x' = f(x) \,\&\, e \geq 0 \vee x = y\rangle x \neq y}{x{=}y, \dot{e}^{(*)} \geq 0 \vdash \langle x' = f(x) \,\&\, e \geq 0\rangle\bigcirc}}
\end{array}}
\end{array}
$$

with labels $\vee\text{L}$ and $\text{dRW}\langle\cdot\rangle$.

From ②, $\text{dRW}\langle\cdot\rangle$ strengthens the inequality $e \geq 0$ in the domain constraint to an equation $e = 0$. The derivation continues using $\text{DR}\langle\cdot\rangle$, because by $\text{dRI}$, $e = 0$ is provably invariant. The proof is completed with $\text{Cont}$ using the trivial arithmetic fact $1 > 0$:

$$
\dfrac{\dfrac{\quad * \quad}{\text{dRI} \;\; \dot{e}^{(*)} = 0 \vdash [x' = f(x) \,\&\, 1 > 0]e = 0} \qquad \dfrac{\quad * \quad}{\text{Cont} \;\; x{=}y \vdash \langle x' = f(x) \,\&\, 1 > 0\rangle x \neq y}}{\dfrac{x{=}y, \dot{e}^{(*)} = 0 \vdash \langle x' = f(x) \,\&\, e = 0\rangle x \neq y}{x{=}y, \dot{e}^{(*)} = 0 \vdash \langle x' = f(x) \,\&\, e \geq 0\rangle x \neq y}}
$$

with labels $\text{DR}\langle\cdot\rangle$ and $\text{dRW}\langle\cdot\rangle$.

From ①, the premise is lined up for the derived step axiom $\text{LPi}_\geq$. The proof proceeds by closing the (left) premises obtained by iterating $\text{LPi}_\geq$ for higher Lie derivatives. In this way, the derivation continues until the final (rightmost) open premise which is abbreviated here and continued below:

$$
\dfrac{\dfrac{\quad * \quad}{\mathbb{R} \;\; \dot{e}^{(*)} > 0 \vdash e \geq 0} \qquad \dfrac{\dfrac{\quad * \quad}{\mathbb{R} \;\; \dot{e}^{(*)} > 0, e = 0 \vdash \dot{e} \geq 0} \qquad \dfrac{x{=}y, \dot{e}^{(*)} > 0, \ldots \vdash \ldots}{\ldots}}{\text{LPi}_\geq \;\; x{=}y, \dot{e}^{(*)} > 0, e = 0 \vdash \langle x' = f(x) \,\&\, \dot{e} \geq 0\rangle x \neq y}}{\text{LPi}_\geq \;\; x{=}y, \dot{e}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, e \geq 0\rangle x \neq y}
$$

The open premise corresponds to the last conjunct of $\dot{e}^{(*)} > 0$. The implication in the conjunct uses the gathered antecedents $e = 0, \ldots, \dot{e}^{(N-2)} = 0$ after which $\text{Cont}, \text{dRW}\langle\cdot\rangle$ completes the proof:

$$
\dfrac{\dfrac{\quad * \quad}{x{=}y, \dot{e}^{(N-1)} > 0 \vdash \langle x' = f(x) \,\&\, \dot{e}^{(N-1)} \geq 0\rangle x \neq y}}{x{=}y, \dot{e}^{(*)} > 0, e = 0, \ldots, \dot{e}^{(N-2)} = 0 \vdash \langle x' = f(x) \,\&\, \dot{e}^{(N-1)} \geq 0\rangle x \neq y} \qquad \square
$$

with labels $\text{Cont}, \text{dRW}\langle\cdot\rangle$ and $\text{cut}$.

Unlike the non-strict case just derived for Lemma 6.3, the strict case (where $\succcurlyeq$ is $>$) crucially uses the fact that the $\bigcirc$ modality *excludes* the initial state, so that it is possible to locally progress into the strict inequality $e > 0$ without already satisfying it in the initial state. Topological considerations made this exclusion irrelevant for the non-strict case (see Section 6.1), as derived axiom Init explains logically. The idea behind the remaining proof of Lemma 6.3 for the strict case is to syntactically embed this difference into the derivation of $\text{LP}_{>*}$. Moreover, this syntactic transformation reduces the proof to the non-strict case, so that the derived step axiom $\text{LPi}_\geq$ can again be used to progressively analyze higher Lie derivatives. The following proposition is used for the transformation:

PROPOSITION B.3. *Let $d = e^k$ for some $k \geq 1$ and $x' = f(x)$ be an ODE with extended terms $e, d, f(x)$. For each $0 \leq i \leq k - 1$, there (computably) exists an extended term cofactor $g$ such that the following identity is provable in real arithmetic:*

$$\dot{d}^{(i)} = ge$$

PROOF. The proof proceeds by induction on $k$.

- For $k = 1$, $d = e^1$ so $\dot{e}^{(0)} = e$ hence the cofactor $g = 1$ suffices.
- For $d = e^{k+1}$, the $j$-th Lie derivative of $d$ for $0 \leq j \leq k$ is given by Leibniz's rule:

$$\dot{d}^{(j)} = \mathcal{L}_{f(x)}^{(j)}(e^k e) = \sum_{i=0}^{j} \binom{j}{i} (\dot{e^k})^{(j-i)} \dot{e}^{(i)}$$

The induction hypothesis implies $(\dot{e^k})^{(j-i)} = g_i e$ is a provable identity for some computable extended term cofactor $g_i$ for each $1 \leq i \leq j$. The final summand for $i = 0$ is:

$$\binom{j}{0} (\dot{e^k})^{(j)} \dot{e}^{(0)} = (\dot{e^k})^{(j)} e$$

Thus, the cofactor $g = (\dot{e^k})^{(j)} + \sum_{i=1}^{j} \binom{j}{i} g_i \dot{e}^{(i)}$ yields the identity $\dot{d}^{(j)} = ge$. This identity is provable because it only depends on first-order properties of real arithmetic. □

For $d = e^k, k \geq 1$, Proposition B.3 implies that the formula $e = 0 \rightarrow \bigwedge_{i=0}^{k-1} \dot{d}^{(i)} = 0$ is provable in real arithmetic for extended terms $e, d$. This enables the remaining proof of Lemma 6.3.

PROOF OF LEMMA 6.3 (LP$_{>*}$). Let $N \geq 1$ be the rank of extended term $e$ with respect to $x' = f(x)$. This rank bounds the number of higher Lie derivatives of $e$ that need to be considered.

The derivation starts by unfolding the syntactic abbreviation of the $\bigcirc$ modality and reducing to the non-strict case with dRW$\langle \cdot \rangle$ and the real arithmetic fact $e - d \geq 0 \rightarrow e > 0 \vee x = y$ for the abbreviation $d \overset{\text{def}}{=} |x - y|^{2N}$, which is a (polynomial) term: $\left( (x_1 - y_1)^2 + \cdots + (x_n - y_n)^2 \right)^N$.

$$\text{dRW}\langle \cdot \rangle \frac{\mathbb{R}\dfrac{*}{e - d \geq 0 \vdash e > 0 \vee x = y} \qquad x = y, \dot{e}^{(*)} > 0 \vdash \langle x' = f(x) \, \& \, e - d \geq 0 \rangle x \neq y}{\dfrac{x = y, \dot{e}^{(*)} > 0 \vdash \langle x' = f(x) \, \& \, e > 0 \vee x = y \rangle x \neq y}{x = y, \dot{e}^{(*)} > 0 \vdash \langle x' = f(x) \, \& \, e > 0 \rangle \bigcirc}}$$

Next, the initial assumption $x = y$ in the antecedent is used. The first cut proves using the formula of real arithmetic: $x = y \rightarrow |x - y|^2 = 0$. As remarked, with $|x - y|^2 = 0$ and $N \geq 1$, by Proposition B.3, $|x - y|^2 = 0 \rightarrow \bigwedge_{i=0}^{N-1} \dot{d}^{(i)} = 0$ is a provable real arithmetic formula. The second cut proves using this fact. The resulting open premise is abbreviated ①.

$$\text{cut}, \mathbb{R} \frac{\text{cut}, \mathbb{R} \dfrac{x = y, \bigwedge_{i=0}^{N-1} \dot{d}^{(i)} = 0, \dot{e}^{(*)} > 0 \vdash \langle x' = f(x) \, \& \, e - d \geq 0 \rangle x \neq y}{x = y, |x - y|^2 = 0, \dot{e}^{(*)} > 0 \vdash \langle x' = f(x) \, \& \, e - d \geq 0 \rangle x \neq y}}{x = y, \dot{e}^{(*)} > 0 \vdash \langle x' = f(x) \, \& \, e - d \geq 0 \rangle x \neq y}$$

To continue from ①, observe that for $0 \leq i \leq N - 1$, by linearity of the Lie derivative:

$$\mathcal{L}_{f(x)}^{(i)}(e - d) = \dot{e}^{(i)} - \dot{d}^{(i)}$$

Using the conjunction $\bigwedge_{i=0}^{N-1} \dot{d}^{(i)} = 0$ in the antecedents, the formula $(\dot{e - d})^{(i)} = \dot{e}^{(i)}$ proves by a cut and real arithmetic for $0 \leq i \leq N - 1$. This justifies the next real arithmetic step from ①, with

the assumptions $\Gamma_d \stackrel{\text{def}}{\equiv} \bigwedge_{i=0}^{N-1} (e-d)^{(i)} = \dot{e}^{(i)}$. Intuitively, $\Gamma_d$ allows the derivation to locally work with higher Lie derivatives of $e$ instead of higher Lie derivatives of $e - d$ in subsequent steps.

$$\text{cut, } \mathbb{R} \frac{\Gamma_d, x{=}y, \dot{e}^{(*)} > 0 \vdash \langle x' = f(x) \& e{-}d \geq 0 \rangle x \neq y}{x{=}y, \bigwedge_{i=0}^{N-1} \dot{d}^{(i)} = 0, \dot{e}^{(*)} > 0 \vdash \langle x' = f(x) \& e{-}d \geq 0 \rangle x \neq y}$$

The derivation is completed using the same technique of iterating $\text{LPi}_{\geq}$, as shown in the earlier proof of Lemma 6.3 for the non-strict case $\text{LP}_{\geq *}$. It starts with a single $\text{LPi}_{\geq}$ step. The left premise closes by real arithmetic because $\dot{e}^{(*)} > 0$ has the conjunct $e \geq 0$, and $\Gamma_d$ provides $e - d = e$, which imply $e - d \geq 0$. The right premise is abbreviated ②.

$$\text{LPi}_{\geq} \frac{\mathbb{R} \frac{*}{\Gamma_d, \dot{e}^{(*)} > 0 \vdash e{-}d \geq 0} \qquad \Gamma_d, x{=}y, \dot{e}^{(*)} > 0, e{-}d = 0 \vdash \langle x' = f(x) \& (e{-}d)^{(1)} \geq 0 \rangle x \neq y}{\Gamma_d, x{=}y, \dot{e}^{(*)} > 0 \vdash \langle x' = f(x) \& e{-}d \geq 0 \rangle x \neq y}$$

From ②, local progress for the first Lie derivative of $e{-}d$ is shown. The first step simplifies formula $e{-}d = 0$ in the antecedents using $\Gamma_d$. The derived axiom $\text{LPi}_{\geq}$, together with $\Gamma_d$, simplifies and proves the left premise. The right premise is abbreviated ③ (shown and continued below).

$$\mathbb{R} \frac{\text{LPi}_{\geq} \frac{\mathbb{R} \frac{\mathbb{R} \frac{*}{e = 0 \rightarrow \dot{e} \geq 0, e = 0 \vdash \dot{e}^{(1)} \geq 0}}{\Gamma_d, \dot{e}^{(*)} > 0, e = 0 \vdash (e{-}d)^{(1)} \geq 0} \qquad ③}{\Gamma_d, x{=}y, \dot{e}^{(*)} > 0, e = 0 \vdash \langle x' = f(x) \& (e{-}d)^{(1)} \geq 0 \rangle x \neq y}}{\Gamma_d, x{=}y, \dot{e}^{(*)} > 0, e{-}d = 0 \vdash \langle x' = f(x) \& (e{-}d)^{(1)} \geq 0 \rangle x \neq y}$$

The derivation continues from ③ similarly for higher Lie derivatives of $e{-}d$, using $\Gamma_d$ to replace $(e{-}d)^{(i)}$ with $\dot{e}^{(i)}$, and then using the corresponding conjunct of $\dot{e}^{(*)} > 0$. The final open premise obtained from ③ by iterating $\text{LPi}_{\geq}$ corresponds to the last conjunct of $\dot{e}^{(*)} > 0$:

$$\mathbb{R} \frac{\text{LPi}_{\geq} \frac{\text{LPi}_{\geq} \frac{\Gamma_d, x{=}y, \dot{e}^{(*)} > 0, e = 0, \ldots, \dot{e}^{(N-2)} = 0 \vdash \langle x' = f(x) \& (e{-}d)^{(N-1)} \geq 0 \rangle x \neq y}{\cdots}}{\Gamma_d, x{=}y, \dot{e}^{(*)} > 0, e = 0, \dot{e}^{(1)} \geq 0 \vdash \langle x' = f(x) \& (e{-}d)^{(2)} \geq 0 \rangle x \neq y}}{\Gamma_d, x{=}y, \dot{e}^{(*)} > 0, e = 0, (e{-}d)^{(1)} \geq 0 \vdash \langle x' = f(x) \& (e{-}d)^{(2)} \geq 0 \rangle x \neq y}$$

The gathered antecedents $e = 0, \ldots, \dot{e}^{(N-2)} = 0$ are respectively obtained from $\Gamma_d$ by real arithmetic. The proof is closed with $\text{dRW}\langle \cdot \rangle$, Cont, similarly to the non-strict case.

$$\text{cut} \frac{\text{dRW}\langle \cdot \rangle \frac{\text{cut, } \mathbb{R} \frac{\text{Cont} \frac{*}{x{=}y, (e{-}d)^{(N-1)} > 0 \vdash \langle x' = f(x) \& (e{-}d)^{(N-1)} > 0 \rangle x \neq y}}{\Gamma_d, x{=}y, \dot{e}^{(N-1)} > 0 \vdash \langle x' = f(x) \& (e{-}d)^{(N-1)} > 0 \rangle x \neq y}}{\Gamma_d, x{=}y, \dot{e}^{(N-1)} > 0 \vdash \langle x' = f(x) \& (e{-}d)^{(N-1)} \geq 0 \rangle x \neq y}}{\Gamma_d, x{=}y, \dot{e}^{(*)} > 0, e = 0, .., \dot{e}^{(N-2)} = 0 \vdash \langle x' = f(x) \& (e{-}d)^{(N-1)} \geq 0 \rangle x \neq y} \qquad \square$$

*B.2.2 Semianalytic Formulas.* The proof in the semianalytic case is outlined in Section 6.1. It lifts derived axioms $\text{LP}_{\geq *}$ and $\text{LP}_{> *}$ according to the homomorphic definition of the semianalytic progress formula, using Uniq to prove local progress into a conjunction of two formulas simultaneously.

Proof of Lemma 6.5. By congruential equivalence [32], assume, without loss of generality, that formula $P$ is propositionally rewritten to the same normal form (5) as in the corresponding semianalytic progress formula $\dot{P}^{(*)}$. Throughout this proof, similar premises are collapsed in proofs and directly indexed by $i, j$. The $i$-th disjunct of $P$ is abbreviated with $P_i \overset{\text{def}}{\equiv} \bigwedge_{j=0}^{m(i)} e_{ij} \geq 0 \wedge \bigwedge_{j=0}^{n(i)} \tilde{e}_{ij} > 0$.

The derivation starts by splitting the (outermost) disjunction in $\dot{P}^{(*)}$ with $\vee$L. For each resulting premise (indexed by $i$), local progress is proved for the corresponding disjunct $P_i$ of $P$. The domain change with $\mathrm{dRW}\langle\cdot\rangle$ proves because $P_i \vee x = y \to P \vee x = y$ is a propositional tautology for each $i$.

$$
\frac{\dfrac{x{=}y, \bigwedge_{j=0}^{m(i)} \dot{e}_{ij}^{(*)} \geq 0 \wedge \bigwedge_{j=0}^{n(i)} \dot{\tilde{e}}_{ij}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, P_i \rangle \bigcirc}{\underset{\mathrm{dRW}\langle\cdot\rangle}{\phantom{x}} \; x{=}y, \bigwedge_{j=0}^{m(i)} \dot{e}_{ij}^{(*)} \geq 0 \wedge \bigwedge_{j=0}^{n(i)} \dot{\tilde{e}}_{ij}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, P \rangle \bigcirc}}{\underset{\vee\mathrm{L}}{\phantom{x}} \; x{=}y, \dot{P}^{(*)} \vdash \langle x' = f(x) \,\&\, P \rangle \bigcirc}
$$

It suffices now to prove local progress in $P_i$. The uniqueness axiom Uniq splits conjuncts in $P_i$. The $\mathrm{dRW}\langle\cdot\rangle$ step distributes $x{=}y$ in domain constraint from $\bigcirc$ over conjunctions using the propositional tautology $(R_1 \wedge R_2) \vee x{=}y \leftrightarrow (R_1 \vee x{=}y) \wedge (R_2 \vee x = y)$. This leaves premises (indexed by $j$) for the non-strict and strict inequalities of $P_i$ which are closed by $\mathrm{LP}_{\geq^*}$ and $\mathrm{LP}_{>^*}$ respectively.

$$
\underset{\text{Uniq, } \wedge\mathrm{R, dRW}\langle\cdot\rangle}{\dfrac{\mathrm{LP}_{\geq^*} \dfrac{*}{x{=}y, \dot{e}_{ij}^{(*)} \geq 0 \vdash \langle x'{=}f(x) \,\&\, e_{ij}{\geq}0 \rangle \bigcirc} \qquad \mathrm{LP}_{>^*} \dfrac{*}{x{=}y, \dot{\tilde{e}}_{ij}^{(*)} > 0 \vdash \langle x'{=}f(x) \,\&\, \tilde{e}_{ij}{>}0 \rangle \bigcirc}}{x{=}y, \bigwedge_{j=0}^{m(i)} \dot{e}_{ij}^{(*)} \geq 0 \wedge \bigwedge_{j=0}^{n(i)} \dot{\tilde{e}}_{ij}^{(*)} > 0 \vdash \langle x'{=}f(x) \,\&\, P_i \rangle \bigcirc}} \qquad \square
$$

Using Proposition B.2, the implicational semianalytic local progress axiom $\mathrm{LP}_{\mathbb{R}}$ from Lemma 6.5 is strengthened to an equivalent characterization of semianalytic local progress.

Proof of Theorem 6.6. By congruential equivalence [32], assume, without loss of generality, that formula $P$ is propositionally rewritten to the same normal form (5) as in the corresponding semianalytic progress formula $\dot{P}^{(*)}$. By Proposition B.2, there is a normal form for $\neg P$ with the provable equivalence $\neg(\dot{P}^{(*)}) \leftrightarrow (\dot{\neg P})^{(*)}$. The "$\leftarrow$" direction of the inner equivalence is $\mathrm{LP}_{\mathbb{R}}$. The derivation in the "$\to$" direction of the inner equivalence starts by reducing to the contrapositive statement by propositional logic transformations. The final step rewrites the negation in the antecedents using the above normal form for $\neg P$ from Proposition B.2.

$$
\underset{\text{cut, } \neg\mathrm{L}, \neg\mathrm{R}}{\dfrac{\mathbb{R} \dfrac{x{=}y, (\dot{\neg P})^{(*)} \vdash \neg \langle x' = f(x) \,\&\, P \rangle \bigcirc}{x{=}y, \neg(\dot{P}^{(*)}) \vdash \neg \langle x' = f(x) \,\&\, P \rangle \bigcirc}}{x{=}y, \langle x' = f(x) \,\&\, P \rangle \bigcirc \vdash \dot{P}^{(*)}}}
$$

By the derived axiom $\mathrm{LP}_{\mathbb{R}}$ from Lemma 6.5, the progress formula for $\neg P$ in the antecedent implies local progress for $\neg P$. The proof is completed with derived axiom $\neg\bigcirc_{\to}$ of Corollary A.6:

$$
\underset{\mathrm{LP}_{\mathbb{R}}}{\dfrac{\neg\bigcirc_{\to} \dfrac{*}{x{=}y, \langle x' = f(x) \,\&\, \neg P \rangle \bigcirc \vdash \neg \langle x' = f(x) \,\&\, P \rangle \bigcirc}}{x{=}y, (\dot{\neg P})^{(*)} \vdash \neg \langle x' = f(x) \,\&\, P \rangle \bigcirc}} \qquad \square
$$

Proof of Corollary 6.7. Self-duality axiom $\neg\bigcirc$ derives by using LP twice together with the provable equivalence $\neg(\dot{P}^{(*)}) \leftrightarrow (\dot{\neg P})^{(*)}$ from Proposition B.2 (and double negation elimination).

$$
\dfrac{
\dfrac{
\dfrac{*}{x{=}y \vdash \langle x' = f(x) \,\&\, P\rangle\bigcirc \leftrightarrow \dot{P}^{(*)}} \text{ LP}
}{x{=}y \vdash \langle x' = f(x) \,\&\, P\rangle\bigcirc \leftrightarrow \neg(\dot{\neg P})^{(*)}} \ \mathbb{R}
}{x{=}y \vdash \langle x' = f(x) \,\&\, P\rangle\bigcirc \leftrightarrow \neg\langle x' = f(x) \,\&\, \neg P\rangle\bigcirc} \text{ LP}
$$

Local progress congruence rule CLP derives similarly by introducing an initial assumption $x{=}y$ with cut, $\mathbb{R}$, $\exists$L, equivalently rewriting with LP, and congruential equivalence [32] in the last step.

$$
\dfrac{
\dfrac{
\dfrac{\vdash P \leftrightarrow R}{\vdash \langle x' = f(x) \,\&\, P\rangle\bigcirc \leftrightarrow \langle x' = f(x) \,\&\, R\rangle\bigcirc}
}{x{=}y \vdash \dot{P}^{(*)} \leftrightarrow \dot{R}^{(*)}} \text{ LP}
}{\vdash \dot{P}^{(*)} \leftrightarrow \dot{R}^{(*)}} \ \text{cut, } \mathbb{R}, \exists\text{L}
\qquad\square
$$

## B.3 Analytic Invariants

This section derives the analytic completeness axiom DRI (and its generalization DRI&), thus proving completeness for analytic (Noetherian) invariants and also for analytic postconditions.

### B.3.1 Differential Radical Invariants.
The differential radical invariants proof rule dRI derives from vdbx by turning the differential radical identity (3) into a provable vectorial Darboux equality.

Proof of Theorem 4.3. Let $e$ be an extended term satisfying both premises of the dRI proof rule and let $\mathbf{e}$ be the vector of extended terms with components $\mathbf{e}_i \stackrel{\text{def}}{=} \dot{e}^{(i-1)}$ for $i = 1, 2, \ldots, N$. The derivation starts by setting up the premise for an application of derived rule vdbx. In the first step, axiom DX is used to assume that the domain constraint $Q$ is true initially. On the left premise after the cut, arithmetic equivalence $\bigwedge_{i=0}^{N-1} \dot{e}^{(i)} = 0 \leftrightarrow \mathbf{e} = 0$ is used to rewrite the succedent to the left premise of dRI. On the right premise, monotonicity M['] strengthens the postcondition to $\mathbf{e} = 0$:

$$
\dfrac{
\dfrac{\Gamma, Q \vdash \bigwedge_{i=0}^{N-1} \dot{e}^{(i)} = 0}{\Gamma, Q \vdash \mathbf{e} = 0} \ \mathbb{R}
\qquad
\dfrac{\mathbf{e} = 0 \vdash [x' = f(x) \,\&\, Q]\mathbf{e} = 0}{\mathbf{e} = 0 \vdash [x' = f(x) \,\&\, Q]e = 0} \ \text{M[']}
}{
\dfrac{\Gamma, Q \vdash [x' = f(x) \,\&\, Q]e = 0}{\Gamma \vdash [x' = f(x) \,\&\, Q]e = 0} \ \text{DX}
} \ \text{cut}
$$

Continuing from the right premise, the component-wise Lie derivative of $\mathbf{e}$ is defined as $(\dot{\mathbf{e}})_i = \mathcal{L}_{f(x)}(\mathbf{e}_i) = \dot{e}^{(i)}$. The vector $\dot{\mathbf{e}}$ will be obtained from $\mathbf{e}$ by matrix multiplication with an $N \times N$ extended term cofactor matrix $G$ with 1 on its superdiagonal, and the $g_i$ cofactors in the last row:

$$
G = \begin{pmatrix}
0 & 1 & 0 & \ldots & 0 \\
0 & 0 & \ddots & \ddots & \vdots \\
\vdots & \vdots & \ddots & \ddots & 0 \\
0 & 0 & \ldots & 0 & 1 \\
g_0 & g_1 & \ldots & g_{N-2} & g_{N-1}
\end{pmatrix}, \quad
\mathbf{e} = \begin{pmatrix}
e \\
\dot{e}^{(1)} \\
\vdots \\
\dot{e}^{(N-2)} \\
\dot{e}^{(N-1)}
\end{pmatrix}, \quad
\dot{\mathbf{e}} = \begin{pmatrix}
\dot{e}^{(1)} \\
\dot{e}^{(2)} \\
\vdots \\
\dot{e}^{(N-1)} \\
\dot{e}^{(N)}
\end{pmatrix}
$$

The vectorial equation $\dot{\mathbf{e}} = G\mathbf{e}$ is provably equivalent to the equation $\dot{e}^{(N)} = \sum_{i=0}^{N-1} g_i \dot{e}^{(i)}$. To see this, note that for indices $1 \leq i < N$, matrix multiplication yields:

$$
(\dot{\mathbf{e}})_i = \dot{e}^{(i)} = (\mathbf{e})_{i+1} = (G\mathbf{e})_i
$$

Therefore, all but the final component-wise equality are trivially valid and prove by $\mathbb{R}$. The remaining (non-trivial) equation for $i = N$ is $(\dot{\mathbf{e}})_N = (G\mathbf{e})_N$. The LHS of this equation simplifies with $(\dot{\mathbf{e}})_N = \dot{e}^{(N)}$, while the RHS simplifies by matrix multiplication to:

$$(G\mathbf{e})_N = \sum_{i=1}^{N} g_{i-1}(\mathbf{e})_i = \sum_{i=1}^{N} g_{i-1}\dot{e}^{(i-1)} = \sum_{i=0}^{N-1} g_i\dot{e}^{(i)}$$

Hence, real arithmetic equivalently turns the formula $\dot{\mathbf{e}} = G\mathbf{e}$ into the succedent of the right premise of rule dRI. An application of derived rule vdbx from Corollary 4.2 with cofactor matrix $G$ followed by rule $\mathbb{R}$ yields the remaining right premise of rule dRI, completing the derivation.

$$\text{vdbx}\frac{\mathbb{R}\dfrac{Q \vdash \dot{e}^{(N)} = \sum_{i=0}^{N-1} g_i\dot{e}^{(i)}}{Q \vdash \dot{\mathbf{e}} = G\mathbf{e}}}{\mathbf{e} = 0 \vdash [x' = f(x)\,\&\,Q]\mathbf{e} = 0} \qquad\qquad \square$$

The derivation of rule dRI uses a specific choice of cofactor matrix $G$ in rule vdbx to prove invariance of the equation $e = 0$. This suffices for analytic completeness because analytic formulas can always be normalized to a single equation in real arithmetic. However, such normalization may not yield the computationally most efficient way of proving an analytic invariant (see Example 7.10).

*B.3.2 Completeness for Analytic Invariants.* The analytic completeness axiom with semianalytic domain constraints DRI& from Theorem 6.10 is derived next, making use of LP$\mathbb{R}$ from Lemma 6.5. The completeness argument can be summarized by contrapositives: if the local progress formula $\dot{e}^{(*)} = 0$ is false in an initial state, then some higher Lie derivative of $e$ is non-zero and gives a definite (local) sign to the value of $e$, which, by LP$\mathbb{R}$ implies progress to $e \neq 0$. For completeness, axiom DRI& also handles the vacuous case where domain constraint $Q$ is false initially ($Q \rightarrow \dots$) and the stuck case where the domain constraint is true initially but cannot locally progress ($\dot{Q}^{(*)} \rightarrow \dots$).

PROOF OF THEOREM 6.10 (IMPLIES THEOREM 4.5). For formulas $Q$ formed from conjunctions and disjunctions of strict inequalities, $Q \rightarrow \dot{Q}^{(*)}$ is provable in real arithmetic, so axiom DRI follows as an arithmetical corollary of DRI&. The derivation of axiom DRI& starts by rewriting its LHS equivalently with axiom DX. This is followed by a series of equivalent propositional rewrites that simplify the logical structure of the succedent. The propositional steps are shown below, first pulling out the common implication $Q$ then the common conjunct $e = 0$ as antecedent assumptions.

$$\text{DX}\frac{\dfrac{\dfrac{Q, e = 0 \vdash \big([x' = f(x)\,\&\,Q]e = 0\big) \leftrightarrow \big(\dot{Q}^{(*)} \rightarrow \dot{e}^{(*)} = 0\big)}{Q \vdash \big(e = 0 \wedge [x' = f(x)\,\&\,Q]e = 0\big) \leftrightarrow \big(e = 0 \wedge (\dot{Q}^{(*)} \rightarrow \dot{e}^{(*)} = 0)\big)}}{\vdash \big(Q \rightarrow e = 0 \wedge [x' = f(x)\,\&\,Q]e = 0\big) \leftrightarrow \big(Q \rightarrow e = 0 \wedge (\dot{Q}^{(*)} \rightarrow \dot{e}^{(*)} = 0)\big)}}{\vdash [x' = f(x)\,\&\,Q]e = 0 \leftrightarrow \big(Q \rightarrow e = 0 \wedge (\dot{Q}^{(*)} \rightarrow \dot{e}^{(*)} = 0)\big)}$$

Next, a cut of the first-order formula $\exists y\, x{=}y$ proves trivially in real arithmetic and Skolemizing it with $\exists L$ yields an initial state assumption ($x{=}y$ for fresh variables $y$). To make use of this initial state assumption, the derivation continues with a classical case split on whether the semianalytic progress formula $\dot{Q}^{(*)}$ is true initially. The resulting premises are labeled ① (for the $\dot{Q}^{(*)}$ disjunct)

and ② (for the $\neg(\dot{Q}^{(*)})$ disjunct) and continued below.

$$
\begin{array}{c}
\text{①} \quad\quad \text{②} \\
\vee\text{L} \dfrac{x{=}y, Q, e = 0, \dot{Q}^{(*)} \vee \neg(\dot{Q}^{(*)}) \vdash ([x' = f(x) \,\&\, Q]e = 0) \leftrightarrow (\dot{Q}^{(*)} \to \dot{e}^{(*)} = 0)}{}\\
\text{cut} \dfrac{}{x{=}y, Q, e = 0 \vdash ([x' = f(x) \,\&\, Q]e = 0) \leftrightarrow (\dot{Q}^{(*)} \to \dot{e}^{(*)} = 0)}\\
\exists\text{L} \dfrac{}{\exists y\, x{=}y, Q, e = 0 \vdash ([x' = f(x) \,\&\, Q]e = 0) \leftrightarrow (\dot{Q}^{(*)} \to \dot{e}^{(*)} = 0)}\\
\text{cut, } \mathbb{R} \dfrac{}{Q, e = 0 \vdash ([x' = f(x) \,\&\, Q]e = 0) \leftrightarrow (\dot{Q}^{(*)} \to \dot{e}^{(*)} = 0)}
\end{array}
$$

The premise ② corresponds to the case where solutions are *stuck* in the initial state because no local progress in the domain constraint $Q$ is possible. Topologically, this corresponds to the situation where initial states are on the boundary of the set characterized by $Q$ (and also in $Q$)[9] but the ODE locally leaves $Q$. Since $e = 0$ is already true in this stuck state, it trivially remains true for all solutions staying in domain constraint $Q$. The derivation from ② starts with a propositional simplification of the succedent since its RHS is vacuously equivalent to *true* by assumption $\neg(\dot{Q}^{(*)})$. The local progress characterization axiom LP equivalently rewrites the sub-formula $\dot{Q}^{(*)}$ to local progress for $Q$ before axiom $\langle\cdot\rangle$ unfolds the $\bigcirc$ modality turning it into a box modality formula.

$$
\begin{array}{c}
\dfrac{x{=}y, e = 0, [x' = f(x) \,\&\, Q \vee x = y]x = y \vdash [x' = f(x) \,\&\, Q]e = 0}{}\\
\langle\cdot\rangle \dfrac{}{x{=}y, e = 0, \neg(\langle x' = f(x) \,\&\, Q\rangle \bigcirc) \vdash [x' = f(x) \,\&\, Q]e = 0}\\
\text{LP} \dfrac{}{x{=}y, e = 0, \neg(\dot{Q}^{(*)}) \vdash [x' = f(x) \,\&\, Q]e = 0}\\
\mathbb{R} \dfrac{}{x{=}y, e = 0, \neg(\dot{Q}^{(*)}) \vdash ([x' = f(x) \,\&\, Q]e = 0) \leftrightarrow (\dot{Q}^{(*)} \to \dot{e}^{(*)} = 0)}
\end{array}
$$

By axiom V, the constant assumption $e(y) = 0$ (with $y$ in place of $x$) strengthens the postcondition of the antecedent box modality to $e = 0$ using the provable arithmetic formula $e(y) = 0 \wedge x = y \to e = 0$. A subsequent DMP, dW step finishes the proof using the propositional tautology $Q \to Q \vee x = y$.

$$
\begin{array}{c}
* \\
\text{DMP, dW} \dfrac{\dfrac{Q \vdash Q \vee x = y}{[x' = f(x) \,\&\, Q \vee x = y]e = 0 \vdash [x' = f(x) \,\&\, Q]e = 0}}{}\\
\text{V} \dfrac{}{x{=}y, e = 0, [x' = f(x) \,\&\, Q \vee x = y]x = y \vdash [x' = f(x) \,\&\, Q]e = 0}
\end{array}
$$

From premise ①, the succedent propositionally simplifies to $([x' = f(x) \,\&\, Q]e = 0) \leftrightarrow \dot{e}^{(*)} = 0$ by assumption $\dot{Q}^{(*)}$. The two directions of this simplified succedent are proved separately. In the "$\leftarrow$" direction, the derivation uses rule dRI by setting $N$ to the rank of extended term $e$, so that the succedent of its left premise is exactly $\dot{e}^{(*)} = 0$. The right premise resulting from dRI closes by real arithmetic, since $N$ is the rank of $e$, it must, by definition satisfy the provable rank identity (3).

$$
\begin{array}{c}
* \\
\mathbb{R} \dfrac{}{\vdash \dot{e}^{(N)} = \sum_{i=0}^{N-1} g_i \dot{e}^{(i)}}\\
\text{dRI} \dfrac{}{\dot{e}^{(*)} = 0 \vdash [x' = f(x) \,\&\, Q]e = 0}
\end{array}
$$

The derivation in the "$\to$" direction starts by reducing to the contrapositive statement with duality $\langle\cdot\rangle$ and propositional logical manipulation.

$$
\begin{array}{c}
\dfrac{x{=}y, Q, \dot{Q}^{(*)}, \neg(\dot{e}^{(*)} = 0) \vdash \langle x' = f(x) \,\&\, Q\rangle e \neq 0}{}\\
\neg\text{L, } \neg\text{R} \dfrac{}{x{=}y, Q, \dot{Q}^{(*)}, \neg\langle x' = f(x) \,\&\, Q\rangle e \neq 0 \vdash \dot{e}^{(*)} = 0}\\
\langle\cdot\rangle \dfrac{}{x{=}y, Q, \dot{Q}^{(*)}, [x' = f(x) \,\&\, Q]e = 0 \vdash \dot{e}^{(*)} = 0}
\end{array}
$$

---

[9]This situation is impossible for domain constraints $Q$ characterizing topologically open sets, which is the semantical reason for derived axiom DRI having a simpler RHS characterization than DRI&.

By derived axiom LP, the antecedent assumption $\dot{Q}^{(*)}$ is equivalently rewritten to local progress for $Q$ before Init (Corollary A.5) is used to strengthen it with the assumption $Q$. The final step rewrites the resulting negated differential radical formula in the antecedents to two progress formulas by (11) from Proposition B.1. Subsequent splitting with $\lor L$ yields two premises, which are abbreviated ③ (for disjunct $\dot{e}^{(*)} > 0$) and ④ (for disjunct $(-\dot{e})^{(*)} > 0$) respectively, and continued below.

$$
\begin{array}{c}
\hspace{4cm} \overline{\hspace{2cm}③\hspace{2cm}④\hspace{2cm}} \\
{}_{\lor L}\overline{x{=}y, \langle x' = f(x) \,\&\, Q\rangle x \neq y, \dot{e}^{(*)} > 0 \lor (-\dot{e})^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, Q\rangle e \neq 0} \\
{}_{\mathbb{R}}\overline{x{=}y, \langle x' = f(x) \,\&\, Q\rangle x \neq y, \neg(\dot{e}^{(*)} = 0) \vdash \langle x' = f(x) \,\&\, Q\rangle e \neq 0} \\
{}_{\text{Init}}\overline{x{=}y, Q, \langle x' = f(x) \,\&\, Q\rangle\bigcirc, \neg(\dot{e}^{(*)} = 0) \vdash \langle x' = f(x) \,\&\, Q\rangle e \neq 0} \\
{}_{\text{LP}}\overline{x{=}y, Q, \dot{Q}^{(*)}, \neg(\dot{e}^{(*)} = 0) \vdash \langle x' = f(x) \,\&\, Q\rangle e \neq 0}
\end{array}
$$

Continuing from ③, the assumption $\dot{e}^{(*)} > 0$ is rewritten with $\text{LP}_{>*}$ to obtain local progress for $e > 0$. Unfolding the $\bigcirc$ abbreviation, the uniqueness axiom Uniq combines the two diamond modality formulas in the antecedent:

$$
\begin{array}{c}
{}_{\text{Uniq}}\overline{\langle x' = f(x) \,\&\, Q \land (e > 0 \lor x = y)\rangle x \neq y \vdash \langle x' = f(x) \,\&\, Q\rangle e \neq 0} \\
\overline{\langle x' = f(x) \,\&\, Q\rangle x \neq y, \langle x' = f(x) \,\&\, e > 0 \lor x = y\rangle x \neq y \vdash \langle x' = f(x) \,\&\, Q\rangle e \neq 0} \\
{}_{\text{LP}_{>*}}\overline{\langle x' = f(x) \,\&\, Q\rangle x \neq y, \langle x' = f(x) \,\&\, e > 0\rangle\bigcirc \vdash \langle x' = f(x) \,\&\, Q\rangle e \neq 0} \\
\overline{x{=}y, \langle x' = f(x) \,\&\, Q\rangle x \neq y, \dot{e}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, Q\rangle e \neq 0}
\end{array}
$$

The succedent's domain constraint is strengthened to match the antecedent's using rule $\text{dRW}\langle\cdot\rangle$ since $Q \land (e > 0 \lor x = y) \rightarrow Q$ is a propositional tautology. The Kripke axiom $\text{K}\langle\cdot\rangle$ reduces the succedent to the box modality, after which the proof finishes with a dW step because the formula $e > 0 \lor x = y$ in the domain constraint implies the succedent by real arithmetic.

$$
\begin{array}{c}
{}_{\mathbb{R}}\overline{\hspace{3cm}*\hspace{3cm}} \\
{}_{\mathbb{R}}\overline{Q \land (e > 0 \lor x = y) \vdash (x \neq y \rightarrow e \neq 0)} \\
{}_{\text{dW}}\overline{\vdash [x' = f(x) \,\&\, Q \land (e > 0 \lor x = y)](x \neq y \rightarrow e \neq 0)} \\
{}_{\text{K}\langle\cdot\rangle}\overline{\langle x' = f(x) \,\&\, Q \land (e > 0 \lor x = y)\rangle x \neq y \vdash \langle x' = f(x) \,\&\, Q \land (e > 0 \lor x = y)\rangle e \neq 0} \\
{}_{\text{dRW}\langle\cdot\rangle}\overline{\langle x' = f(x) \,\&\, Q \land (e > 0 \lor x = y)\rangle x \neq y \vdash \langle x' = f(x) \,\&\, Q\rangle e \neq 0}
\end{array}
$$

The remaining premise ④ follows similarly, except that the progress formula $(-\dot{e})^{(*)} > 0$ enables the cut $\langle x' = f(x) \,\&\, -e > 0\rangle\bigcirc$ which leads to the same postcondition $e \neq 0$ in the succedent. □

## B.4 Completeness for Semianalytic Invariants with Semianalytic Evolution Domains

The following generalized version of rule sAI from Theorem 6.8 additionally handles evolution domain constraints. It derives from derived rule rI& and derived axiom LP.

THEOREM B.4 (SEMIANALYTIC INVARIANTS WITH SEMIANALYTIC DOMAIN CONSTRAINTS). *The semi-analytic invariant proof rule with semianalytic domain constraints sAI& derives from RI&, Dadj, Cont, Uniq for semianalytic formulas $P, Q$.*

$$
\text{sAI\&} \quad \frac{P, Q, \dot{Q}^{(*)} \vdash \dot{P}^{(*)} \quad \neg P, Q, \dot{Q}^{-(*)} \vdash (\neg\dot{P})^{-(*)}}{P \vdash [x' = f(x) \,\&\, Q]P}
$$

PROOF (IMPLIES THEOREM 6.8). Rule sAI& derives from rule rI& derived in Corollary A.8 and the characterization of semianalytic local progress LP derived in Theorem 6.6. The $x{=}y$ assumptions provided by rI& are used to convert between local progress modalities and the semianalytic progress formulas by LP, but, by weakening, $x{=}y$ can be elided again in the premises of sAI&. □

Recalling the earlier discussion for derived rule rI&, axiom V can be used, as usual, to keep *constant* context assumptions that do not depend on variables $x$ for the ODEs $x' = f(x)$ in rule sAI&, because it immediately derives from rI&, which supports constant contexts. The proof rule sAI& is complete for invariance properties. This is proved syntactically, enabling complete disproofs of invariance. The completeness of sAI from Theorem 6.9 follows as a special case, where $Q \equiv \textit{true}$.

THEOREM B.5 (SEMIANALYTIC INVARIANT COMPLETENESS WITH SEMIANALYTIC DOMAINS). *The semianalytic invariant axiom with semianalytic domain constraints SAI& derives from RI&, Dadj, Cont, Uniq for semianalytic formulas $P, Q$.*

$$\text{SAI\&} \quad \forall x \left( P \rightarrow [x' = f(x) \,\&\, Q]P \right) \leftrightarrow \underbrace{\forall x \left( P \wedge Q \wedge \dot{Q}^{(*)} \rightarrow \dot{P}^{(*)} \right)}_{\textcircled{a}} \wedge \underbrace{\forall x \left( \neg P \wedge Q \wedge \dot{Q}^{-(*)} \rightarrow (\dot{\neg P})^{-(*)} \right)}_{\textcircled{b}}$$

PROOF (IMPLIES THEOREM 6.9). The left and right conjunct on the RHS of SAI& are abbreviated ⓐ and ⓑ respectively. The "←" direction derives by sAI&. The antecedents ⓐ and ⓑ are first-order formulas quantified over $x$, the variables evolved by the ODE $x' = f(x)$. They are kept as constant context in the antecedents of the premises when applying rule sAI& and later instantiated by ∀L.

$$
\begin{array}{c}
\dfrac{
\dfrac{*}{\overset{\text{∀L, →L}}{\textcircled{a}, P, Q, \dot{Q}^{(*)} \vdash \dot{P}^{(*)}}} \qquad
\dfrac{*}{\overset{\text{∀L, →L}}{\textcircled{b}, \neg P, Q, \dot{Q}^{-(*)} \vdash (\dot{\neg P})^{-(*)}}}
}{
\dfrac{\textcircled{a}, \textcircled{b}, P \vdash [x' = f(x) \,\&\, Q]P}{\textcircled{a}, \textcircled{b} \vdash \forall x \left( P \rightarrow [x' = f(x) \,\&\, Q]P \right)}
}
\end{array}
\quad
\begin{array}{l}
\text{sAI\&} \\[4pt]
\text{∀R, →R}
\end{array}
$$

In the "→" direction, the derivation proceeds by contraposition in both cases after ∧R. For ⓑ, the derived invariant reflection axiom (rfl) is used to syntactically turn the invariance assumption for the forwards ODE into an invariance assumption for the backwards ODE.

$$
\dfrac{
\forall x \left( P \rightarrow [x' = f(x) \,\&\, Q]P \right) \vdash \textcircled{a}
\qquad
\dfrac{\forall x \left( \neg P \rightarrow [x' = -f(x) \,\&\, Q]\neg P \right) \vdash \textcircled{b}}{\forall x \left( P \rightarrow [x' = f(x) \,\&\, Q]P \right) \vdash \textcircled{b}} \; \text{rfl}
}{
\forall x \left( P \rightarrow [x' = f(x) \,\&\, Q]P \right) \vdash \textcircled{a} \wedge \textcircled{b}
} \; \text{∧R}
$$

Continuing from the left premise (with ⓐ in its succedent), standard logical manipulation is used to dualize both sides of the sequent. The ∃L step Skolemizes the existential in the antecedent, with the resulting $x$ used to witness the (then) existentially quantified succedent with ∃R:

$$
\begin{array}{c}
\dfrac{
\dfrac{
\dfrac{
P, Q, \dot{Q}^{(*)}, \neg(\dot{P}^{(*)}) \vdash \langle x' = f(x) \,\&\, Q \rangle \neg P
}{
P, Q, \dot{Q}^{(*)}, \neg(\dot{P}^{(*)}) \vdash \exists x \left( P \wedge \langle x' = f(x) \,\&\, Q \rangle \neg P \right)
}
}{
\exists x \left( P \wedge Q \wedge \dot{Q}^{(*)} \wedge \neg(\dot{P}^{(*)}) \right) \vdash \exists x \left( P \wedge \langle x' = f(x) \,\&\, Q \rangle \neg P \right)
}
}{
\forall x \left( P \rightarrow [x' = f(x) \,\&\, Q]P \right) \vdash \forall x \left( P \wedge Q \wedge \dot{Q}^{(*)} \rightarrow \dot{P}^{(*)} \right)
}
\end{array}
\quad
\begin{array}{l}
\text{∃R, ∧R} \\[6pt]
\text{∃L} \\[6pt]
\langle \cdot \rangle, \neg\text{L}, \neg\text{R}
\end{array}
$$

Next, an initial state assumption $x=y$ is introduced by a cut, ℝ followed by ∃L to Skolemize the resulting existential quantifier. The antecedent assumption $\neg(\dot{P}^{(*)})$ is replaced with $(\dot{\neg P})^{(*)}$ equivalently, by Proposition B.2. Both local progress formulas in the antecedents are then replaced equivalently with the local progress modalities using the derived axiom LP.

$$
\begin{array}{c}
\dfrac{
\dfrac{
\dfrac{
\dfrac{
x=y, P, Q, \langle x' = f(x) \,\&\, Q \rangle \bigcirc, \langle x' = f(x) \,\&\, \neg P \rangle \bigcirc \vdash \langle x' = f(x) \,\&\, Q \rangle \neg P
}{
x=y, P, Q, \dot{Q}^{(*)}, (\dot{\neg P})^{(*)} \vdash \langle x' = f(x) \,\&\, Q \rangle \neg P
}
}{
x=y, P, Q, \dot{Q}^{(*)}, \neg(\dot{P}^{(*)}) \vdash \langle x' = f(x) \,\&\, Q \rangle \neg P
}
}{
\exists y\, x=y, P, Q, \dot{Q}^{(*)}, \neg(\dot{P}^{(*)}) \vdash \langle x' = f(x) \,\&\, Q \rangle \neg P
}
}{
P, Q, \dot{Q}^{(*)}, \neg(\dot{P}^{(*)}) \vdash \langle x' = f(x) \,\&\, Q \rangle \neg P
}
\end{array}
\quad
\begin{array}{l}
\text{LP} \\[6pt]
\mathbb{R} \\[6pt]
\text{∃L} \\[6pt]
\text{cut}, \mathbb{R}
\end{array}
$$

By Init from Corollary A.5, local progress for $Q$ is strengthened, while $\bigcirc$ can only be unfolded for $\neg P$. The two resulting diamond modality formulas are combined with Uniq:

$$
\text{Init} \dfrac{\text{Uniq} \dfrac{\langle x' = f(x) \,\&\, Q \wedge (\neg P \vee x = y)\rangle x \neq y \vdash \langle x' = f(x) \,\&\, Q \rangle \neg P}{P, \langle x' = f(x) \,\&\, Q \rangle x \neq y, \langle x' = f(x) \,\&\, \neg P \vee x = y \rangle x \neq y \vdash \langle x' = f(x) \,\&\, Q \rangle \neg P}}{x{=}y, P, Q, \langle x' = f(x) \,\&\, Q \rangle \bigcirc, \langle x' = f(x) \,\&\, \neg P \rangle \bigcirc \vdash \langle x' = f(x) \,\&\, Q \rangle \neg P}
$$

With a $K\langle\cdot\rangle$, dW step, the diamond modality in the antecedent strengthens to $\neg P$ in its post-condition with the propositional tautology $Q \wedge (\neg P \vee x = y) \to (x \neq y \to \neg P)$. A dRW$\langle\cdot\rangle$ step completes the proof using the propositional tautology $Q \wedge (\neg P \vee x = y) \to Q$.

$$
\text{K}\langle\cdot\rangle, \text{dW} \dfrac{\text{dRW}\langle\cdot\rangle \dfrac{*}{\langle x' = f(x) \,\&\, Q \wedge (\neg P \vee x = y)\rangle \neg P \vdash \langle x' = f(x) \,\&\, Q \rangle \neg P}}{\langle x' = f(x) \,\&\, Q \wedge (\neg P \vee x = y)\rangle x \neq y \vdash \langle x' = f(x) \,\&\, Q \rangle \neg P}
$$

The remaining derivation from the right premise (with ⓑ in its succedent) is similar using local progress for the already reflected backwards differential equations instead. □

## C HYBRID PROGRAMS

This appendix is devoted to proving Corollary 4.6. The syntax of hybrid programs and the axioms of dL for handling the hybrid program operators are recalled [29, 32] below. Readers are referred to the literature [29, 32] for a complete definition of hybrid program semantics.

The syntax of hybrid programs $\alpha, \beta$ is given by the following grammar. The formula $Q$ is semianalytic in both tests $?Q$ and in evolution domain constraints of ODEs $x' = f(x) \,\&\, Q$:

$$
\alpha, \beta ::= x := e \mid ?Q \mid x' = f(x) \,\&\, Q \mid \alpha \cup \beta \mid \alpha; \beta \mid \alpha^* \tag{12}
$$

The following dL axioms are sound for reasoning about hybrid programs [32]:

THEOREM C.1 (HYBRID PROGRAM AXIOMS [32]). *The following are sound axioms of* dL.

[:=] $[x := e]\phi(x) \leftrightarrow \phi(e)$    (e free for $x$ in $\phi$)    [;] $[\alpha; \beta]\phi \leftrightarrow [\alpha][\beta]\phi$

[?] $[?Q]\phi \leftrightarrow (Q \to \phi)$                                    [*] $[\alpha^*]\phi \leftrightarrow \phi \wedge [\alpha][\alpha^*]\phi$

[∪] $[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \wedge [\beta]\phi$                        I $[\alpha^*]\phi \leftrightarrow \phi \wedge [\alpha^*](\phi \to [\alpha]\phi)$

The loop induction rule derives from induction axiom I using Gödel's generalization rule G [29]:

$$
\text{loop} \quad \dfrac{\phi \vdash [\alpha]\phi}{\phi \vdash [\alpha^*]\phi}
$$

Corollary 4.6 is proved using the equivalent characterization of future truth of analytic formulas along ODEs from Theorem 4.5. It applies to the fragment of dL programs generated by the grammar (12), where formula $Q$ in tests and domain constraints are negations of analytic formulas (so $d \neq 0$ for some extended term $d$). The loop-free fragment further removes the $\alpha^*$ clause from (12).

The set of extended terms always forms a ring because the $+, \cdot$ operations are interpreted as the usual real-valued addition and multiplication and hence obey the ring axioms [6] for $\mathbb{R}$. The extended term language is said to be *Noetherian* if its corresponding ring of extended terms is Noetherian. Similar to the computable differential radicals condition (R), an algorithm is assumed that decides (and proves) ideal membership in the ring of extended terms.

In particular, polynomial term languages without extensions are Noetherian and have decidable ideal membership. Extended term languages are not necessarily Noetherian, even if all additional

fixed function symbols are Noetherian functions. For example, extended term language (1), even only with exp, is not Noetherian [40, Remark 1.4.2].

PROOF OF COROLLARY 4.6. The analytic formula $P$ is provably equivalent in real arithmetic to a formula $e = 0$ for some extended term $e$ by normalizing with the provable arithmetic equivalences $e = 0 \wedge \tilde{e} = 0 \leftrightarrow e^2 + \tilde{e}^2 = 0$ and $e = 0 \vee \tilde{e} = 0 \leftrightarrow e\tilde{e} = 0$. Assume without loss of generality that it is already written in this form (and accordingly for the negative analytic formulas in $\alpha$).

Following [29, Theorem 1], the proof proceeds by structural induction on the form of $\alpha$, showing that for some (computable) extended term $\tilde{e}$, the equivalence $[\alpha]e = 0 \leftrightarrow \tilde{e} = 0$ is derivable in dL.

- Case $x' = f(x) \,\&\, d \neq 0$. The formula $d \neq 0$ is a strict inequality so Theorem 4.5 derives $[x' = f(x) \,\&\, d \neq 0]e = 0 \leftrightarrow (d \neq 0 \rightarrow \dot{e}^{(*)} = 0)$. Let $N$ be the rank of $e$ so that $\dot{e}^{(*)} = 0$ expands to $\bigwedge_{i=0}^{N-1} \dot{e}^{(i)} = 0$ and let $\tilde{e} = d(\sum_{i=0}^{N-1}(\dot{e}^{(i)})^2)$, giving the provable real arithmetic equivalence $(d \neq 0 \rightarrow \dot{e}^{(*)} = 0) \leftrightarrow \tilde{e} = 0$. Rewriting with this derives in dL the equivalence:

$$[x' = f(x) \,\&\, d \neq 0]e = 0 \leftrightarrow \tilde{e} = 0$$

- Case $x := e$. By axiom [:=], $[x := e]\tilde{e}(x) = 0 \leftrightarrow \tilde{e}(e) = 0$ derives and $\tilde{e}(e)$ is an extended term.
- Case $?d \neq 0$. By axiom [?], $[?d \neq 0]e = 0 \leftrightarrow (d \neq 0 \rightarrow e = 0)$ derives. Rewriting with the provable real arithmetic equivalence $(d \neq 0 \rightarrow e = 0) \leftrightarrow de = 0$ derives the equivalence:

$$[?d \neq 0]e = 0 \leftrightarrow de = 0$$

- Case $\alpha \cup \beta$. By axiom [∪], $[\alpha \cup \beta]e = 0 \leftrightarrow [\alpha]e = 0 \wedge [\beta]e = 0$ derives. By the induction hypothesis on $\alpha, \beta$, the equivalences $[\alpha]e = 0 \leftrightarrow \tilde{e}_1 = 0$ and $[\beta]e = 0 \leftrightarrow \tilde{e}_2 = 0$ derive for some extended terms $\tilde{e}_1, \tilde{e}_2$. Moreover, $\tilde{e}_1 = 0 \wedge \tilde{e}_2 = 0 \leftrightarrow \tilde{e}_1^2 + \tilde{e}_2^2 = 0$ is provable in real arithmetic. Rewriting with the derived equivalences derives the equivalence:

$$[\alpha \cup \beta]e = 0 \leftrightarrow \tilde{e}_1^2 + \tilde{e}_2^2 = 0$$

- Case $\alpha; \beta$. By axiom [;], $[\alpha; \beta]e = 0 \leftrightarrow [\alpha][\beta]e = 0$ derives. By the induction hypothesis on $\beta$, the equivalence $[\beta]e = 0 \leftrightarrow \tilde{e}_2 = 0$ derives for some extended term $\tilde{e}_2$. Rewriting with this equivalence derives $[\alpha; \beta]e = 0 \leftrightarrow [\alpha]\tilde{e}_2 = 0$. By the induction hypothesis on $\alpha$, the equivalence $[\alpha]\tilde{e}_2 = 0 \leftrightarrow \tilde{e}_1 = 0$ derives for some extended term $\tilde{e}_1$. Rewriting with the chain of derived equivalences derives the equivalence:

$$[\alpha; \beta]e = 0 \leftrightarrow \tilde{e}_1 = 0$$

- Case $\alpha^*$. This case crucially requires that the extended term language is Noetherian. First, construct the sequence of terms $\tilde{e}_i$ defined inductively with $\tilde{e}_0 \overset{\text{def}}{=} e$ and $\tilde{e}_{i+1}$ is the term satisfying the derived equivalence $[\alpha]\tilde{e}_i = 0 \leftrightarrow \tilde{e}_{i+1} = 0$ obtained by applying the induction hypothesis on $\alpha$ with postcondition $\tilde{e}_i = 0$ for $i = 0, 1, 2, \ldots$. Since the term language is assumed to be Noetherian, the following ascending chain of ideals stabilizes:

$$(\tilde{e}_0) \subseteq (\tilde{e}_0, \tilde{e}_1) \subseteq (\tilde{e}_0, \tilde{e}_1, \tilde{e}_2) \subseteq \cdots$$

Moreover, by decidable ideal membership for the extended term language, there is a (smallest) computable $k$ such that $\tilde{e}_k$ satisfies the following provable identity, with cofactor terms $g_i$:

$$\tilde{e}_k = \sum_{i=0}^{k-1} g_i \tilde{e}_i \tag{13}$$

The following equivalence is provable by real arithmetic: $\sum_{i=0}^{k-1} \tilde{e}_i^2 = 0 \leftrightarrow \bigwedge_{i=0}^{k-1} \tilde{e}_i = 0$. Thus, to derive the equivalence $[\alpha^*]e = 0 \leftrightarrow \sum_{i=0}^{k-1} \tilde{e}_i^2 = 0$, it suffices to show that the equivalence $[\alpha^*]e = 0 \leftrightarrow \bigwedge_{i=0}^{k-1} \tilde{e}_i = 0$ is derivable. The two directions of this claim are shown separately:

"→" This direction is straightforward using $k$ times the iteration axiom $[^*]$ together with derived axiom $[\cdot]\wedge$. By construction, the formulas $[\alpha]\tilde{e}_i = 0$ are provably equivalent to $\tilde{e}_{i+1} = 0$ using derived equivalences, which derives the required implication:

$$
\begin{array}{c}
\ast \\
\hline
\tilde{e}_0 = 0 \wedge \tilde{e}_1 = 0 \wedge \tilde{e}_2 = 0 \wedge \cdots \wedge \tilde{e}_{k-1} = 0 \vdash \bigwedge_{i=0}^{k-1} \tilde{e}_i = 0 \\
\hline
e = 0 \wedge [\alpha]e = 0 \wedge [\alpha][\alpha]e = 0 \wedge \cdots \wedge \underbrace{[\alpha]\ldots[\alpha]}_{k-1 \text{ times}} e = 0 \vdash \bigwedge_{i=0}^{k-1} \tilde{e}_i = 0
\end{array}
$$

$$
\begin{array}{c}
[^*],[\cdot]\wedge \quad\quad\quad\quad\quad\quad\quad\quad\quad \cdots \\
\hline
[^*],[\cdot]\wedge \quad e = 0 \wedge [\alpha]e = 0 \wedge [\alpha][\alpha][\alpha^*]e = 0 \vdash \bigwedge_{i=0}^{k-1} \tilde{e}_i = 0 \\
\hline
[^*],[\cdot]\wedge \quad\quad e = 0 \wedge [\alpha][\alpha^*]e = 0 \vdash \bigwedge_{i=0}^{k-1} \tilde{e}_i = 0 \\
\hline
[^*] \quad\quad\quad\quad\quad [\alpha^*]e = 0 \vdash \bigwedge_{i=0}^{k-1} \tilde{e}_i = 0
\end{array}
$$

"←" The postcondition of the box modality is strengthened to $\bigwedge_{i=0}^{k-1} \tilde{e}_i = 0$ by monotonicity with K, G, recalling that $\tilde{e}_0 \overset{\text{def}}{=} e$, so $\bigwedge_{i=0}^{k-1} \tilde{e}_i = 0 \rightarrow e = 0$ is a propositional tautology. Subsequently, the loop rule is used to prove $\bigwedge_{i=0}^{k-1} \tilde{e}_i = 0$ is a loop invariant of $\alpha^*$:

$$
\begin{array}{c}
\bigwedge_{i=0}^{k-1} \tilde{e}_i = 0 \vdash [\alpha] \bigwedge_{i=0}^{k-1} \tilde{e}_i = 0 \\
\hline
\text{loop} \quad \bigwedge_{i=0}^{k-1} \tilde{e}_i = 0 \vdash [\alpha^*] \bigwedge_{i=0}^{k-1} \tilde{e}_i = 0 \\
\hline
\text{K, G} \quad \bigwedge_{i=0}^{k-1} \tilde{e}_i = 0 \vdash [\alpha^*]e = 0
\end{array}
$$

By axiom $[\cdot]\wedge$ and $\wedge$R, each conjunct of the postcondition (indexed by $0 \le i \le k-1$) is proved separately. By construction, each $[\alpha]\tilde{e}_i = 0$ is provably equivalent to $\tilde{e}_{i+1} = 0$:

$$
\begin{array}{c}
\ast \\
\hline
\mathbb{R},\wedge\text{R} \quad \bigwedge_{i=0}^{k-1} \tilde{e}_i = 0 \vdash \bigwedge_{i=0}^{k-1} \tilde{e}_{i+1} = 0 \\
\hline
\bigwedge_{i=0}^{k-1} \tilde{e}_i = 0 \vdash \bigwedge_{i=0}^{k-1} [\alpha]\tilde{e}_i = 0 \\
\hline
[\cdot]\wedge \quad \bigwedge_{i=0}^{k-1} \tilde{e}_i = 0 \vdash [\alpha] \bigwedge_{i=0}^{k-1} \tilde{e}_i = 0
\end{array}
$$

The premises for indices $0 \le i < k-1$ all close trivially because $\tilde{e}_{i+1} = 0$ is already in the antecedent. The last premise for index $i = k-1$ has succedent $\tilde{e}_k = 0$. However, this follows (by construction and $\mathbb{R}$) from the antecedent using the provable identity (13).  □