Differential Equation Axiomatization

The Impressive Power of Differential Ghosts

André Platzer
Computer Science Department
Carnegie Mellon University
aplatzer@cs.cmu.edu

Yong Kiam Tan
Computer Science Department
Carnegie Mellon University
yongkiat@cs.cmu.edu

Abstract

We prove the completeness of an axiomatization for differential equation invariants. First, we show that the differential equation axioms in differential dynamic logic are complete for all algebraic invariants. Our proof 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 enables its analysis.

We then show that extending the axiomatization with existence and uniqueness axioms makes it complete for all local progress properties, and further extension with a real induction axiom makes it complete for all real arithmetic invariants. This yields a parsimonious axiomatization, which serves as the logical foundation for reasoning about invariants of differential equations. Moreover, our approach is purely axiomatic, and so the axiomatization is suitable for sound implementation in foundational theorem provers.

Keywords differential equation axiomatization, differential dynamic logic, differential ghosts

1 Introduction

Classically, differential equations are studied by analyzing their solutions. This is at odds with the fact that solutions are often much more complicated than the differential equations themselves. The stark difference between the simple local description as differential equations and the complex global behavior exhibited by solutions is fundamental to the descriptive power of differential equations.

Poincaré's qualitative study of differential equations crucially exploits this difference by deducing properties of solutions *directly from the differential equations*. This paper completes an important step in this enterprise by identifying the logical foundations for proving invariance properties of polynomial differential equations.

We exploit the differential equation axioms of differential dynamic logic (dL) [13, 15]. dL is a logic for deductive verification of hybrid systems that are modelled 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 [13, 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 our findings about differential equations to hybrid systems. The remaining practical challenge is to find succinct real arithmetic system invariants; any such invariant, once found, can be proved within our calculus.

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 impractical for most loops to reason about their global behavior by unfolding all possible iterations. Instead, the premier reasoning technique for loops is to study their loop invariants, i.e., properties that are preserved across each execution of the loop body.

Similarly, invariants of ODEs are real arithmetic formulas that describe subsets of the state space from which we cannot escape by continuously following the local dynamics specified by the ODEs. The three basic dL axioms for reasoning about such invariants are: (1) *differential invariants*, which prove simple invariants by analyzing their local (Lie) derivatives, (2) *differential cuts*, which refine the state space with additional provable invariants, and (3) *differential ghosts*, which add differential equations for new ghost variables to the existing system of differential equations.

We may relate these reasoning principles to their discrete loop counterparts: (1) corresponds to loop induction and analysis of 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, and should be adverse to analyzing it! However, just as discrete ghosts [11] allow the expression of new relationships between variables along execution of a program, differential ghosts that suitably co-evolve with the ODEs crucially allow the expression of new relationships along solutions to the differential equations. Unlike the case for discrete loops, differential cuts strictly increase the deductive power of differential invariants for proving invariants of ODEs; differential ghosts further increase this deductive power [14].

This paper has the following contributions:

1. We show that *all* algebraic invariants, i.e., where the invariant set is described by a formula formed from finite conjunctions and disjunctions of polynomial equations, are provable using *only* the three ODE principles outlined above.
2. We introduce two axioms internalizing the existence and uniqueness theorems for solutions of differential equations. We show that they suffice for reasoning about all *local progress* properties of ODEs for all real arithmetic formulas.
3. We introduce a real induction axiom that allows us to reduce invariance to local progress. The resulting calculus can prove *all* real arithmetic invariants of differential equations.

Just as discrete ghosts can make a program logic relatively complete [11], our first completeness result shows that differential ghosts do the same for algebraic invariants in dL. We extend the

LICS'18, Jul 9-12 , 2018, Oxford, UK
2018.

[1] In fact, this analogy can be made precise: dL also has a converse relative completeness theorem [13, Theorem 2] that reduces ODEs to discrete Euler approximation loops.

result to larger classes of hybrid programs, including, e.g., loops that switch between multiple different ODEs.

We note that there already exist prior, complete procedures for checking algebraic, and real arithmetic invariants of differential equations [7, 9]. Our result identifies a list of axioms that serve as a *logical foundation* from which these procedures can be implemented as derived rules. This logical approach allows us to precisely understand the underlying properties of differential equations that are needed for invariance reasoning. Our axiomatization is also *not limited* to invariance properties, and other qualitative properties such as local progress can also be proved with the axiomatization.

Finally, our axioms are a list of concrete formulas without any side conditions. This is crucial to make our axiomatization amenable to sound implementation and verification in foundational theorem provers [3, 6] using dL's uniform substitution calculus [15], and is in stark contrast to previous highly schematic procedures [7, 9].

Some of our results appear in a previous technical report [16]. We take a more elegant axiomatization here, which gives significantly simpler correctness proofs.

2 Background

This section briefly reviews the relevant continuous fragment of dL, and establishes the notational conventions that we will use in this paper. We refer readers to the literature [13, 15] and Appendix A for a complete exposition of dL, including its discrete fragment.

2.1 Syntax

Terms in dL are generated by the following grammar, where x is a variable, and c is a rational constant:

$$e ::= x \mid c \mid e_1 + e_2 \mid e_1 \cdot e_2$$

These terms correspond to polynomials over the variables under consideration. For the purposes of this paper, we write x to refer to a vector of variables $x_1, \ldots, x_n$, and we use $p(x), q(x)$ to stand for polynomial terms over these variables. When the variable context is clear, we write p, q without arguments instead. Vectors of polynomials are written in bold $\mathbf{p}, \mathbf{q}$, with $\mathbf{p}_i, \mathbf{q}_i$ for their i-th components.

The formulas of dL are given by the following grammar, where $\sim$ is a comparison operator $=, \geq, >$, and α is a hybrid program:

$$\phi ::= e_1 \sim e_2 \mid \phi_1 \land \phi_2 \mid \phi_1 \lor \phi_2 \mid \phi_1 \to \phi_2 \mid \neg\phi \mid \forall x\, \phi \mid \exists x\, \phi \mid [\alpha]\phi \mid \langle\alpha\rangle\phi$$

By appropriately normalizing terms, it is enough to assume that all the formulas of the form $e_1 \sim e_2$ have 0 on the right-hand side. We write $p \gtrsim 0$ if there is a free choice of $\gtrsim$ between $\geq$ or $>$. We define $p \lesssim 0 \overset{\text{def}}{\equiv} -p \gtrsim 0$, where $\lesssim$ stands for $\leq$ or $<$, and $\gtrsim$ is correspondingly chosen. Other logical connectives, such as $\leftrightarrow$ can be defined similarly. We write $P(x), Q(x)$ for first-order formulas of real arithmetic, i.e., formulas not containing the modal connectives. We drop the dependency on x when the variable context is clear. The modal formula $[\alpha]\phi$ is true iff ϕ is true after all transitions of α, and its dual $\langle\alpha\rangle\phi$ is true iff ϕ is true after some transition of α.

Hybrid programs α allow us to express both discrete and continuous dynamics. We shall primarily use the continuous fragment[2]:

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

We write $x' = f(x) \,\&\, Q$ for an autonomous vectorial ODE system in variables $x_1, \ldots, x_n$ where the RHS of the system for each x_i is a polynomial term $f_i(x)$. The evolution domain constraint Q is a formula of real arithmetic, which restricts the set of states in which we are allowed to continuously evolve. When $Q \equiv \mathit{true}$, we write $x' = f(x)$. We will use the following system, which is visualized in Fig. 1 as a running example:

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

Following our analogy in Section 1, solutions of $x' = f(x)$ must continuously (locally) follow its RHS, $f(x)$. We visualize this in Fig. 1 with directional arrows corresponding to the RHS of α_e evaluated at points on the plane. Even though the RHS of α_e are polynomials, its solutions, which must locally follow the arrows, already exhibit complex global behavior. In Fig. 1, we see, e.g., that all points (except the origin) globally evolve towards the unit circle.

[2]We only consider weak-test dL, where Q is a first-order formula of real arithmetic.

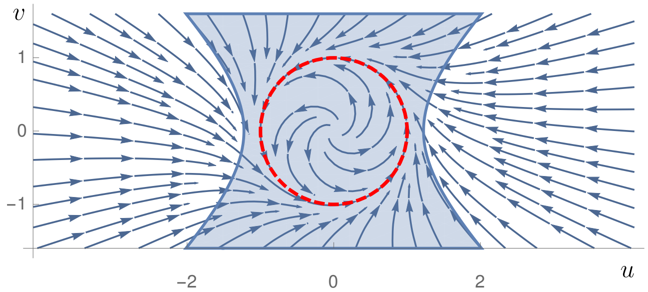

Figure 1. A visualization of α_e. The red dashed circle $u^2 + v^2 = 1$ is approached by solutions from all points except the origin. Both the circle and the blue region $u^2 \leq v^2 + \frac{3}{2}$ are invariants of the system.

2.2 Semantics

A state $\omega : \mathbb{V} \to \mathbb{R}$ assigns a real value to each variable in the (finite) set $\mathbb{V}$. We may let $\mathbb{V} = \{x_1, \ldots, x_n\}$ since we only need to consider the variables occurring in differential equations $x' = f(x)$. Hence, we shall also write states as n-tuples $\omega : \mathbb{R}^n$ where the i-th component is the value of x_i in that state.

Terms are given the usual interpretation in first-order real arithmetic with respect to a state. We write $\omega[\![e]\!]$ for the valuation of term e in state ω. The semantics of comparison operations and logical connectives (except the modal ones) are also defined in the standard way. We write $[\![\phi]\!]$ for the set of states in which ϕ is true. For example, $\omega \in [\![e_1 \leq e_2]\!]$ iff $\omega[\![e_1]\!] \leq \omega[\![e_2]\!]$, and $\omega \in [\![\phi_1 \land \phi_2]\!]$ iff $\omega \in [\![\phi_1]\!]$ and $\omega \in [\![\phi_2]\!]$.

Hybrid programs are interpreted as transition relations, $[\![\alpha]\!] \subseteq \mathbb{R}^n \times \mathbb{R}^n$, between states. In particular, the transition semantics of a system of ODEs is defined as:

$$(\omega, \nu) \in [\![x' = f(x) \,\&\, Q]\!] \text{ iff there is } T \geq 0 \text{ and a function}$$
$$\varphi : [0, T] \to \mathbb{R}^n \text{ with } \varphi(0) = \omega, \varphi(T) = \nu, \varphi \models x' = f(x) \,\&\, Q$$

The $\varphi \models x' = f(x) \,\&\, Q$ condition checks that φ is indeed a solution of the system $x' = f(x)$, and that $\varphi(\zeta) \in [\![Q]\!]$ for all $\zeta \in [0, T]$. Given any such solution φ, we may restrict its interval of definition to obtain a truncation $\varphi|_\zeta : [0, \zeta] \to \mathbb{R}^n$, where $\varphi|_\zeta(\tau) \overset{\text{def}}{=} \varphi(\tau)$ for all $\tau \in [0, \zeta]$. Since all such truncations are themselves solutions, we also have $(\omega, \varphi(\zeta)) \in [\![x' = f(x) \,\&\, Q]\!]$ for all $\zeta \in [0, T]$.

Finally, $\omega \in [\![[\alpha]\phi]\!]$ iff for all states ν such that $(\omega, \nu) \in [\![\alpha]\!]$, ϕ is true in ν. Dually, $\omega \in [\![\langle\alpha\rangle\phi]\!]$ iff there exists a state ν, where $(\omega, \nu) \in [\![\alpha]\!]$ and ϕ is true in ν.

Formulas P, where the formula $P \to [x' = f(x) \,\&\, Q]P$ is valid, are called *invariants* of the system $x' = f(x) \,\&\, Q$. Unfolding the semantics above, this means that from any initial state $\omega \in [\![P]\!]$, any solution φ from ω, which does not leave the evolution domain $[\![Q]\!]$, stays in $[\![P]\!]$ for its *entire duration*.

Returning to Fig. 1, we immediately identify several invariants. The unit circle, $u^2 + v^2 = 1$, is an equational invariant because the direction of flow on the circle is always tangential to the circle. The region described by $u^2 \le v^2 + \frac{3}{2}$ is also invariant. This is not immediately obvious, however, and requires a careful proof. The equilibrium point at the origin is also trivially invariant.

2.3 Differentials and Lie Derivatives

The *Lie derivative* of a polynomial p along $x' = f(x)$ is:

$$\mathcal{L}_{f(x)}(p) \stackrel{\text{def}}{=} \sum_{x_i} \frac{\partial p}{\partial x_i} f_i(x) = \nabla p \cdot f(x)$$

For polynomial differential equations and polynomials p, $\mathcal{L}_{f(x)}(p)$ is also a polynomial. We shall write $\dot{p}$ for $\mathcal{L}_{f(x)}(p)$, because $x' = f(x)$ will be clear from the context. We use $\mathcal{L}_{f(x)}(\cdot)$ only when considering Lie derivation as an operator. Note that $\mathcal{L}_{f(x)}(\cdot)$ satisfies the familiar sum and product rules of differentiation.

A calculus for reasoning about differential equations must suitably handle Lie derivatives. The uniform substitution calculus [15] for dL uses the differential, $(p)'$, and differential variables x'. As the notation suggests, $(p)'$ is closely related to $\dot{p}$. By the differential lemma [15, Lemma 35], along solutions to the system $x' = f(x)$, the value of the differential, $(p)'$, coincides exactly with that of the Lie derivative $\dot{p}$. This is internalized in dL by the differential effect axiom DE, and axioms for computing derivatives by axioms for differentials c',x',$+'$,$\cdot'$ [15, Lemmas 36-37]. Crucially, these axioms allow Lie derivation to be performed *purely syntactically* and mechanically. For this paper, we work directly with the Lie derivatives. Under the hood, the computation of these Lie derivatives is done using differentials and DE, as we show in Appendix A.2.

We write $\dot{p}^{(i)}$ for the *i-th Lie derivative of* p along $x' = f(x)$, where higher Lie derivatives are defined by iterating the Lie derivation operator. By the aforementioned closure property of polynomials under derivation, all of the higher Lie derivatives of p exist, and are also polynomials in the indeterminates x.

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

2.4 Axiomatization

The reasoning principles for differential equations in dL are stated as axioms in its uniform substitution calculus [15, Figure 3]. For ease of presentation in this paper, we shall work with a sequent calculus presentation, with derived rule versions of these principles. The derivation of these rules from the axioms is shown in Appendix A.2.

We assume a standard classical sequent calculus with all the usual rules for manipulating logical connectives and sequents, e.g., $\vee$L,$\exists$R, and cut. Since we are only reasoning about a single succedent, we gather all additional context in the antecedents as Γ. In addition, because the theory of first-order real arithmetic is decidable [2], we assume access to such a decision procedure, and we label steps with $\mathbb{R}$ whenever they follow as a consequence of first-order real arithmetic. We write $*$ to indicate a completed (closed) derivation.

Theorem 2.1 (Differential equation axiomatization [15])**.** *The following sound proof rules derive from the axioms of* dL*:*

$$\text{dI}_= \ \frac{\Gamma, Q \vdash p = 0 \qquad Q \vdash \dot{p} = 0}{\Gamma \vdash [x' = f(x) \,\&\, Q]p = 0}$$

$$\text{dI}_{\succsim} \ \frac{\Gamma, Q \vdash p \succsim 0 \qquad Q \vdash \dot{p} \ge 0}{\Gamma \vdash [x' = f(x) \,\&\, Q]p \succsim 0} \quad (\text{where } \succsim \text{ is either } \ge \text{ or } >)$$

$$\text{dC} \ \frac{\Gamma \vdash [x' = f(x) \,\&\, Q]C \qquad \Gamma \vdash [x' = f(x) \,\&\, Q \wedge C]P}{\Gamma \vdash [x' = f(x) \,\&\, Q]P}$$

$$\text{dW} \ \frac{Q \vdash P}{\Gamma \vdash [x' = f(x) \,\&\, Q]P}$$

$$\text{dG} \ \frac{\Gamma \vdash \exists y \, [x' = f(x), y' = a(x) \cdot y + b(x) \,\&\, Q]P}{\Gamma \vdash [x' = f(x) \,\&\, Q]P}$$

Differential invariants (dI) reduces questions about invariance of $p = 0, p \succsim 0$ to questions about their respective Lie derivatives. In this way, it reduces a global invariance property (along solutions of the ODE) to a question about its local Lie derivatives. We have only shown two instances ($\text{dI}_=$,$\text{dI}_{\succsim}$) of the more general dI rule [15] that we will need for this paper. These instances internalize the mean value theorem[3] (see Appendix A.2). Differential cut (dC) asserts that if we can separately prove that the systems never leaves C while staying in Q (the left premise), then we may additionally assume C when proving the postcondition P (the right premise).

Once we have sufficiently enriched the evolution domain using dI,dC, differential weakening (dW) allows us to remove the ODEs, and instead prove the postcondition P directly from the evolution domain constraint Q. In the same vein, the following derived rule and axiom from dL will be useful to manipulate postconditions:

$$\text{M}[\cdot] \ \frac{\phi_2 \vdash \phi_1 \qquad \Gamma \vdash [\alpha]\phi_2}{\Gamma \vdash [\alpha]\phi_1} \qquad [\cdot]\wedge \ [\alpha](\phi_1 \wedge \phi_2) \leftrightarrow [\alpha]\phi_1 \wedge [\alpha]\phi_2$$

The M[$\cdot$] monotonicity rule allows us to strengthen the postcondition to ϕ_2 if it implies ϕ_1. The $[\cdot]\wedge$ axiom allows us to prove conjunctive postconditions separately.

Even if dC increases the deductive power over dI, the deductive power increases even further [14] with the differential ghosts rule dG. It allows us to add a *fresh* variable y to the system of equations. The main soundness restriction of dG is that the new ODE must be linear[4] in y. This restriction is enforced by ensuring that $a(x)$, $b(x)$ do not mention y. For our purposes, we will allow $\mathbf{y}$ to be vectorial, i.e. we allow the existing differential equations to be extended by a system that is linear in a vector of variables $\mathbf{y}$. In this setting, $a(x)$ (resp. $b(x)$) is a matrix (resp. vector) of polynomials in x.

As mentioned, adding auxiliary differential ghost variables using dG crucially allows us to express new relationships between variables along the differential equations. The next section shows how dG can be used along with the rest of the rules to prove a class of invariants satisfying Darboux-type properties. We exploit this increased deductive power in full in later sections.

3 Darboux Polynomials

This section illustrates the use of dG in proving invariance properties involving Darboux polynomials [5]. A polynomial p is a

[3]Note that for rule $\text{dI}_{\succsim}$, we only require $\dot{p} \ge 0$ even for the $p > 0$ case.

[4]Linearity prevents the newly added equation from unsoundly restricting the duration of existence for solutions to the differential equations.

Darboux polynomial for the system $x' = f(x)$ iff it satisfies the polynomial identity $\dot{p} = gp$ for some polynomial cofactor g.

3.1 Darboux Equalities

We first recall the following useful notion from algebraic geometry:

Definition 3.1 (Ideal [2]). The *ideal* generated by the polynomials $p_1, \dots, p_s \in \mathbb{R}[x]$ is defined as the set of polynomials[5]:

$$(p_1, \dots, p_s) \overset{\text{def}}{=} \{\Sigma_{i=1}^{s} g_i p_i \ : \ g_i \in \mathbb{R}[x]\}$$

Let us assume that p satisfies the Darboux polynomial identity $\dot{p} = gp$. Taking Lie derivatives on both sides, we get:

$$\begin{aligned} \dot{p}^{(2)} &= \mathcal{L}_{f(x)}(\dot{p}) = \mathcal{L}_{f(x)}(gp) = \mathcal{L}_{f(x)}(g)p + \mathcal{L}_{f(x)}(p)g \\ &= \dot{g}p + \dot{p}g = (\dot{g} + g^2)p \in (p) \end{aligned}$$

By repeatedly taking Lie derivatives, it is easy to see that all higher Lie derivatives of p are contained in the ideal (p). Now, let us consider an initial state ω where p evaluates to $\omega[\![p]\!] = 0$, then we have:

$$\omega[\![\dot{p}]\!] = \omega[\![gp]\!] = \omega[\![g]\!] \cdot \omega[\![p]\!] = 0$$

Similarly, because every higher Lie derivative of a Darboux polynomial is contained in the ideal generated by p, all of them are simultaneously 0 in state ω. Thus, it should be the case[6] that $p = 0$ stays invariant along solutions to the ODE starting at ω. The question is how to prove it axiomatically.

In the first derivation below, we give a proof of invariance for $p = 0$ using dG. We explain the derivation in detail as it further illustrates the use of the surrounding proof calculus.

Lemma 3.2 (Darboux equalities are differential ghosts). *The proof rule for Darboux equalities derives from dG (and dI):*

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

Proof. Let ① denote the use of the premise of dbx, and ② abbreviate the right premise in the following derivation.

$$\dfrac{\dfrac{\dfrac{p{=}0 \vdash [x' = f(x),\, y' = -gy \,\&\, Q]py{=}0 \qquad ②}{p = 0,\, y \neq 0 \vdash [x' = f(x),\, y' = -gy \,\&\, Q](y \neq 0 \land py = 0)}\,[\cdot]\land,\land R}{p = 0 \vdash \exists y\, [x' = f(x),\, y' = -gy \,\&\, Q]p = 0}\,\text{M}[\cdot],\exists R}{p = 0 \vdash [x' = f(x) \,\&\, Q]p = 0}\,\text{dG}$$

In the first dG step, we introduce a new ghost variable y satisfying a carefully chosen differential equation $y' = -gy$ as a counterweight. Next, $\exists$R allows us to pick an initial value for y. We simply pick any $y \neq 0$. We then observe that in order to prove $p = 0$, it suffices to prove the stronger invariant $y \neq 0 \land py = 0$, so we use the monotonicity rule M[·] to strengthen the postcondition. Next, $[\cdot]\land,\land$R lets us prove each conjunct in the new postcondition separately.

Continuing on the left premise:

$$\dfrac{\dfrac{*}{p = 0 \vdash py = 0}\,\mathbb{R} \qquad \dfrac{① \qquad \dfrac{*}{\vdash gpy - gyp = 0}\,\mathbb{R}}{Q \vdash \dot{p}y - gyp = 0}\,\text{cut}}{p = 0 \vdash [x' = f(x),\, y' = -gy \,\&\, Q]py = 0}\,\text{dI}$$

We use dI to prove the equational invariant $py = 0$; its left premise is a consequence of real arithmetic. On the right premise, we compute the Lie derivative of py using the usual product rule as follows:

$$\mathcal{L}_{f(x),-gy}(py) = \mathcal{L}_{f(x),-gy}(p)y + p\mathcal{L}_{f(x),-gy}(y) = \dot{p}y - gyp$$

[5] $\mathbb{R}[x]$ denotes the ring of polynomials in indeterminates x.

[6] This requires the solutions to the ODEs to be analytic, which is the case here.

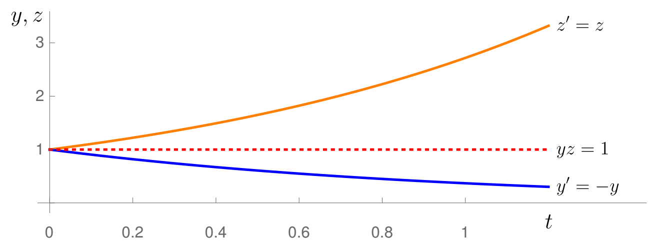

Figure 2. The differential ghost $z' = z$ (in orange) balances out $y' = -y$ (in blue) so that the value of yz (the red dotted line) remains constant at 1. The horizontal axis tracks the evolution of time.

We complete the derivation by cutting in the premise of dbx (①). Note that our choice of differential ghost $y' = -gy$ was precisely chosen so that the final arithmetic step closes trivially.

The remaining premise ② is:

$$y \neq 0 \vdash [x' = f(x),\, y' = -g(x)y \,\&\, Q]y \neq 0$$

Its proof continues using a second ghost $z' = gz$:

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{\vdash -(gy)z + y(gz) = 0}\,\mathbb{R}}{yz = 1 \vdash [x' = f(x),\, y' = -gy,\, z' = gz \,\&\, Q]yz = 1}\,\text{dI}}{y \neq 0 \vdash \exists z\, [x' = f(x),\, y' = -gy,\, z' = gz \,\&\, Q]y \neq 0}\,\text{M}[\cdot],\exists R}{y \neq 0 \vdash [x' = f(x),\, y' = -gy \,\&\, Q]y \neq 0}\,\text{dG}$$

This derivation is similar to the one for the previous premise. In the M[·],∃R step, we observe that if $y \neq 0$ initially, then there exists z such that $yz = 1$. Moreover, $yz = 1$ is sufficient to imply $y \neq 0$ in the postcondition. The differential ghost $z' = gz$ is chosen so that $yz = 1$ can be proved invariant *along the differential equation*. □

Fig. 2 illustrates the effect of the second ghost in the proof above for $g = -1$, where $y = 1, z = 1$ initially. Although y decays exponentially towards $y = 0$, the ghost z balances this by growing exponentially so that yz stays constant at its initial value 1.

3.2 Darboux Inequalities

Using a variation of the derivation proving Lemma 3.2, we can also derive invariant inequality properties for Darboux polynomials using dG. In fact, we will only require that p satisfies a Darboux *inequality* $\dot{p} \geq gp$ for some cofactor polynomial g.

Lemma 3.3 (Darboux inequalities are differential ghosts). *The proof rule for Darboux inequalities derives from dG (and dI,dC):*

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

Proof Summary (See Appendix C). The derivation is similar to the one used for Lemma 3.2; we use the same first choice of differential ghost $y' = -gy$. However, instead of $y \neq 0 \land py = 0$, we prove a stronger sign condition on y, namely $y > 0 \land py \succcurlyeq 0$. Consequently, in the second differential ghost step, we use $z' = \frac{g}{2}z$ and prove the invariant $yz^2 = 1$, which implies $y > 0$. □

Example 3.4 (Proving continuous properties in dL). Returning to the running example, we show that the unit circle $u^2 + v^2 - 1 = 0$ is an equational invariant for α_e. This follows by an immediate application of dbx with cofactor $-2(u^2 + v^2)$:

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

By a similar derivation with dbx$\gtrsim$, we can show that the disk $u^2 + v^2 - 1 \gtrsim 0$ and its complement are inequational invariants.

These derivations demonstrate the clever use of differential ghosts. In fact, we have already exceeded the deductive power of dI,dC because the formula $y > 0 \rightarrow [y' = -y]y > 0$ is valid but not provable with dI,dC alone but needs a dG [14]. It is a simple consequence of dbx$\gtrsim$, since the polynomial y satisfies the Darboux equality $\dot{y} = -y$ with cofactor -1. We can intuitively see why this is difficult from Fig. 2; y evolves exponentially towards $y = 0$, i.e., we get closer to violating the postcondition $y > 0$ along the solution.

4 Algebraic Invariants

We now consider polynomials that are not Darboux for the given differential equations, but instead satisfy a *differential radical property* [7] with respect to its higher Lie derivatives. Let g_i be cofactor polynomials, we assume that p satisfies the polynomial identity:

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

Following the intuition from Section 3.1, we again take Lie derivatives on both sides of the equation:

$$\begin{aligned}\dot{p}^{(N+1)} &= \mathcal{L}_{f(x)}(\dot{p}^{(N)}) = \mathcal{L}_{f(x)}\Big(\sum_{i=0}^{N-1} g_i \dot{p}^{(i)}\Big) = \sum_{i=0}^{N-1} \mathcal{L}_{f(x)}(g_i \dot{p}^{(i)}) \\ &= \sum_{i=0}^{N-1} \left(\dot{g_i}\dot{p}^{(i)} + g_i \dot{p}^{(i+1)}\right) \in (p, \dot{p}, \ldots, \dot{p}^{(N-1)})\end{aligned}$$

In the last step, ideal membership follows by observing that, by (1), $\dot{p}^{(N)}$ is contained in the ideal generated by the lower Lie derivatives. By repeatedly taking Lie derivatives on both sides, we again see that $\dot{p}^{(N)}, \dot{p}^{(N+1)}, \ldots$ are all contained in the ideal $(p, \dot{p}, \ldots, \dot{p}^{(N-1)})$. Thus, if we start in state ω where $\omega[\![p]\!], \omega[\![\dot{p}]\!], \ldots, \omega[\![\dot{p}^{(N-1)}]\!]$ all simultaneously evaluate to 0, then $p = 0$ (and all of its higher Lie derivatives) must stay invariant along solutions to the ODE.

This section shows how to axiomatically prove this invariance property using (vectorial) dG. We shall see at the end of the section that this allows us to prove *all* true algebraic invariants.

4.1 Vectorial Darboux Equalities

We first derive a vectorial generalization of the Darboux rule dbx, which will allow us to derive the rule for algebraic invariants as a special case by exploiting a vectorial version of (1). Let us assume that the n-dimensional vector of polynomials $\mathbf{p}$ satisfies the vectorial polynomial identity $\dot{\mathbf{p}} = G\mathbf{p}$, where G is an $n \times n$ matrix of polynomials, and $\dot{\mathbf{p}}$ denotes component-wise Lie derivation of $\mathbf{p}$.

Similarly, let $\omega[\![\mathbf{p}]\!]$ be the vector where $(\omega[\![\mathbf{p}]\!])_i \overset{\text{def}}{=} \omega[\![\mathbf{p}_i]\!]$. In states ω where $\omega[\![\mathbf{p}]\!] = 0$, we have $\omega[\![p_i(x)]\!] = 0$ for all i, and therefore, $\omega[\![\dot{\mathbf{p}}]\!] = \omega[\![G\mathbf{p}]\!] = 0$.

Lemma 4.1 (Vectorial Darboux equalities are vectorial ghosts)**.** *The vectorial Darboux proof rule derives from vectorial dG.*

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

Proof. Let G be an $n \times n$ matrix of polynomials, and $\mathbf{p}$ be an n-dimensional vector of polynomials satisfying the premise of vdbx.

First, we develop a proof that we will have occasion to use repeatedly. This proof adds an n-dimensional vectorial ghost $\mathbf{y}$ such that the vanishing of the scalar product, i.e., $\mathbf{p} \cdot \mathbf{y} = 0$, is a provable invariant. In the derivation below, we have suppressed the initial choice of values for $\mathbf{y}$. ① denotes the use of the premise of vdbx. In the dC step, we mark the remaining open premise with ②.

$$\text{dG}\,\dfrac{\text{dC}\,\dfrac{② \qquad \text{dI}\,\dfrac{\text{cut}\,\dfrac{① \qquad \mathbb{R}\,\dfrac{\mathbb{R}\,\dfrac{*}{Q \vdash G\mathbf{p}\cdot\mathbf{y} - G\mathbf{p}\cdot\mathbf{y} = 0}}{Q \vdash G\mathbf{p}\cdot\mathbf{y} - \mathbf{p}\cdot G^T\mathbf{y} = 0}}{Q \vdash \dot{\mathbf{p}}\cdot\mathbf{y} - \mathbf{p}\cdot G^T\mathbf{y} = 0}}{\mathbf{p}\cdot\mathbf{y} = 0 \vdash [x' = f(x), \mathbf{y}' = -G^T\mathbf{y} \,\&\, Q]\mathbf{p}\cdot\mathbf{y} = 0}}{\mathbf{p} = 0 \vdash \exists \mathbf{y}\,[x' = f(x), \mathbf{y}' = -G^T\mathbf{y} \,\&\, Q]\mathbf{p} = 0}}{\mathbf{p} = 0 \vdash [x' = f(x) \,\&\, Q]\mathbf{p} = 0}$$

The open premise ② now includes $\mathbf{p}\cdot\mathbf{y} = 0$ in the evolution domain:

$$② \quad \mathbf{p} = 0 \vdash [x' = f(x), \mathbf{y}' = -G^T\mathbf{y} \,\&\, Q \wedge \mathbf{p}\cdot\mathbf{y} = 0]\mathbf{p} = 0$$

The proof thus far is similar to the first ghost step in dbx. Unfortunately, for $n > 1$, the postcondition $\mathbf{p} = 0$ does *not* follow from the evolution domain constraint $\mathbf{p}\cdot\mathbf{y} = 0$ even when $\mathbf{y} \neq 0$, because $\mathbf{p}\cdot\mathbf{y} = 0$ merely implies that $\mathbf{p}$ and $\mathbf{y}$ are orthogonal, not that $\mathbf{p}$ is 0.

The idea is to repeat the above proof sufficiently often to obtain an entire matrix Y of differential ghost variables such that both $Y\mathbf{p} = 0$ and $\det(Y) \neq 0$ can be proved invariant.[7] The latter implies that Y is invertible, so that $Y\mathbf{p} = 0$ implies $\mathbf{p} = 0$.

We obtain the matrix Y by repeating n times the derivation above on the premise ②, using dG to add n copies of the ghost vectors, $\mathbf{y}_1, \ldots, \mathbf{y}_n$, each satisfying the system $\mathbf{y}_i' = -G^T\mathbf{y}_i$. As we have seen above, each of these ghost vectors satisfies the provable invariant $\mathbf{y}_i \cdot \mathbf{p} = 0$. We write this concisely as a system of equations:

$$\overbrace{\begin{pmatrix} y_{11} & y_{12} & \cdots & y_{1n} \\ y_{21} & y_{22} & \cdots & y_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ y_{n1} & y_{n2} & \cdots & y_{nn} \end{pmatrix}}^{Y} \overbrace{\begin{pmatrix} p_1 \\ p_2 \\ \cdots \\ p_n \end{pmatrix}}^{\mathbf{p}} = 0$$

Using dI,$[\cdot]\wedge$, we prove:

$$\mathbf{p}{=}0 \vdash [x' = f(x), \mathbf{y}_1' = -G^T\mathbf{y}_1, \ldots, \mathbf{y}_n' = -G^T\mathbf{y}_n \,\&\, Q] \bigwedge_{j=1}^{n} \mathbf{y}_j \cdot \mathbf{p}{=}0$$

which we summarize using the above matrix notation as:

$$③ \quad \mathbf{p} = 0 \vdash [x' = f(x), Y' = -YG \,\&\, Q]Y\mathbf{p} = 0$$

because when Y' is the component-wise derivative of Y, all the differential ghost equations are summarized as $Y' = -YG$.[8] Now that we have the invariant $Y\mathbf{p} = 0$ from ③, it remains to show the invariance of $\det(Y) > 0$ to complete the proof.

Since Y only contains y_{ij} variables, $\det(Y)$ is a polynomial term in the variables y_{ij}. These y_{ij} are ghost variables that we have introduced, and so we are free to pick their initial values. For convenience, we shall pick initial values forming the identity matrix $Y = \mathbb{I}$, so that $\det(Y) = \det(\mathbb{I}) = 1 > 0$ is true initially.

[7] For a square matrix of polynomials Y, we write $\det(Y)$ for its determinant, Y^T for its transpose, $\text{adj}(Y)$ for its adjugate, and $\text{tr}(Y)$ for its trace.

[8] This can be seen explicitly by examining the entries on both sides of the differential equations: $Y_{ij}' = (y_{ij})' = -(G^T\mathbf{y}_i)_j = -\sum_{k=1}^{n} G^T_{jk} y_{ik} = -\sum_{k=1}^{n} G_{kj} y_{ik} = -\sum_{k=1}^{n} y_{ik} G_{kj} = -(YG)_{ij}$.

In order to show that $\det(Y) > 0$ is an invariant, we first observe the following critical polynomial identity:

$$\begin{aligned}\dot{\det(Y)} &= \mathrm{tr}(\mathrm{adj}(Y)\dot{Y}) = \mathrm{tr}\left(\mathrm{adj}(Y)(-YG)\right) = -\,\mathrm{tr}\left((Y^T\,\mathrm{adj}(Y))G\right)\\ &= -\,\mathrm{tr}\left(\det(Y)\,\mathbb{I}\,G\right) = -\,\mathrm{tr}\,(G)\det(Y)\end{aligned}$$

The first equality is Liouville's formula [21, §15.III], and the others are properties of linear algebra. We take Lie derivatives with respect to the extended system of equations $x' = f(x), Y' = -YG$.

Thus, $\det(Y)$ is a Darboux polynomial over the variables y_{ij}, with polynomial cofactor $-\,\mathrm{tr}(G)$. Therefore, this is a valid deduction:

$$④ \qquad \text{dbx}_{\gtrsim}\frac{Q \vdash \dot{\det(Y)} = -\,\mathrm{tr}(G)\det(Y)}{\det(Y){>}0 \vdash [x' = f(x), Y' = -YG \,\&\, Q]\det(Y){>}0}$$

Putting ③ and ④ together allows us to complete the derivation for the invariance of $\mathbf{p} = 0$. We start with the dG step, and abbreviate the ghost matrix as above.

$$\text{dG}\dfrac{\dfrac{\mathbf{p} = 0 \vdash \exists Y\,[x' = f(x),\ Y' = -YG \,\&\, Q]\mathbf{p} = 0}{\mathbf{p} = 0 \vdash \exists \mathbf{y}_1, \ldots, \mathbf{y}_n\,[x' = f(x), \mathbf{y}_1' = -G^T\mathbf{y}_1, \ldots, \mathbf{y}_n' = -G^T\mathbf{y}_n \,\&\, Q]\mathbf{p} = 0}}{\mathbf{p} = 0 \vdash [x' = f(x) \,\&\, Q]\mathbf{p} = 0}$$

Now, we carry out the rest of the proof as outlined above.

$$\exists\mathbb{R}\dfrac{\text{cut}\dfrac{\text{dC}\dfrac{\text{dC}\dfrac{\text{dW}\dfrac{\mathbb{R}\dfrac{*}{Q \wedge Y\mathbf{p}{=}0 \wedge \det(Y){>}0 \vdash \mathbf{p}{=}0}}{④ \quad \mathbf{p}{=}0 \vdash [x' = f(x),\ Y' = -YG \,\&\, Q \wedge Y\mathbf{p}{=}0 \wedge \det(Y){>}0]\mathbf{p}{=}0}}{③ \quad \mathbf{p}{=}0,\ \det(Y){>}0 \vdash [x' = f(x),\ Y' = -YG \,\&\, Q \wedge Y\mathbf{p} = 0]\mathbf{p}{=}0}}{\mathbf{p}{=}0,\ \det(Y){>}0 \vdash [x' = f(x),\ Y' = -YG \,\&\, Q]\mathbf{p}{=}0}}{\mathbf{p}{=}0,\ Y = \mathbb{I} \vdash [x' = f(x),\ Y' = -YG \,\&\, Q]\mathbf{p}{=}0}}{\mathbf{p}{=}0 \vdash \exists Y\,[x' = f(x),\ Y' = -YG \,\&\, Q]\mathbf{p}{=}0}$$

The order of the differential cuts ③ and ④ is irrelevant. ◻

Since $\det(Y) \neq 0$ is invariant, we can view the $n \times n$ ghost matrix Y in the proof of vdbx as a basis matrix for $\mathbb{R}^n$ that *continuously evolves* along the differential equations. To see what Y does geometrically, let $\mathbf{p}_0$ be the initial values of $\mathbf{p}$, and $Y = \mathbb{I}$ initially. With our choice of Y, we can show, using a variation of ③ in the proof of vdbx, that $Y\mathbf{p}{=}\mathbf{p}_0$ is invariant. Thus, the evolution of Y *balances out* the evolution of $\mathbf{p}$, so that $\mathbf{p}$ remains constant with respect to the evolving basis Y. This generalizes the intuition illustrated in Fig. 2 to the n-dimensional case. Crucially, differential ghosts let us express this time-varying change of basis purely syntactically.

4.2 Differential Radical Invariants

We now return to polynomials p satisfying property (1), and show how to prove $p = 0$ invariant using an instance of vdbx.

Theorem 4.2 (Differential radical invariants are vectorial Darboux). *The differential radical invariant proof rule derives from vdbx (which in turn derives from vectorial dG).*

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

Proof Summary (See Appendix C). This follows from vdbx with:

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

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 $\mathbf{p} = 0$ initially, while the right premise is used to show the premise of vdbx. ◻

4.3 Completeness for Algebraic Invariants

Algebraic formulas are formed from finite conjunctions and disjunctions of polynomial equations. We may, however, restrict attention to a single equation $p = 0$ because all algebraic formulas can be normalized to this form using the real arithmetic equivalences:

$$p = 0 \wedge q = 0 \leftrightarrow p^2 + q^2 = 0, \quad p = 0 \vee q = 0 \leftrightarrow pq = 0$$

The key insight behind completeness of dRI is that higher Lie derivatives stabilize. Since the polynomials $\mathbb{R}[x]$ form a Noetherian ring, for every polynomial p and differential equation $x' = f(x)$, there is a smallest natural number $N{\geq}1$ called *order* [7, 9, 10] where:

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

This N is computable by successive ideal membership checks [7].

Thus, a suitable *order* at which the right premise of dRI proves always exists for any polynomial p.[9] We call the succedent in the remaining left premise of dRI the differential radical formula.

Definition 4.3 (Differential radical formula)**.** The *differential radical formula* $\dot{p}^{(*)} = 0$ of a polynomial p with order N and Lie derivatives with respect to $x' = f(x)$ is defined to be:

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

We write $\dot{p}^{(-*)} = 0$ when the Lie derivatives are taken with respect to $x' = -f(x)$ instead.

The completeness of dRI can be proved semantically [7]. However, using the extensions developed in Section 5, we derive the following characterization for algebraic invariants axiomatically.

Theorem 4.4 (Algebraic invariant completeness)**.** *Let Q be a real arithmetic formula that characterizes an open set. The following is a derived axiom in* dL*:*

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

Proof Summary (See Appendix B.1). The "←" direction follows by an application of dRI (whose right premise closes immediately for any Q). The "→" direction relies on the existence and uniqueness of solutions to differential equations, which are internalized as additional axioms in Section 5. ◻

For the proof of Theorem 4.4, we emphasize that additional axioms are *only required* for syntactically deriving the "→" direction (completeness) of DRI. Hence, the base dL axiomatization with differential ghosts is complete for proving properties of the form $[x' = f(x) \,\&\, Q]p = 0$ because dRI reduces all such questions to $Q \rightarrow \dot{p}^{(*)} = 0$, which is a formula of real arithmetic, and hence, decidable. The same applies for our next result, which is a corollary of Theorem 4.4, but applies beyond the continuous fragment of dL.

[9] Our derivation shows that it is sound to additionally assume Q when proving ideal membership of $\dot{p}^{(N)}$. However, since the order of p exists even without this assumption, our rule may also be seen as an optimization that helps reduce the number of Lie derivatives p that need to be considered.

Corollary 4.5 (Test-free decidability). *Let α be a hybrid program without tests or evolution domain constraints (see Appendix B.1), and P be an algebraic formula. There is a (computable) polynomial q such that the equivalence $[\alpha]P \leftrightarrow q = 0$ is derivable in* dL.

Proof Summary (See Appendix B.1). By structural induction on α, using Theorem 4.4 for the differential equations case. □

5 Extended Axiomatization

In this section, we present the axiomatic extensions that we will use for the rest of this paper. Without loss of generality, we assume that the system of differential equations, $x' = f(x)$, already contains $t' = 1$, which makes t act as a clock to track the passage of time. Such a clock variable can always be added using dG if necessary.

5.1 Existence, Uniqueness, and Continuity

The differential equations considered in this paper have polynomial right-hand sides, which are smooth and analytic. In particular, they satisfy the premises of the Picard-Lindelöf theorem [21, §10.VI], which guarantees that for any initial state $\omega \in \mathbb{R}^n$, a *unique* solution of the system $x' = f(x)$, i.e. $\varphi : [0,T] \to \mathbb{R}^n$ with $\varphi(0) = \omega$, *exists* for some non-empty time interval $T > 0$. Moreover, the solution φ may be extended (uniquely) to its maximal open interval of existence [21, §10.IX]. The solution $\varphi(\zeta)$ is, by definition, differentiable, and hence continuous with respect to ζ.

Lemma 5.1 (Existence, uniqueness and continuity). *The following axioms are sound. In Cont, t_0 is a fresh variable (not in x, $f(x)$ or p).*

$$\text{Uniq}\quad \begin{aligned}&\langle x' = f(x) \,\&\, Q_1\rangle P_1 \land \langle x' = f(x) \,\&\, Q_2\rangle P_2\\ &\to \langle x' = f(x) \,\&\, Q_1 \land Q_2\rangle (P_1 \lor P_2)\end{aligned}$$

$$\text{Cont}\quad t = t_0 \to \big(p > 0 \to \langle x' = f(x) \,\&\, p > 0\rangle t \neq t_0\big)$$

Proof Summary (See Appendix A.3). Uniq internalizes uniqueness, while Cont internalizes continuity and existence of solutions. □

Axiom Uniq can be intuitively read as follows. Suppose that we had two solutions φ_1, φ_2 respectively staying in evolution domains Q_1, Q_2 and whose endpoints satisfy P_1, P_2. Then one of φ_1 or φ_2 is a prefix of the other, and therefore, the prefix stays in the evolution domain $Q_1 \land Q_2$, and satisfies $P_1 \lor P_2$ at its endpoint.

Axiom Cont uses the clock variable t to express a notion of *local progress* for differential equations. Intuitively, it says that from the current time t_0, the system can locally progress to some different time $t \neq t_0$ by following the differential equations while staying in the *open set* of states characterized by $p > 0$. This notion can be encoded in dL in several ways. We have used a clock variable for simplicity. For emphasis, we use the following syntax for local progress within domain Q:

$$\big\langle x' = f(x) \,\&\, Q\big\rangle \circ \overset{\text{def}}{\equiv} \langle x' = f(x) \,\&\, Q\rangle t \neq t_0$$

For the remaining derivations in this paper, we only encounter $\langle x' = f(x) \,\&\, Q\rangle\circ$ when we have an assumption $t = t_0$. In this case, where $\omega[\![t]\!] = \omega[\![t_0]\!]$, the modality has the following semantics:

$$\begin{aligned}&\omega \in [\![\big\langle x' = f(x) \,\&\, Q\big\rangle\circ]\!] \text{ iff there is a function } \varphi : [0,T] \to \mathbb{R}^n\\ &\text{with } T > 0, \varphi(0) = \omega, \varphi(T) = \nu, \varphi \models x' = f(x) \,\&\, Q\end{aligned}$$

This resembles a continuous version of the next modality $\circ$ of temporal logic. For brevity, we directly use $\langle x' = f(x) \,\&\, Q\rangle\circ$, and drop $t = t_0$ from the antecedents, e.g., with this derived rule:

$$\text{cont}\ \frac{*}{p > 0 \vdash \langle x' = f(x) \,\&\, p > 0\rangle\circ}$$

To make use of Uniq and Cont, it will be useful to derive rules and axioms that allow us to work directly in the diamond modality, rather than the box modality that we have used so far.

Corollary 5.2 (Derived diamond modality rules and axioms). *The following derived rules and axioms are sound for* dL*:*

$$\langle\cdot\rangle\text{dR}\ \frac{\Gamma \vdash [x' = f(x) \,\&\, R]Q \quad \Gamma \vdash \langle x' = f(x) \,\&\, R\rangle P}{\Gamma \vdash \langle x' = f(x) \,\&\, Q\rangle P}$$

$$\langle\cdot\rangle\text{dRW}\ \frac{R \vdash Q \quad \Gamma \vdash \langle x' = f(x) \,\&\, R\rangle P}{\Gamma \vdash \langle x' = f(x) \,\&\, Q\rangle P}$$

$$\&\land\quad \begin{aligned}&\langle x' = f(x) \,\&\, Q \land R\rangle P\\ &\leftrightarrow \langle x' = f(x) \,\&\, Q\rangle P \land \langle x' = f(x) \,\&\, R\rangle P\end{aligned}$$

Proof Summary (See Appendix A.4). The $\langle\cdot\rangle$dR rule derives from the diamond version of the dL refinement axiom that underlies dC; if we never leave Q when staying in R (its left premise), then any solution staying in R for its entire duration (its right premise) must also stay in Q for its entire duration (its conclusion).

The rule $\langle\cdot\rangle$dRW follows from $\langle\cdot\rangle$dR by simplifying its left premise with dW. The equivalence $\&\land$ follows from $\langle\cdot\rangle$dRW for the "$\to$" direction, while the "$\leftarrow$" direction is an instance of Uniq by setting P_1, P_2 to P, and Q_1, Q_2 to Q, R respectively. □

5.2 Real Induction

We state a symmetric version of the real induction principle [4].

Definition 5.3 (Inductive subset [4]). The subset $S \subseteq [a,b]$ is called an *inductive* subset of the interval $[a,b]$ with reals $a \leq b$ iff:

1. $a \in S$
2. If $a \leq x < b$ and $x \in S$, then $[x, x + \epsilon] \subseteq S$ for some $0 < \epsilon$
3. If $a < x \leq b$ and $x \in S^{\complement}$, then $[x - \epsilon, x] \subseteq S^{\complement}$ for some $0 < \epsilon$, where we write $S^{\complement}$ for the complement $[a,b] \setminus S$.

Proposition 5.4 (Real induction principle [4]). *The subset $S \subseteq [a,b]$ is inductive if and only if $S = [a,b]$.*

Crucially, this induction principle can be lifted to invariance properties for differential equations. For brevity, we present the axiom for systems without evolution domain constraints, leaving the general version to Appendix A.3.

Lemma 5.5 (Real induction). *The following real induction axiom and its corresponding derived rule are sound (t_0 is fresh).*

$$\begin{aligned}\text{RInd}\ &[x' = f(x)]P \leftrightarrow P \land [x' = f(x)]\forall t_0 \big(t = t_0 \to\\ &\quad (P \to \big\langle x' = f(x) \,\&\, P\big\rangle\circ) \land (\neg P \to \big\langle x' = -f(x) \,\&\, \neg P\big\rangle\circ)\big)\end{aligned}$$

$$\text{rInd}\ \frac{P \vdash \langle x' = f(x) \,\&\, P\rangle\circ \quad \neg P \vdash \langle x' = -f(x) \,\&\, \neg P\rangle\circ}{P \vdash [x' = f(x)]P}$$

Proof Summary (See Appendix A.3). The RInd axiom follows from the real induction principle and the Picard-Lindelöf theorem. The rInd rule derives from RInd with dW. □

RInd reduces invariance of P to local progress of P and local progress backwards of $\neg P$. Rule rInd shows what this principle buys us: instead of a global invariance property on the ODEs, its premises only require reasoning about local progress properties. These properties can be proved using Cont,Uniq, as we show next.

6 Semialgebraic Invariants

Throughout this section, we will let $Q \equiv \mathit{true}$ to simplify notation since Q is not central to our remaining discussion.[10] Any first-order formula of real arithmetic, P, characterizes a *semialgebraic set*, and by quantifier elimination [2] may equivalently be written as a finite, quantifier-free formula (p_{ij}, q_{ij} are polynomials):

$$P \equiv \bigwedge_{i=0}^{M} \big(\bigvee_{j=0}^{m(i)} p_{ij} = 0 \lor \bigvee_{j=0}^{n(i)} q_{ij} > 0 \big) \tag{2}$$

We therefore refer to P as a *semialgebraic* formula, and the first step in our invariance proofs for semialgebraic P will be to apply the rInd rule, yielding premises of the form (modulo sign changes and negation): $P \vdash \langle x' = f(x) \,\&\, P \rangle \circ$.

6.1 Local Progress

Our objective shall be to derive local progress rules of the form

$$\frac{\Gamma \vdash R}{\Gamma, P \vdash \langle x' = f(x) \,\&\, P \rangle \circ}$$

where R is a formula of real arithmetic, computable from the form of P. We proceed in cases, starting from the simplest forms of P.

6.1.1 Atomic Equations

Let $P \equiv p = 0$. By Theorem 4.4, $\dot{p}^{(*)} = 0$ is a sufficient condition for $p = 0$ to be invariant. It is also a sufficient condition for local progress, i.e., we have the derived rule:

$$\langle\cdot\rangle\text{dRI}\ \frac{\Gamma \vdash \dot{p}^{(*)} = 0}{\Gamma, p = 0 \vdash \langle x' = f(x) \,\&\, p = 0 \rangle \circ}$$

which derives using cont and the trivial arithmetic fact $1 > 0$:

$$\langle\cdot\rangle\text{dR}\ \dfrac{\text{dRI}\ \dfrac{\Gamma \vdash \dot{p}^{(*)} = 0}{\Gamma \vdash [x' = f(x) \,\&\, 1 > 0] p = 0} \qquad \mathbb{R},\text{cont}\ \dfrac{*}{\vdash \langle x' = f(x) \,\&\, 1 > 0 \rangle \circ}}{\Gamma, p = 0 \vdash \langle x' = f(x) \,\&\, p = 0 \rangle \circ}$$

6.1.2 Strict Open Inequalities

Let $P \equiv \bigvee_{i=0}^{n} q_i > 0$. Topologically, this case is easy, because a *continuous* solution that starts in an open set must locally stay in that open set. Indeed, the derivation here uses continuity, and does not need any premises. We have collapsed the multiple (similar) cases arising from $\lor$L into a single case, indexed by i. In the $\langle\cdot\rangle$dRW step, we used the tautology $q_i > 0 \to \bigvee_{i=0}^{n} q_i > 0$.

$$\lor\text{L}\ \dfrac{\langle\cdot\rangle\text{dRW}\ \dfrac{\text{cont}\ \dfrac{*}{q_i > 0 \vdash \langle x' = f(x) \,\&\, q_i > 0 \rangle \circ}}{q_i > 0 \vdash \big\langle x' = f(x) \,\&\, \bigvee_{i=0}^{n} q_i > 0 \big\rangle \circ}}{\Gamma, \bigvee_{i=0}^{n} q_i > 0 \vdash \big\langle x' = f(x) \,\&\, \bigvee_{i=0}^{n} q_i > 0 \big\rangle \circ}$$

We summarize with the following derived rule:

$$\text{cont}^o\ \frac{*}{\Gamma, \bigvee_{i=0}^{n} q_i > 0 \vdash \big\langle x' = f(x) \,\&\, \bigvee_{i=0}^{n} q_i > 0 \big\rangle \circ}$$

6.1.3 Mixed Equality and Strict Inequality

The interesting case arises with $P \equiv p = 0 \lor q > 0$. The inequality $p_e \geq 0, p_e \overset{\text{def}}{=} v^2 - u^2 + \frac{3}{2}$ in our running example can be written in this form, because of the arithmetic equivalence $p \geq 0 \leftrightarrow p = 0 \lor p > 0$. We first note a simple reduction using $\lor$L:

$$\lor\text{L}\ \dfrac{\Gamma, p = 0 \vdash \langle x' = f(x) \,\&\, p = 0 \lor q > 0 \rangle \circ \qquad \langle\cdot\rangle\text{dRW,cont}\ \dfrac{*}{q > 0 \vdash \ldots}}{\Gamma, p = 0 \lor q > 0 \vdash \langle x' = f(x) \,\&\, p = 0 \lor q > 0 \rangle \circ}$$

One possibility for dealing with the open (left) premise is to use $\langle\cdot\rangle$dRI. However, this does not provide necessary conditions in general. In our example, this would require us to show $\dot{p_e}^{(*)} = 0$, i.e., points satisfying $p_e = 0$ locally stay on $p_e = 0$. From Fig. 1, this is clearly false because the arrows at $p_e = 0$ point inwards, i.e., towards $p_e > 0$. More generally, the open premise requires us to find conditions where we start on $p = 0$, but *locally enter* $q > 0$ for any q. However, the disjunction in the evolution domain is not easy to work with in dL. We remove it with the following observations:

Proposition 6.1. *Let $r = p^2$, then $\bigwedge_{i=0}^{n} \dot{p}^{(i)} = 0 \to \bigwedge_{i=0}^{n+1} \dot{r}^{(i)} = 0$ is a consequence of real arithmetic.*

Proof. Since $r = p^2$, applying the Leibniz rule yields that $\dot{r}^{(k)}$ equals:

$$\sum_{i=0}^{k} \binom{k}{i} \dot{p}^{(k-i)} \dot{p}^{(i)} = p\dot{p}^{(k)} + \sum_{i=0}^{k-1} \binom{k}{i} \dot{p}^{(k-i)} \dot{p}^{(i)} = \sum_{i=0}^{k-1} \binom{k}{i} \dot{p}^{(k-i)} \dot{p}^{(i)}$$

The last equality follows by the assumption $p = 0$ (recall that $n \geq 0$). Now, consider $0 \leq k \leq n+1$. By assumption, for $0 \leq i < k$, $\dot{p}^{(i)} = 0$, and therefore the remaining term in the sum is also 0. In other words, $r = 0, \dot{r} = 0, \ldots, \dot{r}^{(n+1)} = 0$. □

Corollary 6.2. *Let $r = p^{2n}$ for any $n \geq 1$, $p = 0 \to \bigwedge_{i=0}^{n} \dot{r}^{(i)} = 0$ is a consequence of real arithmetic.*

Proof. By repeated squaring, and applying Proposition 6.1. □

Using Corollary 6.2, we note that by choosing $r = p^{2n}$ for sufficiently large $n \geq 1$, we have the following derivation[11]:

$$\text{cut}\ \dfrac{\langle\cdot\rangle\text{dRW}\ \dfrac{\langle\cdot\rangle\text{dRW}\ \dfrac{\Gamma_r \vdash \langle x' = f(x) \,\&\, q \geq r \rangle \circ}{\Gamma_r \vdash \langle x' = f(x) \,\&\, r = 0 \lor q > 0 \rangle \circ}}{\Gamma, r = 0, \ldots, \dot{r}^{(n)} = 0 \vdash \langle x' = f(x) \,\&\, p = 0 \lor q > 0 \rangle \circ}}{\Gamma, p = 0 \vdash \langle x' = f(x) \,\&\, p = 0 \lor q > 0 \rangle \circ}$$

The first $\langle\cdot\rangle$dRW step, uses the arithmetic equivalence $p = 0 \leftrightarrow p^{2n} = 0$. In the second $\langle\cdot\rangle$dRW step, we observe that since $r = p^{2n} \geq 0$, we have $q \geq r \geq 0$ which implies $r = 0 \lor q > 0$ as required. We abbreviate the antecedents Γ extended with the $r = 0, \ldots, \dot{r}^{(n)} = 0$ assumptions as Γ_r. The disjunction in the evolution domain constraint has been changed to a single weak inequality. We work on this inequality with the following derived rules:

Lemma 6.3 (Local progress)**.** *These rules derive from cont,dI,dC.*

$$\text{lp}_{>}\ \frac{\Gamma \vdash q > r}{\Gamma \vdash \langle x' = f(x) \,\&\, q \geq r \rangle \circ}$$

$$\text{lp}_{\geq}\ \frac{\Gamma \vdash q \geq r \qquad \Gamma, q = r \vdash \big\langle x' = f(x) \,\&\, \dot{q} \geq \dot{r} \big\rangle \circ}{\Gamma \vdash \langle x' = f(x) \,\&\, q \geq r \rangle \circ}$$

Proof. lp$_{>}$ derives from lp$_{\geq}$, because $q > r$ implies $q \geq r$, but contradicts $q = r$ (in the right premise of lp$_{\geq}$). To derive lp$_{\geq}$, let us denote the use of its left (resp. right) premise by ① (resp. ②). We start using ① immediately, and then perform a simple arithmetic case split on the left. In the $q > r$ case, we apply cont and $\langle\cdot\rangle$dRW to close the premise. The remaining premise arising from the $q = r$ case is abbreviated with ③.

[10] The case of arbitrary semialgebraic Q can be found in Appendix B.

[11] With a more careful analysis in Proposition 6.1, we actually only need to pick $r = p^{2(O(\log n))}$ to achieve the same conclusion.

$$\text{cut}\ \dfrac{① \quad \mathbb{R},\vee\text{L}\ \dfrac{③ \quad \langle\cdot\rangle\text{dRW}\ \dfrac{\text{cont}\ \dfrac{*}{q > r \vdash \langle x' = f(x) \,\&\, q > r\rangle\circ}}{\Gamma, q > r \vdash \langle x' = f(x) \,\&\, q \geq r\rangle\circ}}{\Gamma, q \geq r \vdash \langle x' = f(x) \,\&\, q \geq r\rangle\circ}}{\Gamma \vdash \langle x' = f(x) \,\&\, q \geq r\rangle\circ}$$

On ③, we continue by cutting in second premise of $\text{lp}_{\geq}$. This allows us to use $\langle\cdot\rangle$dR, and subsequently finish the proof using dI.

$$\text{cut}\ \dfrac{② \quad \langle\cdot\rangle\text{dR}\ \dfrac{\text{dI}\ \dfrac{*}{q = r \vdash [x' = f(x) \,\&\, \dot{q} \geq \dot{r}] q \geq r}}{q = r, \langle x' = f(x) \,\&\, \dot{q} \geq \dot{r}\rangle\circ \vdash \langle x' = f(x) \,\&\, q \geq r\rangle\circ}}{\Gamma, q = r \vdash x' = f(x) q \geq r}$$

∎

Observe that $\text{lp}_{\geq}$ allows us to pass from reasoning about local progress for $q \geq r$ to local progress for their Lie derivatives $\dot{q} \geq \dot{r}$ whilst accumulating $q = r$ in the antecedent. It is clear, then, that we can iterate application of the rule from the initial premise until we eventually apply $\text{lp}_{>}$:

$$\text{lp}_{\geq}\ \dfrac{\Gamma \vdash q \geq r \quad \text{lp}_{\geq}\ \dfrac{\Gamma, q = r \vdash \dot{q} \geq \dot{r} \qquad \begin{matrix} \text{lp}_{>}\ \dfrac{\Gamma, q = r, \ldots \vdash \dot{q}^{(k)} > \dot{r}^{(k)}}{\ldots} \\ \vdots \end{matrix}}{\Gamma, q = r \vdash \langle x' = f(x) \,\&\, \dot{q} \geq \dot{r}\rangle\circ}}{\Gamma \vdash \langle x' = f(x) \,\&\, q \geq r\rangle\circ}$$

Gathering the succedents of the open premises above, we can instead directly prove the following formula from antecedents Γ:

$$\begin{aligned} & q \geq r \wedge \big(q = r \rightarrow \dot{q} \geq \dot{r}\big) \wedge \big(q = r \wedge \dot{q} = \dot{r} \rightarrow \dot{q}^{(2)} \geq \dot{r}^{(2)}\big) \\ & \wedge \ldots \\ & \wedge \big(q = r \wedge \dot{q} = \dot{r} \wedge \cdots \wedge \dot{q}^{(k-1)} = \dot{r}^{(k-1)} \rightarrow \dot{q}^{(k)} > \dot{r}^{(k)}\big) \end{aligned}$$

Working in antecedents $\Gamma \overset{\text{def}}{\equiv} \Gamma_r$ with $r = p^{2(k+1)}$, we may equivalently prove this formula where all of the Lie derivatives of r are set to 0 instead. Moreover, a sensible choice of k is $N - 1$, where N is the order of q. Recall that if $q, \dot{q}, \ldots, \dot{q}^{(N-1)}$ are simultaneously zero, then all higher Lie derivatives of q are also 0. This motivates the following definition that summarizes the above intuition:

Definition 6.4 (Progress formula)**.** The *progress formula* $\dot{q}^{(*)} > 0$ for a polynomial q with order N is defined as the following formula, where the Lie derivatives are computed with respect to $x' = f(x)$:

$$\begin{aligned} \dot{q}^{(*)} > 0 \overset{\text{def}}{\equiv} & q \geq 0 \wedge \big(q = 0 \rightarrow \dot{q} \geq 0\big) \wedge \big(q = 0 \wedge \dot{q} = 0 \rightarrow \dot{q}^{(2)} \geq 0\big) \\ & \wedge \ldots \\ & \wedge \big(q = 0 \wedge \dot{q} = 0 \wedge \cdots \wedge \dot{q}^{(N-2)} = 0 \rightarrow \dot{q}^{(N-1)} > 0\big) \end{aligned}$$

We write $\dot{q}^{(-*)} > 0$ when taking Lie derivatives with respect to $x' = -f(x)$ instead.

Putting everything together, we have the following derivation where the first cut proves $\dot{q}^{(*)} > 0$ from Γ, and the second cut extends Γ to Γ_r using $p = 0$:

$$\text{cut}\ \dfrac{\Gamma \vdash \dot{q}^{(*)} > 0 \quad \text{cut},\langle\cdot\rangle\text{dRW}\ \dfrac{\text{lp}_{\geq},\text{lp}_{>}\ \dfrac{*}{\Gamma_r, \dot{q}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, q \geq r\rangle\circ}}{\Gamma, p = 0, \dot{q}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, p = 0 \vee q > 0\rangle\circ}}{\Gamma, p = 0 \vdash \langle x' = f(x) \,\&\, p = 0 \vee q > 0\rangle\circ}$$

We summarize with the following derived rule:

$$\text{lp}_{=\vee>}\ \dfrac{\Gamma \vdash \dot{q}^{(*)} > 0}{\Gamma, p = 0 \vdash \langle x' = f(x) \,\&\, p = 0 \vee q > 0\rangle\circ}$$

6.1.4 Semialgebraic Case

We now consider the general normal form for semialgebraic P.

Lemma 6.5 (Semialgebraic local progress)**.** *Let P be a semialgebraic formula in normal form* (2)*. The following rule derives from* dL *extended with Cont,Uniq.*

$$\text{lp}\mathbb{R}\ \dfrac{\Gamma \vdash \bigwedge_{i=0}^{M} \big(\bigvee_{j=0}^{m(i)} \dot{p_{ij}}^{(*)} = 0 \vee \bigvee_{j=0}^{n(i)} \dot{q_{ij}}^{(*)} > 0\big)}{\Gamma, P \vdash \langle x' = f(x) \,\&\, P\rangle\circ}$$

Proof Summary (See Appendix C). We decompose P using $\wedge$L,&$\wedge$. Axiom Uniq is crucially used in &$\wedge$. This yields premises with disjunctive conditions. We prove local progress for these disjuncts using cont^o,$\langle\cdot\rangle$dRI,$\text{lp}_{=\vee>}$, and then lift the result to the full disjunction using $\langle\cdot\rangle$dRW. ∎

6.2 Proving Semialgebraic Invariants

Let semialgebraic P be written in the normal form (2), and let $\neg P$ also be written in the same normal form:

$$\neg P \equiv \bigwedge_{i=0}^{N} \big(\bigvee_{j=0}^{a(i)} r_i = 0 \vee \bigvee_{j=0}^{b(i)} s_{ij} > 0\big) \tag{3}$$

We summarize our results with the following derived rule.

Theorem 6.6 (Semialgebraic invariants)**.** *For semialgebraic P, with normal forms* (2) *and* (3)*, the following rule (with two premises) is sound and derives from the* dL *calculus extended with RInd,Cont,Uniq.*

$$\text{sAI}\ \dfrac{\begin{matrix} P \vdash \bigwedge_{i=0}^{M} \big(\bigvee_{j=0}^{m(i)} \dot{p_{ij}}^{(*)} = 0 \vee \bigvee_{j=0}^{n(i)} \dot{q_{ij}}^{(*)} > 0\big) \\ \neg P \vdash \bigwedge_{i=0}^{N} \big(\bigvee_{j=0}^{a(i)} \dot{r_{ij}}^{(-*)} = 0 \vee \bigvee_{j=0}^{b(i)} \dot{s_{ij}}^{(-*)} > 0\big) \end{matrix}}{P \vdash [x' = f(x)]P}$$

Proof. Straightforward application of $\text{lp}\mathbb{R}$,rInd. ∎

6.3 Completeness for Semialgebraic Invariants

The completeness of the sAI rule was proved in [9]. Their proof makes crucial use of the fact that solutions to polynomial ODE systems are analytic. Our derivations in this section shows that the sAI proof rule can be *derived* in a purely syntactic manner within the dL calculus. This leads to the following completeness theorem, which applies for all semialgebraic (i.e., first-order real arithmetic) formulas P, because quantifier elimination [2] allows us to equivalently rewrite P to normal form with rule $\mathbb{R}$.

Theorem 6.7 (Semialgebraic invariant completeness)**.** *Let P be a semialgebraic formula. The* dL *calculus is complete for invariance properties of the form $P \vdash [x' = f(x)]P$.*

In Appendix B, we show a more general version of Theorem 6.7 that also handles semialgebraic evolution domains. This crucially relies on the fact that we can characterize local progress properties for semialgebraic formulas using Cont,Uniq, see Theorem B.5.

It is important to note the difference between Theorem 4.4 and Theorem 6.7. In the former, we may decide $[x' = f(x) \,\&\, Q]p = 0$ from *any* set of (non-modal) premises Γ. This is not the case for Theorem 6.7 (or its generalized version), as the completeness result is limited to conclusions of the form $P \vdash [x' = f(x)]P$. Therefore, some work still has to be done to find such an invariant P.

7 Related Work

We focus our discussion on work related to *deductive* verification of hybrid systems. We refer readers interested in the basic theories of ODEs [21], real analysis [4], and real algebraic geometry [2] to the respective cited texts. Orthogonal to our work is the question of how invariants can be efficiently generated. We refer readers to the literature [7, 9, 17, 18]. Although these methods are usually phrased in the language of hybrid automata [1], their core reasoning principles (for ODEs) may also be expressed as proof rules [8].

Proof Rules for Invariants. An overview of proof rules for invariance of algebraic and semialgebraic sets can be found in [8]. The soundness and completeness theorems for dRI,sAI were first shown in [7] and [9] respectively. There are numerous other sound, but incomplete, proof rules for deductive verification along an ODE system [17, 20]. In their original presentation, dRI and sAI, are *algorithmic procedures* for checking invariance, requiring e.g., checking ideal membership for all polynomials in the semialgebraic decomposition. This makes them very difficult to implement soundly as part of a *small*, trusted axiomatic core, such as the implementation of dL in KeYmaera X [6]. We instead show that these rules can be *derived* from a small set of axiomatic principles. Although we also leverage ideal computations, they are only used as part of *derived rules*. With the aid of a theorem prover, derived rules can be implemented as tactics, that crucially remain *outside* the soundness-critical axiomatic core.

Deductive Power and Proof Theory. The derivations shown in this paper are fully general, which is necessary for completeness of the resulting derived rules. However, many simpler classes of invariants can be proved using simpler derivations. This is where a study of the deductive power of various sound, but incomplete, proof rules [8] comes into play. If we know that an invariant of interest is of a simpler class, then we could simply use the proof rule that is complete for that class. This intuition is echoed in [14], which studies the relative deductive power of differential invariants (dI) and differential cuts (dC). Our first result shows, in fact, that dL with dG is already complete for algebraic invariants. Other proof-theoretical studies of dL [13] reveal surprising correspondences between its hybrid, continuous and discrete aspects in the sense that each aspect can be axiomatized completely relative to any other aspect. Our Corollary 4.5 is a step in this direction.

8 Conclusion and Future Work

The first part of this paper demonstrates the impressive deductive power of differential ghosts: they prove all algebraic invariants and Darboux inequalities. We leave open the question of whether their deductive power extends to larger classes of invariants. The second part of this paper introduces extensions to the base dL axiomatization, and shows how they can be used together with the existing axioms to prove all real arithmetic invariants syntactically. The real induction principle is crucially used to reduce global invariance properties to local progress properties. In contrast to local progress, global liveness properties are tricky because solutions of differential equations may blow up in finite time. Indeed, existing liveness rules [12, 19] require the side assumption that solutions exist for sufficient duration. An avenue of future work is to investigate calculi for liveness without the need for these conditions.

It is instructive to examine the mathematical properties of solutions and terms that underlie our axiomatization. In summary:

Axiom	Property
dI	Mean value theorem
dC	Prefix-closure of solutions
dG	Picard-Lindelöf
Cont	Existence of solutions
Uniq	Uniqueness of solutions
RInd	Completeness of $\mathbb{R}$

The soundness of our axiomatization, therefore, easily extends to term languages beyond polynomials, e.g., continuously differentiable terms satisfy the above properties. We may, of course, lose completeness and decidable arithmetic in the extended language, and we leave further exploration of these issues to future work.

References

[1] Rajeev Alur, Costas Courcoubetis, Thomas A. Henzinger, and Pei-Hsin Ho. 1992. Hybrid Automata: An Algorithmic Approach to the Specification and Verification of Hybrid Systems. In *Hybrid Systems (LNCS)*, Robert L. Grossman, Anil Nerode, Anders P. Ravn, and Hans Rischel (Eds.), Vol. 736. Springer, 209–229.

[2] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. 1998. *Real Algebraic Geometry*. A Series of Modern Surveys in Mathematics, Vol. 36. Springer.

[3] 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, 208–221.

[4] Pete L. Clark. 2012. The Instructor's Guide to Real Induction. *arXiv preprint arXiv:1208.0973* (2012).

[5] Gaston Darboux. 1878. Mémoire sur les équations différentielles algébriques du premier ordre et du premier degré. *Bulletin des Sciences Mathématiques et Astronomiques* 2, 1 (1878), 151–200.

[6] 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, 527–538.

[7] 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, 279–294.

[8] Khalil Ghorbal, Andrew Sogokon, and André Platzer. 2017. A Hierarchy of Proof Rules for Checking Positive Invariance of Algebraic and Semi-Algebraic Sets. *Computer Languages, Systems and Structures* 47, 1 (2017), 19–43.

[9] 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, 97–106.

[10] Dmitri Novikov and Sergei Yakovenko. 1999. Trajectories of polynomial vector fields and ascending chains of polynomial ideals. In *ANNALES-INSTITUT FOURIER*, Vol. 49. Association des annales de l'institut Fourier, 563–609.

[11] Susan S. Owicki and David Gries. 1976. Verifying Properties of Parallel Programs: An Axiomatic Approach. *Commun. ACM* 19, 5 (1976), 279–285.

[12] André Platzer. 2010. Differential-algebraic Dynamic Logic for Differential-algebraic Programs. *J. Log. Comput.* 20, 1 (2010), 309–352.

[13] André Platzer. 2012. The Complete Proof Theory of Hybrid Systems. In *LICS*. IEEE, 541–550.

[14] André Platzer. 2012. The Structure of Differential Invariants and Differential Cut Elimination. *Logical Methods in Computer Science* 8, 4 (2012), 1–38.

[15] André Platzer. 2017. A Complete Uniform Substitution Calculus for Differential Dynamic Logic. *J. Autom. Reas.* 59, 2 (2017), 219–265.

[16] André Platzer and Yong Kiam Tan. 2017. *How to Prove "All" Differential Equation Properties*. Technical Report CMU-CS-17-117. School of Computer Science, Carnegie Mellon University, Pittsburgh, PA.

[17] 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, 477–492.

[18] Sriram Sankaranarayanan, Henny B. Sipma, and Zohar Manna. 2008. Constructing invariants for hybrid systems. *Form. Methods Syst. Des.* 32, 1 (2008), 25–55.

[19] Andrew Sogokon and Paul B. Jackson. 2015. Direct Formal Verification of Liveness Properties in Continuous and Hybrid Dynamical Systems. In *FM (LNCS)*, Nikolaj Bjørner and Frank S. de Boer (Eds.), Vol. 9109. Springer, 514–531.

[20] 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 - Leibniz-Zentrum fuer Informatik, 383–394.

[21] Wolfgang Walter. 1998. *Ordinary Differential Equations*. Graduate Texts in Mathematics, Vol. 182. Springer.

A Differential Dynamic Logic Axiomatization

We work with the uniform substitution calculus presented in [15]. The calculus is based on the uniform substitution inference rule:

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

The uniform substitution calculus requires a few extensions to the syntax and semantics presented in Section 2. Firstly we extend the term language with differential terms $(e)'$ and k-ary function symbols f, where $e_1, \ldots, e_k$ are terms. The formulas are similarly extended with k-ary predicate symbols P and predicationals C:

$$e ::= \cdots \mid (e)' \mid f(e_1, \ldots, e_k)$$

$$\phi ::= \cdots \mid P(e_1, \ldots, e_k) \mid C(\phi)$$

The grammar of dL programs is as follows (a is a program symbol):

$$\alpha ::= a \mid x := e \mid ?\phi \mid x' = f(x) \,\&\, Q \mid \alpha_1 \cup \alpha_2 \mid \alpha_1; \alpha_2 \mid \alpha^*$$

We refer readers to [15] for the complete, extended semantics. Briefly, for each variable x, there is an associated differential variable x', and states map all of these variables (including differential variables) to real values; we write $\mathbb{S}$ for the set of all states. The semantics also requires an interpretation I for the uniform substitution symbols. The term semantics, $I\omega[\![e]\!]$, gives the value of e in state ω and interpretation I. The formula semantics, $I[\![\phi]\!]$, is the set of states where ϕ is true in interpretation I, and the transition semantics of hybrid programs $I[\![\alpha]\!]$ is given with respect to interpretation I. The transition semantics for $x' = f(x)$ requires:

$(\omega, \nu) \in [\![x' = f(x) \,\&\, Q]\!]$ iff there is $T \geq 0$ and a function
$\varphi : [0, T] \to \mathbb{S}$ with $\varphi(0) = \omega$ on $\{x'\}^{\complement}$, $\varphi(T) = \nu$, and
$I, \varphi \models x' = f(x) \,\&\, Q$

The $I, \varphi \models x' = f(x) \,\&\, Q$ condition checks that $\varphi(\zeta) \in I[\![x' = f(x) \wedge Q]\!]$, $\varphi(0) = \varphi(\zeta)$ on $\{x, x'\}^{\complement}$ for $0 \leq \zeta \leq T$, and, if $T > 0$, then $\frac{d\varphi(t)(x)}{dt}(\zeta)$ exists, and is equal to $\varphi(\zeta)(x')$ for all $0 \leq \zeta \leq T$. In other words, φ is a solution of the differential equations $x' = f(x)$ that stays in the evolution domain constraint. It is also required to hold all variables other than x, x' constant. Most importantly, the values of the differential variables x' is required to match the valuation of the RHS of the differential equations along the solution. We refer readers to [15, Definition 7] for further details.

The calculus allows all of the axioms (cf. [15, Figures 2 and 3]) to be stated as *concrete* instances, which are then instantiated by uniform substitution. In this appendix, we take the same approach: all of our (new) axioms will be stated as concrete instances as well. We will need to be slightly more careful, and write down explicit variable dependencies for all the axioms. To make this paper self-contained, we state all of the axioms used in the paper and the appendix. However, we only provide justification for derived rules and axioms that are not already justified in [15].

A.1 Base Axiomatization

The following are the base axioms and proof rules for dL from [15, Figure 2].

Theorem A.1 (Base axiomatization [15]). *The following are sound axioms and proof rules for* dL.

$$\text{[:=]}\ \ [x := f]P(x) \leftrightarrow P(f)$$

$$\text{[?]}\ \ [?P]R \leftrightarrow (P \to R)$$

$$[\cup]\ \ [a_1 \cup a_2]P(x) \leftrightarrow [a_1]P(x) \wedge [a_2]P(x)$$

$$[;]\ \ [a_1; a_2]P(x) \leftrightarrow [a_1][a_2]P(x)$$

$$[^*]\ \ [a^*]P \leftrightarrow P \wedge [a][a^*]P$$

$$\langle\cdot\rangle\ \ \langle a\rangle P(x) \leftrightarrow \neg[a]\neg P(x)$$

$$\text{K}\ \ [a](P_1 \to P_2) \to ([a]P_1 \to [a]P_2)$$

$$\text{I}\ \ [a^*](P \to [a]P) \to (P \to [a^*]P)$$

$$\text{G}\ \ \frac{P(x)}{[a]P(x)}$$

In our sequent calculus, we instantiate these axioms using uniform substitution, and then use congruence reasoning for equivalences (and equalities). All of the substitutions that we require are admissible [15, Definition 19]. Note that G above is presented as a Hilbert-style rule. In our sequent calculus formulation, we use it by discarding the context, because if ϕ is valid, then it must also be true after running any program α:

$$\text{G}\ \frac{\vdash \phi}{\Gamma \vdash [\alpha]\phi}$$

The $[\cdot]\wedge$ axiom derives using G,K. For the " $\to$ " direction (the case for $[\alpha]\phi_2$ in the succedent is symmetric):

$$\text{cut,K}\ \dfrac{\text{G},{\to}\text{R}\ \dfrac{\dfrac{*}{\phi_1 \wedge \phi_2 \vdash \phi_1}}{\vdash [\alpha](\phi_1 \wedge \phi_2 \to \phi_1)}}{[\alpha](\phi_1 \wedge \phi_2) \vdash [\alpha]\phi_1}$$

In the " $\leftarrow$ " direction we use K twice:

$$\text{cut,K}\ \dfrac{\text{cut,K}\ \dfrac{\text{G},{\to}\text{R}\ \dfrac{\dfrac{*}{\phi_2, \phi_1 \vdash \phi_1 \wedge \phi_2}}{\vdash [\alpha](\phi_2 \to \phi_1 \to \phi_1 \wedge \phi_2)}}{[\alpha]\phi_2 \vdash [\alpha](\phi_1 \to \phi_1 \wedge \phi_2)}}{[\alpha]\phi_1, [\alpha]\phi_2 \vdash [\alpha](\phi_1 \wedge \phi_2)}$$

The M$[\cdot]$ rule derives using G,K as well. Note that applying K produces two premises.

$$\text{K}\ \dfrac{\text{G},{\to}\text{R}\ \dfrac{\phi_2 \vdash \phi_1}{\Gamma \vdash [\alpha](\phi_2 \to \phi_1)} \qquad \Gamma \vdash [\alpha]\phi_2}{\Gamma \vdash [\alpha]\phi_1}$$

The following is the familiar loop induction rule.

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

It derives from the induction axiom I and G.

$$\text{cut,I}\ \dfrac{\text{G},{\to}\text{R}\ \dfrac{\phi \vdash [\alpha]\phi}{\vdash [\alpha^*](\phi \to [\alpha]\phi)}}{\phi \vdash [\alpha^*]\phi}$$

A.2 Differential Equation Axiomatization

The following are axioms for differential equations and differentials from [15, Figure 3]. Note that x is a vector of variables $x_1, x_2, \ldots, x_n$, x' is the corresponding vector of differential variables $x_1', x_2', \ldots, x_n'$, and $f(x)$ is a vector of n-ary function symbols $f_1(x), f_2(x), \ldots, f_n(x)$.

Theorem A.2 (Differential equation axiomatization [15])**.** *The following are sound axioms of* dL.

$$\text{DW}\quad [x' = f(x)\,\&\,Q(x)]Q(x)$$

$$\text{DI}_{=}\quad \begin{array}{l}(Q(x) \to [x' = f(x)\,\&\,Q(x)](p(x))' = 0)\\ \to ([x' = f(x)\,\&\,Q(x)]p(x) = 0 \leftrightarrow [?Q(x)]p(x) = 0)\end{array}$$

$$\text{DI}_{\gtrsim}\quad \begin{array}{l}(Q(x) \to [x' = f(x)\,\&\,Q(x)](p(x))' \geq 0)\\ \to ([x' = f(x)\,\&\,Q(x)]p(x) \gtrsim 0 \leftrightarrow [?Q(x)]p(x) \gtrsim 0)\end{array}$$

$$\text{DE}\quad \begin{array}{l}[x' = f(x)\,\&\,Q(x)]P(x,x')\\ \leftrightarrow [x' = f(x)\,\&\,Q(x)][x':=f(x)]P(x,x')\end{array}$$

$$c'\quad (f)' = 0$$

$$x'\quad (x)' = x'$$

$$+'\quad (f(x) + g(x))' = (f(x))' + (g(x))'$$

$$\cdot'\quad (f(x) \cdot g(x))' = (f(x))' \cdot (g(x)) + (f(x)) \cdot (g(x))'$$

Syntactic derivation under differential equations is performed using the DE axiom along with the axioms for working with differentials c',x',$+'$,$\cdot'$ [15, Lemmas 36-37], and the assignment axiom $[':=]$ for differential variables. We label the exhaustive use of the differential axioms as e'. The following derivation is sound for any polynomial term p (where $\dot{p}$ is the polynomial term for the Lie derivative of p). We write $\sim$ for a free choice between $=$ and $\gtrsim$:

$$\dfrac{\dfrac{\vdash [x' = f(x)\,\&\,Q]\dot{p} \sim 0}{\vdash [x' = f(x)\,\&\,Q][x':=f(x)](p)' \sim 0}\; e',[':=],\mathbb{R}}{\vdash [x' = f(x)\,\&\,Q](p)' \sim 0}\;\text{DE}$$

The e',$[':=]$,$\mathbb{R}$ step first performs syntactic Lie derivation on p, and then additionally uses $\mathbb{R}$ to rearrange the resulting term into $\dot{p}$ as required. To see this more concretely, we perform the above derivation with a polynomial from the running example.

Example A.3 (Using syntactic derivations)**.** Let $p_e \overset{\text{def}}{=} v^2 - u^2 + \frac{3}{2}$, unfolding the Lie derivative, we have:

$$\begin{aligned}\mathcal{L}_{\alpha_e}(p_e) &= \frac{\partial p_e}{\partial u}(-v + u(1 - u^2 - v^2)) + \frac{\partial p_e}{\partial v}(u + v(1 - u^2 - v^2))\\ &= -2u(-v + u(1 - u^2 - v^2)) + 2v(u + v(1 - u^2 - v^2))\\ &= 4uv + 2(1 - u^2 - v^2)(v^2 - u^2) = \dot{p_e}\end{aligned}$$

Now, we may perform the above derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdash [\alpha_e]\dot{p_e} \sim 0}{\vdash [\alpha_e]2v(u + v(1 - u^2 - v^2)) - 2u(-v + u(1 - u^2 - v^2)) \sim 0}\;\mathbb{R}}{\vdash [\alpha_e][u':=-v + u(1 - u^2 - v^2)][v':=u + v(1 - u^2 - v^2)]2vv' - 2uu' \sim 0}\;[':=]}{\vdash [\alpha_e][u':=-v + u(1 - u^2 - v^2)][v':=u + v(1 - u^2 - v^2)](p_e)' \sim 0}\;e'}{\vdash [\alpha_e](p_e)' \sim 0}\;\text{DE}$$

Note that we needed the $\mathbb{R}$ step to rearrange the result from syntactically differentiating p_e to match the expression $\dot{p_e}$ for the Lie derivative. Since the two notions must coincide under the ODEs, this rearrangement step is always possible.

We prove generalized versions of axioms from [15]. These are the vectorial differential ghost axioms (DG and DG$_\forall$)[12] which were proved only for the single variable case, and the differential modus ponens axiom, DMP, which was specialized for differential cuts.

[12] We do not actually need DG$_\forall$ in this paper. We prove it for completeness, because [15] proves a similar axiom.

Lemma A.4. *The following axioms are sound. Note that* $\mathbf{y}$ *is an* m*-dimensional vector of variables,* $\mathbf{y}'$ *is its corresponding vector of differential variables, and* $a(x)$ *(resp.* $b(x)$*) is a* $m \times m$ *matrix (resp.* m*-dimensional vector) of function symbols.*

$$\text{DG}\quad \begin{array}{l}[x' = f(x)\,\&\,Q(x)]P(x)\\ \leftrightarrow \exists\mathbf{y}\,[x' = f(x), \mathbf{y}' = a(x) \cdot \mathbf{y} + b(x)\,\&\,Q(x)]P(x)\end{array}$$

$$\text{DG}_\forall\quad \begin{array}{l}[x' = f(x)\,\&\,Q(x)]P(x)\\ \leftrightarrow \forall\mathbf{y}\,[x' = f(x), \mathbf{y}' = a(x) \cdot \mathbf{y} + b(x)\,\&\,Q(x)]P(x)\end{array}$$

$$\text{DMP}\quad \begin{array}{l}[x' = f(x)\,\&\,Q(x)](Q(x) \to R(x))\\ \to ([x' = f(x)\,\&\,R(x)]P(x) \to [x' = f(x)\,\&\,Q(x)]P(x))\end{array}$$

Proof. In this proof, we use ω for the initial state, and ν for the state reached at the end of a continuous evolution. The valuations for matrix and vectorial terms are applied component-wise.

We first prove vectorial DG and DG$_\forall$. Our proof is specialized to the case of linear (inhomogeneous) systems. We only need to prove the "$\to$" direction for DG$_\forall$, because $\forall\mathbf{y}\,\phi$ implies $\exists\mathbf{y}\,\phi$ over the reals, and so we get the "$\to$" direction for DG from the "$\to$" direction of DG$_\forall$. Conversely, we only need to prove the "$\leftarrow$" direction for DG, because the "$\leftarrow$" direction for DG$_\forall$ follows from it.

"$\to$" We need to show the RHS of DG$_\forall$ assuming its LHS. Let $\omega_{\mathbf{y}}^{\mathbf{d}}$ be identical to ω except where the values for $\mathbf{y}$ are replaced with any initial values $d \in \mathbb{R}^m$. Consider any solution $\varphi_{\mathbf{y}} : [0,T] \to \mathbb{S}$ where $\varphi_{\mathbf{y}}(0) = \omega_{\mathbf{y}}$ on $\{x',\mathbf{y}'\}^{\complement}$, $\varphi_{\mathbf{y}}(T) = \nu$, and $I, \varphi_{\mathbf{y}} \models x' = f(x), \mathbf{y}' = a(x) \cdot \mathbf{y} + b(x)\,\&\,Q(x)$.
Define $\varphi : [0,T] \to \mathbb{S}$ satisfying:

$$\varphi(t)(z) \overset{\text{def}}{=} \begin{cases}\varphi_{\mathbf{y}}(t)(z) & z \in \{\mathbf{y},\mathbf{y}'\}^{\complement}\\ \omega(z) & z \in \{\mathbf{y},\mathbf{y}'\}\end{cases}$$

In other words, φ is identical to $\varphi_{\mathbf{y}}$ except it holds all of $\mathbf{y},\mathbf{y}'$ constant at their initial values in ω. Observe that by construction, $\varphi(0) = \omega$ on $\{x'\}^{\complement}$, and moreover, because $\mathbf{y}$ is fresh i.e., not mentioned in $Q(x)$, $f(x)$, by coincidence for terms [15, Lemma 10], we have that:

$$I, \varphi \models x' = f(x)\,\&\,Q(x)$$

Therefore, $\varphi(T) \in I[\![P(x)]\!]$ from the LHS of DG$_\forall$. Since $\varphi(T)$ coincides with $\varphi_{\mathbf{y}}(T) = \nu$ except on $\{\mathbf{y},\mathbf{y}'\}$ and $\mathbf{y}$ is fresh, by coincidence for formulas [15, Lemma 11] we also have $\nu = \varphi_{\mathbf{y}}(T) \in I[\![P(x)]\!]$ as required.

"$\leftarrow$" We need to show the LHS of DG assuming its RHS. Consider a solution $\varphi : [0,T] \to \mathbb{S}$ where $\varphi(0) = \omega$ on $\{x'\}^{\complement}$, $\varphi(T) = \nu$, and $I, \varphi \models x' = f(x)\,\&\,Q(x)$. Let $\varphi_a(t) \overset{\text{def}}{=} I\varphi(t)[\![a(x)]\!]$, and $\varphi_b(t) \overset{\text{def}}{=} I\varphi(t)[\![b(x)]\!]$ be the valuation of $a(x), b(x)$ along φ respectively. Recall that $\varphi_a : [0,T] \to \mathbb{R}^m \times \mathbb{R}^m$ and $\varphi_b : [0,T] \to \mathbb{R}^m$.
By [15, Definition 5], $\varphi_a(t) = I(a)\big(I(\varphi(t))(x)\big)$, where $I(a)$ is continuous (and similarly for $\varphi_b(t)$). Since φ is a continuous function in t, both $\varphi_a(t), \varphi_b(t)$ are compositions of continuous functions, and are thus, also continuous functions in t. Consider the m-dimensional initial value problem:

$$\mathbf{y}' = \varphi_a(t)\mathbf{y} + \varphi_b(t), \quad \mathbf{y}(0) = \omega[\![\mathbf{y}]\!]$$

By [21, Chapter IV, Theorem 14.VI], there exists a unique solution $\psi : [0,T] \to \mathbb{R}^m$ for this system that is defined on the *entire* interval $[0,T]$. Therefore, we may construct the extended solution $\varphi_{\mathbf{y}}$ satisfying:

$$\varphi_{\mathbf{y}}(t)(z) \overset{\text{def}}{=} \begin{cases} \varphi(t)(z) & z \in \{\mathbf{y}, \mathbf{y}'\}^{\complement} \\ \psi(t)(z) & z \in \mathbf{y} \\ \frac{d\psi(t)(w)}{dt} & z = w' \in \mathbf{y}' \end{cases}$$

By definition, $\varphi_{\mathbf{y}}(0) = \omega$ on $\{x', \mathbf{y}'\}^{\complement}$, and by construction and coincidence for formulas [15, Lemma 11], $I, \varphi_{\mathbf{y}} \models x' = f(x), \mathbf{y}' = a(x) \cdot \mathbf{y} + b(x) \,\&\, Q(x)$. Thus, we have $\varphi_{\mathbf{y}}(T) \in I[\![P(x)]\!]$ from the RHS of DG. Since $\varphi(T)$ coincides with $\varphi_{\mathbf{y}}(T)$ except on $\mathbf{y}, \mathbf{y}'$, again by coincidence for formulas [15, Lemma 11] we have $\nu = \varphi(T) \in I[\![P(x)]\!]$ as required.

We now prove DMP. Consider an initial state ω satisfying both negative premises of DMP, i.e.,

① $\omega \in I[\![[x' = f(x) \,\&\, Q(x)](Q(x) \rightarrow R(x))]\!]$, and

② $\omega \in I[\![[x' = f(x) \,\&\, R(x)]P(x)]\!]$

We need to show $\omega \in I[\![[x' = f(x) \,\&\, Q(x)]P(x)]\!]$, i.e., for any solution $\varphi : [0, T] \rightarrow \mathbb{S}$ where $\varphi(0) = \omega$ on $\{x'\}^{\complement}$, and $I, \varphi \models x' = f(x) \,\&\, Q(x)$, we have $\varphi(T) \in I[\![P(x)]\!]$. By definition, we have $\varphi(t) \in I[\![Q(x)]\!]$ for $t \in [0, T]$, but by ①, we also have that $\varphi(t) \in I[\![Q(x) \rightarrow R(x)]\!]$ for all $t \in [0, T]$. Therefore, $\varphi(t) \in I[\![R(x)]\!]$ for all $t \in [0, T]$, and hence, $I, \varphi \models x' = f(x) \,\&\, R(x)$. Thus, by ②, we have $\varphi(T) \in I[\![P(x)]\!]$ as required. □

Using the axiomatization from Theorem A.2 and Lemma A.4, we now derive all of the rules shown in Theorem 2.1.

Proof of Theorem 2.1. For each rule, we show a derivation from the dL axioms. The open premises in these derivations correspond to the open premises for each rule.

dW We apply DMP and obtain two premises corresponding to the two formulas on the left of its implications. The right premise closes using DW. The left premise uses G, which leaves the open premise of dW.

$$\text{DMP}\dfrac{\text{G},\rightarrow\text{R}\dfrac{Q \vdash P}{\Gamma \vdash [x' = f(x) \,\&\, Q](Q \rightarrow P)} \qquad \text{DW}\dfrac{*}{\Gamma \vdash [x' = f(x) \,\&\, P]P}}{\Gamma \vdash [x' = f(x) \,\&\, Q]P}$$

$\text{dI}_=$ This rule follows from the $\text{DI}_=$ axiom, and also using the equivalence between Lie derivatives and differentials within the context of the ODEs.

$$\text{cut}\dfrac{[?],\rightarrow\text{R}\dfrac{\Gamma, Q \vdash p = 0}{\Gamma \vdash [?Q]p = 0} \qquad \text{cut,DI}_=\dfrac{\text{DE},e',\mathbb{R}\dfrac{\text{dW},\rightarrow\text{R}\dfrac{Q \vdash \dot{p} = 0}{\Gamma, Q \vdash [x' = f(x) \,\&\, Q]\dot{p} = 0}}{\Gamma, Q \vdash [x' = f(x) \,\&\, Q](p)' = 0}}{\Gamma, [?Q]p = 0 \vdash [x' = f(x) \,\&\, Q]p = 0}}{\Gamma \vdash [x' = f(x) \,\&\, Q]p = 0}$$

$\text{dI}_{\gtrsim}$ The derivation is similar to the previous case, using $\text{DI}_{\gtrsim}$ instead of $\text{DI}_=$.

dC We cut in a premise with the postcondition $Q \rightarrow (Q \wedge C)$. We reduce this postcondition to C by M[·] because $C \rightarrow (Q \rightarrow (Q \wedge C))$ is a valid formula. The right premise after the cut is abbreviated by ①.

$$\text{cut}\dfrac{\text{M}[\cdot]\dfrac{\Gamma \vdash [x' = f(x) \,\&\, Q]C}{\Gamma \vdash [x' = f(x) \,\&\, Q](Q \rightarrow (Q \wedge C))} \qquad ①}{\Gamma \vdash [x' = f(x) \,\&\, Q]P}$$

Continuing on ① we use DMP to refine the domain constraint, which leaves open the remaining premise of dC:

$$\text{DMP}\dfrac{\Gamma \vdash [x' = f(x) \,\&\, Q \wedge C]P}{\Gamma, [x' = f(x) \,\&\, Q](Q \rightarrow (Q \wedge C)) \vdash [x' = f(x) \,\&\, Q]P}$$

dG This follows by rewriting the RHS with (vectorial) DG.

$$\text{DG}\dfrac{\Gamma \vdash \exists \mathbf{y}\, [x' = f(x), \mathbf{y}' = a(x) \cdot \mathbf{y} + b(x) \,\&\, Q]P}{\Gamma \vdash [x' = f(x) \,\&\, Q]P}$$

□

We note, additionally, that $\text{dI}_=$ can be derived directly from $\text{DI}_{\gtrsim}$, using $[\cdot]\wedge$, and the real arithmetic equivalence $p = 0 \leftrightarrow p \geq 0 \wedge p \leq 0$. We refer readers to [15, Theorem 38] for a proof of soundness of $\text{DI}_{\gtrsim}$, which relies on the mean value theorem. Briefly, consider any solution $\varphi : [0, T] \rightarrow \mathbb{S}$, and let $\varphi_p(t) \overset{\text{def}}{=} I\varphi(t)[\![p]\!]$ be the valuation of p along φ. We may, without loss of generality, assume $T > 0$, and $\varphi_p(0) \gtrsim 0$. By the assumption on the left of the implication in $\text{DI}_{\gtrsim}$, $(p(x))' \geq 0$, which, by the differential lemma [15, Lemma 35], means that $\frac{d\varphi_p(t)}{dt}(\zeta) \geq 0$ for $0 \leq \zeta \leq T$. By the mean value theorem, we have $\varphi_p(T) = \varphi_p(0) + \frac{d\varphi_p(t)}{dt}(\zeta)(T - 0)$ for some $0 < \zeta < T$. Since $\varphi_p(0) \gtrsim 0, T > 0$, and $\frac{d\varphi_p(t)}{dt}(\zeta) \geq 0$, we therefore have $\varphi_p(T) \gtrsim 0$ as required. We can, conversely, obtain a version of the mean value theorem in dL:

Corollary A.5 (Mean Value Theorem)**.** *The following analogue of the mean value theorem is a derived axiom:*

$$\text{MVT}\ p \geq 0 \wedge \langle x' = f(x) \,\&\, Q \rangle p < 0 \rightarrow \langle x' = f(x) \,\&\, Q \rangle (p)' < 0$$

Proof. This follows immediately by taking contrapositives, dualizing with $\langle\cdot\rangle$, and then applying $\text{DI}_{\gtrsim}$.

$$\neg\text{L},\neg\text{R},\langle\cdot\rangle\dfrac{\text{cut},[?]\dfrac{\text{DI}_{\gtrsim}\dfrac{*}{[?Q]p \geq 0, [x' = f(x) \,\&\, Q](p)' \geq 0 \vdash [x' = f(x) \,\&\, Q]p \geq 0}}{p \geq 0, [x' = f(x) \,\&\, Q](p)' \geq 0 \vdash [x' = f(x) \,\&\, Q]p \geq 0}}{p \geq 0 \wedge \langle x' = f(x) \,\&\, Q \rangle p < 0 \vdash \langle x' = f(x) \,\&\, Q \rangle (p)' < 0}$$

□

Intuitively, this version of the mean value theorem asserts that if p changes sign from $p \geq 0$ to $p < 0$ along a solution, then its Lie derivative must have been negative somewhere along the solution.

A.3 Extended Axiomatization

We re-state the axioms shown in Section 5 as concrete instances and prove their soundness. Consequently, the axioms of Section 5 follow as uniform substitution instances.

For these proofs, we will often need to take truncations of solutions. Let $\varphi : [0, T] \rightarrow \mathbb{S}$ be a solution, we define the *truncation* of φ to a smaller interval as $\varphi|_t : [0, t] \rightarrow \mathbb{S}$, which is identical to φ on the interval $[0, t]$, for $0 \leq t \leq T$. For any solution $\varphi : [0, T] \rightarrow \mathbb{S}$, we write $\varphi([a, b]) \in I[\![P]\!]$ to mean $\varphi(\zeta) \in I[\![P]\!]$ for all $a \leq \zeta \leq b$. We use $\varphi((a, b))$ instead when the interval is open, and similarly for the half-open cases. For example, if φ obeys the evolution domain constraint Q on the interval $[0, T]$, we write $\varphi([0, T]) \in I[\![Q]\!]$. We will only use this notation when $[a, b]$ is a subinterval of $[0, T]$.

As we did in Section 5, we assume that the system of differential equations, $x' = f(x)$, already contains $t' = 1$, which makes t act as a clock that tracks the passage of time.

A.3.1 Existence, Uniqueness, and Continuity

We prove soundness for concrete versions of the axioms in Lemma 5.1.

Lemma A.6 (Existence, Uniqueness and Continuity)**.** *The following axioms are sound.*

$$\text{Uniq}\quad \begin{aligned}&\langle x' = f(x)\,\&\,Q_1(x)\rangle P_1(x) \land \langle x' = f(x)\,\&\,Q_2(x)\rangle P_2(x)\\ &\to \langle x' = f(x)\,\&\,Q_1(x) \land Q_2(x)\rangle (P_1(x) \lor P_2(x))\end{aligned}$$

$$\text{Cont}\quad t = t_0 \to (p(x) > 0 \to \langle x' = f(x)\,\&\,p(x) > 0\rangle t \neq t_0)$$

Proof. For the ODE system $x' = f(x)$, the RHSes, when interpreted as functions on x are continuously differentiable. Therefore, by the Picard-Lindelöf theorem [21, §10.VI], from *any* state ω, there is an interval $[0, \tau), \tau > 0$ on which there is a unique, continuous solution $\varphi : [0, \tau) \to \mathbb{S}$ with $\varphi(0) = \omega$. Moreover, the solution may be uniquely extended in time (to the right), up to its maximal open interval of existence [21, §10.IX].

We first prove axiom Uniq. Consider an initial state ω, satisfying both conjuncts on the left of the implication in Uniq. Expanding the definition of the diamond modality, this means that there exists two solutions from ω, $\varphi_1 : [0, T_1] \to \mathbb{S}$, $\varphi_2 : [0, T_2] \to \mathbb{S}$ where $I, \varphi_1 \models x' = f(x)\,\&\,Q_1(x), I, \varphi_2 \models x' = f(x)\,\&\,Q_2(x)$, with $\varphi(T_1) \in I[\![P_1]\!]$ and $\varphi(T_2) \in I[\![P_2(x)]\!]$.

Now let us first assume $T_1 \leq T_2$. Since both φ_1, φ_2 are solutions starting from ω, the uniqueness of solutions implies that $\varphi_1(t) = \varphi_2(t)$ for $t \in [0, T_1]$. Therefore, since $\varphi_2([0, T_2]) \in I[\![Q_2(x)]\!]$ and $T_1 \leq T_2$, we have $I, \varphi_1 \models x' = f(x)\,\&\,Q_1(x) \land Q_2(x)$. Since $\varphi_1(T) \in I[\![P_1(x)]\!]$, which implies $\varphi_1(T) \in I[\![(P_1(x) \lor P_2(x))]\!]$, we therefore have $\omega \in I[\![\langle x' = f(x)\,\&\,Q_1(x) \land Q_2(x)\rangle(P_1(x) \lor P_2(x))]\!]$.

The case for $T_2 < T_1$ is similar, except now we have $\varphi_2(T) \in I[\![P_2(x)]\!]$. In either case, we have the required RHS of Uniq:

$$\omega \in I[\![\langle x' = f(x)\,\&\,Q_1(x) \land Q_2(x)\rangle(P_1(x) \lor P_2(x))]\!]$$

Next, we prove axiom Cont. Consider an arbitrary initial state ω, with $\omega \in [\![p(x) > 0]\!]$ and $\omega \in [\![t = t_0]\!]$. In other words, we initially have $\omega(t) = \omega(t_0)$.

By the existence theorem, there is a solution $\varphi : [0, \tau) \to \mathbb{S}$, of the system $x' = f(x)$, with $\varphi(0) = \omega$ except on $\{x'\}^\complement$ and $\tau > 0$. Since $t' = 1$ and t_0 is held constant in the system of equations, the valuation of t satisfies $\varphi(\zeta)(t) = \omega(t_0) + \zeta$ along this solution.

When viewed as a function on x, $I[\![p(x)]\!]$ is a *continuous* function from $\mathbb{R}^n \to \mathbb{R}$ (recall that x is shorthand for $x_1, \ldots, x_n$). Moreover, the set $I[\![p(x) > 0]\!]$ is topologically open. Hence, viewing $\omega(x)$ as a point in $\mathbb{R}^n$, there exists $\epsilon > 0$ such that all points d in the open ball, $\|d - \omega(x)\| < \epsilon$, also satisfy $I[\![p(d)]\!] > 0$. In terms of states, this implies that all states ν where $\|\nu(x) - \omega(x)\| < \epsilon$ also satisfy $\nu \in I[\![p(x) > 0]\!]$.

Moreover, the solution $\varphi(\zeta)$ is by definition, differentiable, and hence continuous about $\zeta = 0$ for $x_1, \ldots, x_n$, which implies, for a sufficiently small $0 < \delta < \tau$, that $\|\varphi([0, \delta])(x) - \varphi(0)(x)\| < \epsilon$. Hence, $\varphi([0, \delta]) \in I[\![p(x) > 0]\!]$, and so the truncated solution $\varphi|_\delta$ satisfies $I, \varphi|_\delta \models x' = f(x)\,\&\,p(x) > 0$. Finally, since $\varphi|_\delta(\delta)(t) = \omega(t_0) + \delta > \omega(t_0) = \varphi|_\delta(\delta)(t_0)$, we have $\varphi|_\delta(\delta) \in I[\![t \neq t_0]\!]$, and so $\omega \in I[\![\langle x' = f(x)\,\&\,p(x) > 0\rangle t \neq t_0]\!]$ as required. □

From the proof for Cont, it is clear that we may also write $t > t_0$ in its postcondition. In fact, the choice $t' = 1$ was made for convenience: we only need some way to encode local progress. We also have used $t' = -1$, or even $t' = c$ for any constant $c \neq 0$.

A.3.2 Real Induction

We prove the symmetric real induction principle stated in Proposition 5.4. Variants of this principle can be found in [4].

Proof of Proposition 5.4. In the "$\Longleftarrow$" direction, if $S = [a, b]$, then S is inductive by definition. For the "$\Longrightarrow$" direction, let $S \subseteq [a, b]$ be inductive, i.e., we have:

① $a \in S$
② If $a \leq x < b$ and $x \in S$, then $[x, x + \epsilon] \subseteq S$ for some $0 < \epsilon$
③ If $a < x \leq b$ and $x \in S^\complement$, then $[x - \epsilon, x] \subseteq S^\complement$ for some $0 < \epsilon$, where we write $S^\complement$ for the complement $[a, b] \setminus S$.

Suppose that $S \neq [a, b]$, so that the set $S^\complement$ is non-empty. Let x be the infimum of $S^\complement$, and note that $x \in [a, b]$ since $[a, b]$ is left-closed. We consider various cases for x.

1. Case $x = a$. By properties ① and ②, $[x, x + \epsilon] \subseteq S, \epsilon > 0$, so $x + \epsilon$ is a greater lower bound of $S^\complement$ than x, contradiction.
2. Case $a < x, x \in S$. If $x = b$, then $S = [a, b]$, contradiction. Otherwise, $a < x < b$, then by ②, $[x, x + \epsilon] \subseteq S, \epsilon > 0$, so $x + \epsilon$ is a greater lower bound of $S^\complement$ than x, contradiction.
3. Case $a < x, x \in S^\complement$. By ③, there is $[x - \epsilon, x], \epsilon > 0$, but then $x - \epsilon \in S^\complement$, so x is not a lower bound of $S^\complement$, contradiction.

□

We now restate and prove a generalized, concrete version of the real induction axiom given in Lemma 5.5. This strengthened version includes the evolution domain constraint. We have removed the syntactic abbreviation in Section 5 for a precise statement here.

Lemma A.7. *The following real induction axiom is sound.*

$$\begin{aligned}\text{RInd\&}\ &[x' = f(x)\,\&\,Q(x)]P(x) \leftrightarrow\\ &(Q(x) \to P(x)) \land [x' = f(x)\,\&\,Q(x)]\forall t_0 \Big(t = t_0 \to\\ &\quad \big(P(x) \land \langle x' = f(x)\,\&\,Q(x)\rangle t \neq t_0 \to\\ &\qquad \langle x' = f(x)\,\&\,P(x)\rangle t \neq t_0\big) \land\\ &\quad \big(\neg P(x) \land \langle x' = -f(x)\,\&\,Q(x)\rangle t \neq t_0 \to\\ &\qquad \langle x' = -f(x)\,\&\,\neg P(x)\rangle t \neq t_0\big)\Big)\end{aligned}$$

Proof. We shall label the conjuncts after $\forall t_0 \Big(t = t_0 \to \ldots\Big)$ under the box modality on the RHS as follows:

$$P(x) \land \langle x' = f(x)\,\&\,Q(x)\rangle t \neq t_0 \to \langle x' = f(x)\,\&\,P(x)\rangle t \neq t_0 \quad (ⓐ)$$

$$\neg P(x) \land \langle x' = -f(x)\,\&\,Q(x)\rangle t \neq t_0 \to \langle x' = -f(x)\,\&\,\neg P(x)\rangle t \neq t_0 \quad (ⓑ)$$

Consider an initial state ω, we prove both directions of the axiom separately.

"$\to$" Assume that ⊛ $\omega \models [x' = f(x)\,\&\,Q(x)]P(x)$. If $\omega \in I[\![Q(x)]\!]$, then consider the solution of duration 0 which stays in $Q(x)$. By assumption ⊛, this solution is required to satisfy $P(x)$ at its endpoint, which is identical to ω except on $\{x'\}^\complement$, and so by coincidence for formulas [15, Lemma 11], $\omega \in I[\![P(x)]\!]$. Thus, $\omega \in I[\![Q(x) \to P(x)]\!]$.
Next, we prove the conjunction (ⓐ ∧ ⓑ) under the box modality. Consider any solution $\varphi : [0, T] \to \mathbb{S}$ starting from ω with $I, \varphi \models x' = f(x)\,\&\,Q(x)$. We may also assume $\varphi(T) \in I[\![t = t_0]\!]$.
For conjunct ⓑ we need to show:

$$\varphi(T) \in I[\![\neg P(x) \land \ldots \to \ldots]\!]$$

However, by assumption ⊛, we must have $\varphi(T) \in I[\![P(x)]\!]$, and therefore this conjunct is trivially true.

For the remaining conjunct ⓐ, we additionally assume that:

$$\varphi(T) \in I[\![P(x) \land \langle x' = f(x) \,\&\, Q(x)\rangle t \neq t_0]\!]$$

As we did in the proof of soundness for Cont, we identify t as the clock variable with initial value t_0. Unfolding the diamond modality, there is another solution $\psi : [0, \tau] \to \mathbb{S}$ starting from $\varphi(T)$ with $\psi(\tau) \in I[\![t \neq t_0]\!]$. We also have $I, \psi \models x' = f(x) \,\&\, Q(x)$. Note that $\psi(0) = \varphi(T)$ *exactly* rather than just on $\{x'\}^{\complement}$, because both of these states must have the appropriate values for the differential variables.
We now need to show:

$$\varphi(T) \in I[\![\langle x' = f(x) \,\&\, P(x)\rangle t \neq t_0]\!]$$

We shall directly show:

$$I, \psi \models x' = f(x) \,\&\, P(x)$$

In particular, since ψ already satisfies the requisite differential equations and $\psi(\tau) \in I[\![t \neq t_0]\!]$, it is sufficient to show that it stays in the evolution domain for its entire duration, i.e., $\psi([0, \tau]) \in I[\![P(x)]\!]$.
Let $0 \leq \zeta \leq \tau$ and consider the concatenated solution $\Phi : [0, T + \zeta] \to \mathbb{S}$ defined by:

$$\Phi(t) \stackrel{\text{def}}{=} \begin{cases} \varphi(t) & t \leq T \\ \psi(t - T) & t > T \end{cases}$$

Since ψ must uniquely extend φ [21, §10.IX], the concatenated solution Φ is a solution starting from ω, it solves the system $x' = f(x)$, and it stays in $Q(x)$ for its entire duration. Hence, by ⊛, $\Phi(T + \zeta) = \psi(\zeta) \in I[\![P(x)]\!]$ as required.

"$\leftarrow$" Assume that the RHS of the equivalence is true in state ω. If $\omega \notin I[\![Q(x)]\!]$ then we are done, because there are no solutions that stay in $Q(x)$ and so the box modality on the LHS is trivially satisfied. Otherwise, consider an arbitrary solution $\varphi : [0, T] \to \mathbb{S}$ starting from ω such that $I, \varphi \models x' = f(x) \,\&\, Q(x)$. We need to show $\varphi([0, T]) \in I[\![P(x)]\!]$. We will do this by showing that the subset $\{\zeta : \varphi(\zeta) \in I[\![P(x)]\!]\}$ is an inductive subset of $[0, T]$.

① We have $\omega = \varphi(0)$ except on $\{x'\}^{\complement}$ and $\omega \in I[\![Q(x)]\!]$. By the assumption $\omega \in I[\![Q(x) \to P(x)]\!]$, we have $\omega \in I[\![P(x)]\!]$. Thus, $\varphi(0) \in I[\![P(x)]\!]$ by coincidence for formulas [15, Lemma 11].

② Now, consider $0 \leq \zeta < T$, and suppose $\varphi(\zeta) \in I[\![P(x)]\!]$. We need to show $\varphi([\zeta, \zeta + \epsilon]) \in I[\![P(x)]\!]$ for some $\epsilon > 0$.
For notational simplicity, let $t_0 \stackrel{\text{def}}{=} \varphi(\zeta)(t)$, we instantiate the box modality on the RHS with $\varphi|_\zeta$, and the quantifier with t_0. We therefore, have $\varphi(\zeta) \in I[\![ⓐ]\!]$.
Observe that since $\zeta < T$, we may consider the solution that starts from state $\varphi(\zeta)$, i.e., $\psi : [0, T - \zeta]$, where $\psi(\tau) \stackrel{\text{def}}{=} \varphi(\tau + \zeta)$, and we have $I, \psi \models x' = f(x) \,\&\, Q(x)$. We also have $T - \zeta > 0$, and therefore, $\psi(T - \zeta) \in I[\![t \neq t_0]\!]$ by viewing t as the clock variable. In other words, we have $\varphi(\zeta) \in I[\![\langle x' = f(x) \,\&\, Q(x)\rangle t \neq t_0]\!]$. Therefore, we may discharge the implication in ⓐ to obtain:

$$\varphi(\zeta) \in I[\![\langle x' = f(x) \,\&\, P(x)\rangle t \neq t_0]\!]$$

Unfolding the diamond modality, gives us a solution, which by uniqueness, yields a truncation of ψ, $\psi|_\epsilon$, for some $\epsilon > 0$ which starts from $\varphi(\zeta)$ and satisfies $\psi|_\epsilon([0, \epsilon]) \in I[\![P(x)]\!]$.
Now, by definition, $\psi|_\epsilon(\tau)$ is equal to $\varphi(\tau + \zeta)$ for $0 \leq \tau \leq \epsilon$, which implies $\varphi([\zeta, \zeta + \epsilon]) \in I[\![P(x)]\!]$ as required.

③ In this case, we consider $0 < \zeta \leq T$, and suppose $\varphi(\zeta) \in I[\![\neg P(x)]\!]$. We need to show $\varphi([\zeta - \epsilon, \zeta]) \in I[\![\neg P(x)]\!]$ for $\epsilon > 0$. This is essentially symmetric to ② by the fact that time-reversed solutions of differential equations satisfy the negated system $x' = -f(x)$. Note that we have $t' = -1$ here. We let $t_0 \stackrel{\text{def}}{=} \varphi(\zeta)(t)$, and instantiate the RHS to obtain $\varphi(\zeta) \in I[\![ⓑ]\!]$.
Since $0 < \zeta$, let us consider $\psi : [0, \zeta]$, where

$$\psi(\tau)(z) \stackrel{\text{def}}{=} \begin{cases} \varphi(\zeta - \tau)(z) & z \in \{x'\}^{\complement} \\ -\varphi(\zeta - \tau)(z) & z \in \{x'\} \end{cases}$$

In other words, ψ is the time-reversed solution starting from $\varphi(\zeta)$ and following the system $x' = -f(x)$. Note that in the case for $z \in \{x'\}$, we have explicitly negated the signs of the differential variables along ψ. This is needed to ensure that the differential variables match the RHS of $x' = -f(x)$. By a similar argument to the previous case, ψ is a witness for $\varphi(\zeta) \in I[\![\langle x' = -f(x) \,\&\, Q(x)\rangle t \neq t_0]\!]$, and thus, from the implication in ⓑ we have:

$$\varphi(\zeta) \in I[\![\langle x' = -f(x) \,\&\, \neg P(x)\rangle t \neq t_0]\!]$$

By uniqueness, this gives a truncation $\psi|_\epsilon$, for some $\epsilon > 0$, which starts (backwards) from $\varphi(\zeta)$ and satisfies $\psi|_\epsilon([0, \epsilon]) \in I[\![\neg P(x)]\!]$. This gives us $\varphi([\zeta - \epsilon, \zeta] \in I[\![\neg P(x)]\!]$ as required.

□

We shall work with the following derived real induction rule (with two premises). It derives directly from RInd& using dW. The derived rule rInd follows as a special case, where we ignore the antecedents involving the evolution domain Q.

$$\text{rInd\&}\ \frac{t = t_0, Q, \big\langle x' = f(x) \,\&\, Q\big\rangle\circ, P \vdash \big\langle x' = f(x) \,\&\, P\big\rangle\circ \qquad t = t_0, Q, \big\langle x' = -f(x) \,\&\, Q\big\rangle\circ, \neg P \vdash \big\langle x' = -f(x) \,\&\, \neg P\big\rangle\circ}{P \vdash [x' = f(x) \,\&\, Q]P}$$

A.4 Diamond Modality Rules and Axioms

We derive the rules and axioms from Corollary 5.2, along with an additional derived rule that is used in the appendix.

Corollary A.8 (Derived diamond modality rules and axioms)**.** *In addition to the derived rules and axioms in Corollary 5.2, the following derived rule is sound:*

$$\text{M}\langle\cdot\rangle\ \frac{\Gamma \vdash [\alpha](\phi_2 \to \phi_1) \qquad \Gamma \vdash \langle\alpha\rangle\phi_2}{\Gamma \vdash \langle\alpha\rangle\phi_1}$$

Proof (includes proof of Corollary 5.2). For each rule, we show a derivation from the dL axioms. The open premises in these derivations correspond to the open premises for each rule.

$\langle\cdot\rangle$dR This follows by dualizing with the $\langle\cdot\rangle$ axiom.

$$\text{cut}\ \frac{\Gamma \vdash \langle x' = f(x) \,\&\, R\rangle P \qquad \langle\cdot\rangle,\neg\text{R},\neg\text{L}\ \dfrac{\text{DMP,DW}\ \dfrac{\Gamma \vdash [x' = f(x) \,\&\, R]Q}{\Gamma, [x' = f(x) \,\&\, Q]\neg P \vdash [x' = f(x) \,\&\, R]\neg P}}{\Gamma, \langle x' = f(x) \,\&\, R\rangle P \vdash \langle x' = f(x) \,\&\, Q\rangle P}}{\Gamma \vdash \langle x' = f(x) \,\&\, Q\rangle P}$$

$\langle\cdot\rangle$dRW This follows from $\langle\cdot\rangle$dR by simplifying its left premise with dW.

&∧ This follows from $\langle\cdot\rangle$dRW for the "→" direction, because $Q \land R \rightarrow Q$ and $Q \land R \rightarrow R$ are both valid formulas. The "←" direction is an immediate instance of Uniq by setting P_1, P_2 to P, and Q_1, Q_2 to Q, R respectively.

M⟨·⟩ This follows from K by dualizing its inner implication with the $\langle\cdot\rangle$ axiom.

$$\langle\cdot\rangle,\mathrm{K}\frac{\Gamma \vdash [\alpha](\phi_2 \rightarrow \phi_1) \qquad \Gamma \vdash \langle\alpha\rangle\phi_2}{\Gamma \vdash \langle\alpha\rangle\phi_1}$$

□

B Completeness for Semialgebraic Invariants and Evolution Domain Constraints

This section gives the full completeness arguments for dRI and sAI. With the extended axiomatization, we may prove the completeness direction of dRI and (most of) sAI within dL. We take this syntactic approach here to demonstrate the versatility of the dL calculus. We refer the readers to other presentations [7, 9] for purely semantical completeness arguments. As usual, we will assume that $x' = f(x)$ already contains a clock equation $t' = 1$. We will, however, need to make more use of this specific choice here.

We start with the following definition due to [9], which summarizes the formulas in the premises of sAI. It lifts the progress and differential radical formulas for single polynomials to the general case of an arbitrary semialgebraic formula written in normal form.

Definition B.1 (Semialgebraic progress formula)**.** The semialgebraic progress formula $\dot{P}^{(*)}$ for a semialgebraic formula P written in normal form (2) is defined as follows:

$$\dot{P}^{(*)} \overset{\text{def}}{\equiv} \bigwedge_{i=0}^{M} \Big(\bigvee_{j=0}^{m(i)} \dot{p_{ij}}^{(*)} = 0 \lor \bigvee_{j=0}^{n(i)} \dot{q_{ij}}^{(*)} > 0 \Big)$$

We write $\dot{P}^{(-*)}$ when taking Lie derivatives with respect to $x' = -f(x)$ instead.

We note that the syntactic form of semialgebraic progress formula for P depends on the choice of normal form. This choice will always be made clear in the context when we refer $\dot{P}^{(*)}$.

We first make the following useful observation on various rearrangements of the progress and differential radical formulas for polynomials:

Proposition B.2. *Let N be the order of q. The following are valid equivalences on the progress and differential radical formulas.*

$$\begin{aligned}
\dot{q}^{(*)} > 0 \leftrightarrow & q > 0 \lor (q = 0 \land \dot{q} > 0) \\
& \lor \dots \\
& \lor \big(q = 0 \land \dot{q} = 0 \land \dots \land \dot{q}^{(N-2)} = 0 \land \dot{q}^{(N-1)} > 0\big) \\
\neg(\dot{q}^{(*)} = 0) \leftrightarrow & \dot{q}^{(*)} > 0 \lor \dot{(-q)}^{(*)} > 0 \\
\neg(\dot{q}^{(*)} > 0) \leftrightarrow & \dot{(-q)}^{(*)} > 0 \lor \dot{q}^{(*)} = 0
\end{aligned}$$

Proof. All of these equivalences follow immediately by unfolding the definitions of the progress and differential radical formulas, applying logical rearrangements and real arithmetic identities. □

The latter two equivalences are particularly important, as we show in the next proposition.

Proposition B.3. *Let P be in normal form:*

$$P \equiv \bigwedge_{i=0}^{M} \Big(\bigvee_{j=0}^{m(i)} p_{ij} = 0 \lor \bigvee_{j=0}^{n(i)} q_{ij} > 0 \Big)$$

$\neg P$ can be put in a normal form:

$$\neg P \equiv \bigwedge_{i=0}^{N} \Big(\bigvee_{j=0}^{a(i)} r_{ij} = 0 \lor \bigvee_{j=0}^{b(i)} s_{ij} > 0 \Big)$$

for which we additionally have the valid equivalence:

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

Proof. We start by applying negating P (in normal form), and applying the arithmetic identities $p \neq 0 \leftrightarrow p > 0 \lor -p > 0$ and $q \leq 0 \leftrightarrow -q > 0 \lor q = 0$ to obtain the valid formula:

$$\neg P \leftrightarrow \underbrace{\bigvee_{i=0}^{M} \Big(\bigwedge_{j=0}^{m(i)} (p_{ij} > 0 \lor -p_{ij} > 0) \land \bigwedge_{j=0}^{n(i)} (-q_{ij} > 0 \lor q = 0) \Big)}_{\phi}$$

Expanding and negating the progress formula for P, we have the valid equivalence:

$$\begin{aligned}
&\neg \bigwedge_{i=0}^{M} \Big(\bigvee_{j=0}^{m(i)} \dot{p_{ij}}^{(*)} = 0 \lor \bigvee_{j=0}^{n(i)} \dot{q_{ij}}^{(*)} > 0 \Big) \leftrightarrow \\
&\bigvee_{i=0}^{M} \Big(\bigwedge_{j=0}^{m(i)} \neg \dot{p_{ij}}^{(*)} = 0 \land \bigwedge_{j=0}^{n(i)} \neg \dot{q_{ij}}^{(*)} > 0 \Big)
\end{aligned}$$

The RHS of this equivalence can be rewritten with the latter two equivalences from Proposition B.2 to obtain the following formula, which we label as ψ:

$$\begin{aligned}
\psi \overset{\text{def}}{\equiv} \bigvee_{i=0}^{M} \Big(& \bigwedge_{j=0}^{m(i)} \big(\dot{p_{ij}}^{(*)} > 0 \lor \dot{(-p_{ij})}^{(*)} > 0\big) \land \\
& \bigwedge_{j=0}^{n(i)} \big(\dot{(-q_{ij})}^{(*)} > 0 \lor \dot{q_{ij}}^{(*)} = 0\big) \Big)
\end{aligned}$$

Observe that ϕ, ψ have the same disjunctive normal form shape. We distribute the outer disjunction over the inner conjunctions in ϕ to obtain the following valid equivalence, whose RHS is a normal form for $\neg P$ (for some indices $N, a(i), b(i)$ and polynomials r_{ij}, s_{ij}):

$$\neg P \leftrightarrow \bigwedge_{i=0}^{N} \Big(\bigvee_{j=0}^{a(i)} r_{ij} = 0 \lor \bigvee_{j=0}^{b(i)} s_{ij} > 0 \Big)$$

We distribute the disjunction in ψ following the same syntactic steps taken in ϕ to obtain the following valid equivalence:

$$\psi \leftrightarrow \bigwedge_{i=0}^{N} \Big(\bigvee_{j=0}^{a(i)} \dot{r_{ij}}^{(*)} = 0 \lor \bigvee_{j=0}^{b(i)} \dot{s_{ij}}^{(*)} > 0 \Big)$$

By rewriting with the equivalences derived so far, and using the above normal form for $\neg P$, we have the required, valid equivalence:

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

□

B.1 Algebraic Invariants

We now derive axiom DRI from Theorem 4.4.

Proof of Theorem 4.4. In the "$\leftarrow$" direction, we use dRI, by setting N to the order of p, so that the succedent of its left premise is exactly $\dot{p}^{(*)} = 0$. The right premise closes by real arithmetic, since N is the order of p, it must, by definition satisfy the identity (1).

$$\text{dRI}\ \dfrac{\text{$\to$L}\ \dfrac{*}{Q \to \dot{p}^{(*)} = 0, Q \vdash \dot{p}^{(*)} = 0} \qquad \mathbb{R}\ \dfrac{*}{\vdash \dot{p}^{(N)} = \sum_{i=0}^{N-1} g_i \dot{p}^{(i)}}}{Q \to \dot{p}^{(*)} = 0 \vdash [x' = f(x) \,\&\, Q]p = 0}$$

For the "$\to$" direction, we first reduce to the contrapositive statement by logical manipulation. An application of $\langle\cdot\rangle$ turns the negated box modality in the succedent to a diamond modality. Finally, by Proposition B.2, we equivalently rewrite the negated differential radical formula in the antecedents. We refer to the open premise with ①.

$$\dfrac{\langle\cdot\rangle\ \dfrac{\mathbb{R}\ \dfrac{Q, (\dot{p}^{(*)} > 0 \lor \dot{(-p)}^{(*)} > 0) \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}{Q, \neg(\dot{p}^{(*)} = 0) \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}}{Q, \neg(\dot{p}^{(*)} = 0) \vdash \neg[x' = f(x) \,\&\, Q]p = 0}}{[x' = f(x) \,\&\, Q]p = 0 \vdash Q \to \dot{p}^{(*)} = 0}$$

Since Q characterizes an open, semialgebraic set, by the finiteness theorem [2, Theorem 2.7.2] for open semialgebraic sets, Q may be written as follows (q_{ij} are polynomials):

$$Q \equiv \bigwedge_{i=0}^{M} \bigvee_{j=0}^{m(i)} q_{ij} > 0$$

Thus, we have the following derivation. As usual, we have collapsed similar cases (indexed by i) after the $\&\land$,$\land$L step. All the premises close using cont^o.

$$\mathbb{R}\ \dfrac{\&\land,\land\text{L}\ \dfrac{\text{cont}^o\ \dfrac{*}{t = t_0, \bigvee_{j=0}^{m(i)} q_{ij} > 0 \vdash \left\langle x' = f(x) \,\&\, \bigvee_{j=0}^{m(i)} q_{ij} > 0\right\rangle \circ}}{t = t_0, \bigwedge_{i=0}^{M} \bigvee_{j=0}^{m(i)} q_{ij} > 0 \vdash \left\langle x' = f(x) \,\&\, \bigwedge_{i=0}^{M} \bigvee_{j=0}^{m(i)} q_{ij} > 0\right\rangle \circ}}{t = t_0, Q \vdash \langle x' = f(x) \,\&\, Q\rangle \circ}$$

We are now ready to continue from ①. In the first step, we introduce a clock variable satisfying $t = t_0$ initially using dG,$\exists$R. Next, using the derivation above, we cut in local progress for Q. We then use $\lor$L to case split on the disjunction $\dot{p}^{(*)} > 0 \lor \dot{(-p)}^{(*)} > 0$. The resulting premises are labelled ② and ③.

$$\text{dG},\exists\text{R}\ \dfrac{\text{cut}\ \dfrac{\lor\text{L}\ \dfrac{② \qquad ③}{t = t_0, \langle x' = f(x) \,\&\, Q\rangle \circ, \dot{p}^{(*)} > 0 \lor \dot{(-p)}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}}{t = t_0, Q, \dot{p}^{(*)} > 0 \lor \dot{(-p)}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}}{Q \land (\dot{p}^{(*)} > 0 \lor \dot{(-p)}^{(*)} > 0) \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}$$

Continuing on ②, because we already have $\dot{p}^{(*)} > 0$ in the antecedents, using lp$_{=\lor>}$, we may cut $\langle x' = f(x) \,\&\, t = t_0 \lor p > 0\rangle \circ$. Now, by an application of $\&\land$, we combine the two local progress formulas in the antecedent.

$$\text{cut,lp}_{=\lor>}\ \dfrac{\&\land\ \dfrac{\langle x' = f(x) \,\&\, Q \land (t = t_0 \lor p > 0)\rangle \circ \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}{\langle x' = f(x) \,\&\, Q\rangle \circ, \langle x' = f(x) \,\&\, t = t_0 \lor p > 0\rangle \circ \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}}{t = t_0, \langle x' = f(x) \,\&\, Q\rangle \circ, \dot{p}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}$$

Next, because $\overbrace{Q \land (t = t_0 \lor p > 0)}^{R} \to Q$, we use $\langle\cdot\rangle$dRW to strengthen the evolution domain constraint in the succedent. This allows us to use M$\langle\cdot\rangle$, whose right premise closes trivially. Removing the syntactic abbreviation for $\circ$ allows us to close the premise using dW, because we have $t = t_0 \lor p > 0$ in the domain constraint R.

$$\langle\cdot\rangle\text{dRW}\ \dfrac{\text{M}\langle\cdot\rangle\ \dfrac{\text{dW}\ \dfrac{\mathbb{R}\ \dfrac{*}{R \vdash (t \neq t_0 \to p \neq 0)}}{\vdash [x' = f(x) \,\&\, R](t \neq t_0 \to p \neq 0)}}{\langle x' = f(x) \,\&\, R\rangle \circ \vdash \langle x' = f(x) \,\&\, R\rangle p \neq 0}}{\langle x' = f(x) \,\&\, R\rangle \circ \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}$$

The remaining premise ③ follows similarly, except that the progress formula $\dot{(-p)}^{(*)} > 0$ enables the cut $\langle x' = f(x) \,\&\, t = t_0 \lor -p > 0\rangle \circ$. It leads to the same conclusion of $p \neq 0$ in the postcondition. □

We now prove Corollary 4.5 using the characterization of algebraic invariants of ODEs from Theorem 4.4. The test-free fragment of dL programs is generated by the following grammar, where we have omitted tests, and evolution domain constraints:

$$\alpha ::= x := e \mid x' = f(x) \mid \alpha_1 \cup \alpha_2 \mid \alpha_1; \alpha_2 \mid \alpha^*$$

Proof of Corollary 4.5. Firstly, since P is algebraic, it is equivalent to a formula $p = 0$ for some polynomial p so we may, without loss of generality, assume that it is written in this form.

We proceed by structural induction on the form of test-free α, and show that for some (computable) polynomial q, we can derive the equivalence $[\alpha]p = 0 \leftrightarrow q = 0$ in dL.

- Case $x' = f(x)$. By Theorem 4.4, since the set of all states (i.e., the evolution domain *true*) is open, by DRI, we have the derived equivalence $[x' = f(x)]p = 0 \leftrightarrow \dot{p}^{(*)} = 0$. Let N be the order of p so that $\dot{p}^{(*)} = 0$ expands to $\bigwedge_{i=0}^{N-1} \dot{p}^{(i)} = 0$. Let $q \overset{\text{def}}{=} \sum_{i=0}^{N-1} (\dot{p}^{(i)})^2$ so that we have the valid arithmetic equivalence $\dot{p}^{(*)} = 0 \leftrightarrow q = 0$. Rewriting with this derives the desired equivalence, $[x' = f(x)]p = 0 \leftrightarrow q = 0$.
- Case $x := e$. By [:=], $[x := e]p(x) = 0 \leftrightarrow p(e) = 0$. As a composition of polynomials, $p(e)$ is a polynomial.
- Case $\alpha_1 \cup \alpha_2$. By [$\cup$], $[\alpha_1 \cup \alpha_2]p = 0 \leftrightarrow [\alpha_1]p = 0 \land [\alpha_2]p = 0$. By the induction hypothesis on α_1, α_2, we may derive $[\alpha_1]p = 0 \leftrightarrow q_1 = 0$ and $[\alpha_2]p = 0 \leftrightarrow q_2 = 0$ for some polynomials q_1, q_2. Moreover, $q_1 = 0 \land q_2 = 0 \leftrightarrow q_1^2 + q_2^2 = 0$ is a valid formula of real arithmetic. Rewriting with the derived logical equivalences yields the derived equivalence: $[\alpha_1 \cup \alpha_2]p = 0 \leftrightarrow q_1^2 + q_2^2 = 0$.
- Case $\alpha_1; \alpha_2$. By [;], $[\alpha_1; \alpha_2]p = 0 \leftrightarrow [\alpha_1][\alpha_2]p = 0$. By the induction hypothesis on α_2, we derive $[\alpha_2]p = 0 \leftrightarrow q_2 = 0$. By rewriting with this equivalence, we derive $[\alpha_1; \alpha_2]p = 0 \leftrightarrow [\alpha_1]q_2 = 0$. Now, by the induction hypothesis on α_1, we derive $[\alpha_1]q_2 = 0 \leftrightarrow q_1 = 0$ for some q_1. Rewriting with the derived logical equivalences yields the derived equivalence $[\alpha_1; \alpha_2]p = 0 \leftrightarrow q_1 = 0$.
- Case α^*. This case relies on the fact that the polynomial ring $\mathbb{R}[x]$ (and $\mathbb{Q}[x]$) over a finite number of indeterminates x is a Noetherian domain, which implies that every ascending chain of ideals is finite. We first construct the following sequence of polynomials q_i:

  $$q_0 \overset{\text{def}}{=} p, \quad q_{i+1} \overset{\text{def}}{=} f_i$$

  where f_i is the polynomial satisfying the derived equivalence $f_i \leftrightarrow [\alpha]q_i = 0$ obtained by applying the induction hypothesis on α with postcondition $q_i = 0$.
  Since the ring of polynomials over the (finite set) of variables mentioned in α or p is Noetherian, the following chain of

ideals is finite:

$$(q_0) \subset (q_0, q_1) \subset (q_0, q_1, q_2) \subset \dots$$

Thus, there is some smallest k such that q_k satisfies the following polynomial identity, with polynomial cofactors g_i:

$$q_k = \sum_{i=0}^{k-1} g_i q_i$$

We claim that $\bigwedge_{i=0}^{k-1} q_i = 0 \leftrightarrow [\alpha^*]p = 0$ is derivable. Since we also have the valid equivalence $\sum_{i=0}^{k-1} q_i^2 = 0 \leftrightarrow \bigwedge_{i=0}^{k-1} q_i = 0$, this claim yields the derived equivalence $[\alpha^*]p = 0 \leftrightarrow \sum_{i=0}^{k-1} q_i^2 = 0$, as required. We show both directions of the claim separately.

"$\rightarrow$" We strengthen the postcondition of the box modality to $\bigwedge_{i=0}^{k-1} q_i = 0$ (recall that $q_0 \overset{\text{def}}{=} p$, so $\bigwedge_{i=0}^{k-1} q_i = 0 \rightarrow p = 0$ is valid), and prove it as a loop invariant. By an application of $[\cdot]\wedge$ followed by $\wedge$R, we may split the postcondition to its constituent conjuncts (indexed by $0 \le i \le k-1$). We observe that, by construction, we can equivalently replace each $[\alpha]q_i$ with q_{i+1}.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\bigwedge_{i=0}^{k-1} q_i = 0 \vdash q_{i+1} = 0}{\bigwedge_{i=0}^{k-1} q_i = 0 \vdash [\alpha]q_i = 0}}{\bigwedge_{i=0}^{k-1} q_i = 0 \vdash \bigwedge_{i=0}^{k-1} [\alpha]q_i = 0}\ \wedge\text{R}}{\bigwedge_{i=0}^{k-1} q_i = 0 \vdash [\alpha] \bigwedge_{i=0}^{k-1} q_i = 0}\ [\cdot]\wedge}{\bigwedge_{i=0}^{k-1} q_i = 0 \vdash [\alpha^*] \bigwedge_{i=0}^{k-1} q_i = 0}\ \text{loop}}{\bigwedge_{i=0}^{k-1} q_i = 0 \vdash [\alpha^*]p = 0}\ \text{M}[\cdot]$$

The open premises where $0 \le i < k-1$ close trivially because $q_i = 0$ is already in the antecedent. The final case where $i = k-1$ is where we need to show $q_k = 0$ in the succedent. However, because we have the polynomial identity $q_k = \sum_{i=0}^{k-1} g_i q_i$, the final premise also closes by a cut and real arithmetic.

$$\dfrac{\dfrac{*}{\bigwedge_{i=0}^{k-1} q_i = 0 \vdash \sum_{i=0}^{k-1} g_i q_i = 0}\ \mathbb{R} \qquad \dfrac{*}{\vdash q_k = \sum_{i=0}^{k-1} g_i q_i}\ \mathbb{R}}{\bigwedge_{i=0}^{k-1} q_i = 0 \vdash q_k = 0}\ \text{cut}$$

"$\leftarrow$" This direction is straightforward using k times the iteration axiom $[^*]$ together with $[\cdot]\wedge$. By construction, we may replace the antecedents with q_i, which gives us the required implication.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{q_0 = 0 \wedge q_1 = 0 \wedge q_2 = 0 \wedge \dots \wedge q_{k-1} = 0 \vdash \bigwedge_{i=0}^{k-1} q_i = 0}}{p = 0 \wedge [\alpha]p = 0 \wedge [\alpha][\alpha]p = 0 \wedge \cdots \vdash \bigwedge_{i=0}^{k-1} q_i = 0}}{\dots}\ [^*],[\cdot]\wedge}{p = 0 \wedge [\alpha]p = 0 \wedge [\alpha][\alpha][\alpha^*]p = 0 \vdash \bigwedge_{i=0}^{k-1} q_i = 0}\ [^*],[\cdot]\wedge}{p = 0 \wedge [\alpha][\alpha^*]p = 0 \vdash \bigwedge_{i=0}^{k-1} q_i = 0}\ [^*],[\cdot]\wedge}{[\alpha^*]p = 0 \vdash \bigwedge_{i=0}^{k-1} q_i = 0}\ [^*]$$

□

B.2 Local Progress

Fixing a normal form (2) for P, the following axiom derives from dL extended with Cont,Uniq.

$$\text{lp}\mathbb{R}_{\rightarrow}\ \ t = t_0 \wedge P \wedge \dot{P}^{(*)} \rightarrow \langle x' = f(x) \,\&\, P\rangle\circ$$

This follows by a direct application of lp$\mathbb{R}$, whose premise closes because the succedent is exactly $\dot{P}^{(*)}$.

$$\dfrac{\dfrac{*}{t = t_0 \wedge P \wedge \dot{P}^{(*)} \vdash \bigwedge_{i=0}^{M} \big(\bigvee_{j=0}^{m(i)} \dot{p_{ij}}^{(*)} = 0 \vee \bigvee_{j=0}^{n(i)} \dot{q_{ij}}^{(*)} > 0\big)}}{t = t_0 \wedge P \wedge \dot{P}^{(*)} \vdash \langle x' = f(x) \,\&\, P\rangle\circ}\ \text{lp}\mathbb{R}$$

Note that we have explicitly included $t = t_0$ here, although it was left implicit in the antecedents when we derived lp$\mathbb{R}$. We now derive a converse implication.

Lemma B.4 (Semialgebraic local progress, converse implication)**.** *Let P be a semialgebraic formula in normal form* (2)*. The following axiom derives from* dL *extended with Cont,Uniq.*

$$\text{lp}\mathbb{R}_{\leftarrow}\ \ t = t_0 \wedge \langle x' = f(x) \,\&\, P\rangle\circ \rightarrow \dot{P}^{(*)}$$

Proof. By Proposition B.3, there is a normal form for $\neg P$, i.e.,

$$\neg P \equiv \bigwedge_{i=0}^{N} \Big(\bigvee_{j=0}^{a(i)} r_{ij} = 0 \vee \bigvee_{j=0}^{b(i)} s_{ij} > 0 \Big)$$

where we additionally have the valid equivalence:

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

We first reduce to the contrapositive statement by logical manipulation, and then use the above normal form to rewrite the negation in the antecedents. We refer to the open premise with ①.

$$\dfrac{\dfrac{t = t_0, \dot{(\neg P)}^{(*)} \vdash \neg\langle x' = f(x) \,\&\, P\rangle\circ}{t = t_0, \neg(\dot{P}^{(*)}) \vdash \neg\langle x' = f(x) \,\&\, P\rangle\circ}\ \mathbb{R}}{t = t_0 \wedge \langle x' = f(x) \,\&\, P\rangle\circ \vdash \dot{P}^{(*)}}$$

We have the following valid equivalence, where the RHS is a normal form for $\neg P \vee t - t_0 = 0$. It is obtained by distributing $t - t_0 = 0$ over the conjunction in $\neg P$:

$$\neg P \vee t - t_0 = 0 \leftrightarrow \bigwedge_{i=0}^{N} \Big(\bigvee_{j=0}^{a(i)} r_{ij} = 0 \vee t - t_0 = 0 \vee \bigvee_{j=0}^{b(i)} s_{ij} > 0 \Big)$$

The progress formula for $\neg P \vee t - t_0 = 0$ in this normal form is:

$$\bigwedge_{i=0}^{N} \Big(\bigvee_{j=0}^{a(i)} \dot{r_{ij}}^{(*)} = 0 \vee \dot{(t - t_0)}^{(*)} = 0 \bigvee_{j=0}^{b(i)} \dot{s_{ij}}^{(*)} > 0 \Big)$$

Now, we consider the polynomial $t - t_0$. Since $t' = 1$, the first Lie derivative of $t - t_0$ is 1, which gives the valid equivalence $\dot{(t - t_0)}^{(*)} = 0 \leftrightarrow \textit{false}$ because the LHS contains an unsatisfiable conjunct $1 = 0$. Rewriting with this equivalence yields the valid equivalence $\dot{(\neg P \vee t - t_0 = 0)}^{(*)} \leftrightarrow \dot{(\neg P)}^{(*)}$.

We therefore, have the following derivation, whose conclusion we label ②. In the first cut step, we use the valid implication $t = t_0 \rightarrow \neg P \vee t - t_0 = 0$. We then use the equivalence above to replace the progress formula in the antecedents before closing with lp$\mathbb{R}_{\rightarrow}$.

$$\dfrac{\dfrac{\dfrac{*}{t = t_0, \neg P \vee t - t_0 = 0, \dot{(\neg P \vee t - t_0 = 0)}^{(*)} \vdash \langle x' = f(x) \,\&\, \neg P \vee t - t_0 = 0\rangle\circ}\ \text{lp}\mathbb{R}_{\rightarrow}}{t = t_0, \neg P \vee t - t_0 = 0, \dot{(\neg P)}^{(*)} \vdash \langle x' = f(x) \,\&\, \neg P \vee t - t_0 = 0\rangle\circ}\ \mathbb{R}}{t = t_0, \dot{(\neg P)}^{(*)} \vdash \langle x' = f(x) \,\&\, \neg P \vee t - t_0 = 0\rangle\circ}\ \text{cut}$$

We may now complete the derivation from ①. We first cut in ② using the derivation above. Next, we combine the evolution domain constraints using $\&\wedge$.

$$\dfrac{② \qquad \dfrac{\dfrac{\langle x' = f(x) \,\&\, (\neg P \vee t - t_0 = 0) \wedge P\rangle\circ \vdash \textit{false}}{\langle x' = f(x) \,\&\, \neg P \vee t - t_0 = 0\rangle\circ, \langle x' = f(x) \,\&\, P\rangle\circ \vdash \textit{false}}\ \&\wedge}{\langle x' = f(x) \,\&\, \neg P \vee t - t_0 = 0\rangle\circ \vdash \neg\langle x' = f(x) \,\&\, P\rangle\circ}\ \neg\text{R}}{t = t_0, \dot{(\neg P)}^{(*)} \vdash \neg\langle x' = f(x) \,\&\, P\rangle\circ}\ \text{cut}$$

We continue by dualizing with $\langle\cdot\rangle$, and finish the proof with dW and arithmetic.

$$
\scriptstyle{\langle\cdot\rangle,\neg L}\dfrac{\scriptstyle{dW}\dfrac{\mathbb{R}\dfrac{*}{(\neg P \lor t - t_0 = 0) \land P \vdash t = t_0}}{\vdash [x' = f(x)\,\&\,(\neg P \lor t - t_0 = 0) \land P]t = t_0}}{\langle x' = f(x)\,\&\,(\neg P \lor t - t_0 = 0) \land P\rangle\circ \vdash false}
$$

∎

The above proof used the following valid equivalence where P is in normal form, and we normalize $P \lor t - t_0 = 0$ by distributing $t - t_0$ over the outer conjunction in P:

$$
(P \lor t \mathbin{\dot{-}} t_0 = 0)^{(*)} \leftrightarrow \dot{P}^{(*)} \tag{4}
$$

This equivalence allows us to give a complete characterization of local progress for semialgebraic formulas.

Theorem B.5 (Semialgebraic local progress completeness)**.** *Let P be a semialgebraic formula in normal form* (2)*. The following axiom derives from* dL *extended with Cont,Uniq.*

$$
\text{lp}\mathbb{R}_{\leftrightarrow}\; t = t_0 \rightarrow \left(\dot{P}^{(*)} \leftrightarrow \langle x' = f(x)\,\&\,P \lor t = t_0\rangle\circ\right)
$$

Proof. We derive both directions separately. In both cases, (4) is used crucially. First in the "←" direction, we use $\text{lp}\mathbb{R}_{\leftarrow}$ and (4).

$$
\scriptstyle{\text{lp}\mathbb{R}_{\leftarrow}}\dfrac{\mathbb{R}\dfrac{*}{(P \lor \dot{t} = t_0)^{(*)} \vdash \dot{P}^{(*)}}}{t = t_0,\ \langle x' = f(x)\,\&\,P \lor t = t_0\rangle\circ \vdash \dot{P}^{(*)}}
$$

For the "→" direction, we first use (4) to rewrite the progress formula in the antecedents. However, since $t = t_0$, we cut in $P \lor t = t_0$, which allows us to complete the proof with $\text{lp}\mathbb{R}_{\rightarrow}$.

$$
\mathbb{R}\dfrac{\scriptstyle{cut}\dfrac{\scriptstyle{\text{lp}\mathbb{R}_{\rightarrow}}\dfrac{*}{t = t_0,\ P \lor t = t_0,\ (P \lor \dot{t} = t_0)^{(*)} \vdash \langle x' = f(x)\,\&\,P \lor t = t_0\rangle\circ}}{t = t_0,\ (P \lor \dot{t} = t_0)^{(*)} \vdash \langle x' = f(x)\,\&\,P \lor t = t_0\rangle\circ}}{t = t_0,\ \dot{P}^{(*)} \vdash \langle x' = f(x)\,\&\,P \lor t = t_0\rangle\circ}
$$

∎

B.3 Proving Semialgebraic Invariants with Semialgebraic Evolution Domain Constraints

As a consequence of $\text{lp}\mathbb{R}_{\leftarrow}$, we now have the following general version of sAI, which also handles the evolution domain constraints.

Theorem B.6 (Semialgebraic invariants with semialgebraic domains)**.** *For semialgebraic $Q, P, \neg Q, \neg P$, all written in normal form, the following rule (with two stacked premises) is sound and derives from the* dL *calculus extended with RInd&,Cont,Uniq.*

$$
\text{sAI\&}\ \dfrac{\begin{array}{c} t = t_0, P, Q, \dot{Q}^{(*)} \vdash \dot{P}^{(*)} \\ t = t_0, \neg P, Q, \dot{Q}^{(-*)} \vdash \dot{(\neg P)}^{(-*)} \end{array}}{P \vdash [x' = f(x)\,\&\,Q]P}
$$

Proof. This follows directly from rInd&, by rewriting the progress condition in the antecedents of its premises with $\text{lp}\mathbb{R}_{\leftarrow}$, and proving their succedents using $\text{lp}\mathbb{R}_{\rightarrow}$. ∎

B.4 Completeness for Semialgebraic Invariants with Semialgebraic Evolution Domain Constraints

We now prove the completeness theorem for sAI&, from which Theorem 6.7 follows as a special case. This proof uses a mix of a syntactic derivation, and a minor semantic argument. The semantic part of this argument is straightforward. The essential idea is that solutions of the differential equations $x' = f(x)$ are the reversed solutions of $x' = -f(x)$ and vice-versa. This property underlies the "there and back again" axiom for dL which equivalently expresses properties of differential equations with evolution domain constraints in terms of properties of forwards and backwards differential equations without evolution domain constraints [13]. We can also internalize this property with the differential adjoints axiom, as we do in [16]. Consequently, it is possible to prove a form of the completeness theorem purely syntactically, however, we omit the additional formal development for this paper.

Theorem B.7 (Semialgebraic invariant completeness with semialgebraic domains)**.** *Let P, Q be semialgebraic formulas. The* dL *calculus is complete for invariance properties of the form:*

$$
P \vdash [x' = f(x)\,\&\,Q]P
$$

Proof. We may, without loss of generality, assume that P, Q (and $\neg P, \neg Q$) are equivalently rewritten into appropriate normal forms when necessary by an application of rule $\mathbb{R}$. To show that the calculus is complete, we shall prove that the premises of sAI& are necessary, i.e., if there are states that do not satisfy the premises of sAI&, then the conclusion $P \vdash [x' = f(x)\,\&\,Q]P$ is not valid.

Using the characterization of local progress, we first derive the following valid formula (labelled ①):

$$
t = t_0 \land P \land Q \land \dot{Q}^{(*)} \land \neg(\dot{P}^{(*)}) \rightarrow \langle x' = f(x)\,\&\,Q\rangle\neg P
$$

In the first step, we apply Proposition B.3. This is followed by using $\text{lp}\mathbb{R}_{\leftrightarrow}$ on $\neg P$, and $\text{lp}\mathbb{R}_{\rightarrow}$ on Q. Note that we only use $\text{lp}\mathbb{R}_{\rightarrow}$ on Q and not $\text{lp}\mathbb{R}_{\leftrightarrow}$.

$$
\mathbb{R}\dfrac{\scriptstyle{\text{lp}\mathbb{R}_{\leftrightarrow}}\dfrac{\scriptstyle{\text{lp}\mathbb{R}_{\rightarrow}}\dfrac{\scriptstyle{\&\land}\dfrac{\langle x' = f(x)\,\&\,Q \land (\neg P \lor t = t_0)\rangle\circ \vdash \langle x' = f(x)\,\&\,Q\rangle\neg P}{\langle x' = f(x)\,\&\,\neg P \lor t = t_0\rangle\circ,\ \langle x' = f(x)\,\&\,Q\rangle\circ \vdash \langle x' = f(x)\,\&\,Q\rangle\neg P}}{t = t_0,\ Q,\ \dot{Q}^{(*)},\ \langle x' = f(x)\,\&\,\neg P \lor t = t_0\rangle\circ \vdash \langle x' = f(x)\,\&\,Q\rangle\neg P}}{t = t_0,\ Q,\ \dot{Q}^{(*)},\ \dot{(\neg P)}^{(*)} \vdash \langle x' = f(x)\,\&\,Q\rangle\neg P}}{t = t_0,\ P,\ Q,\ \dot{Q}^{(*)},\ \neg(\dot{P}^{(*)}) \vdash \langle x' = f(x)\,\&\,Q\rangle\neg P}
$$

The remainder of the derivation is similar to what we did for algebraic invariants. Since $\overbrace{Q \land (\neg P \lor t = t_0)}^{R} \rightarrow Q$, we use $\langle\cdot\rangle$dRW to strengthen the evolution domain constraint in the succedent. This allows us to use M$\langle\cdot\rangle$, whose right premise closes trivially. Removing the syntactic abbreviation for ∘ allows us to close the premise using dW, because we have $\neg P \lor t = t_0$ in the domain constraint R.

$$
\scriptstyle{\langle\cdot\rangle\text{dRW}}\dfrac{\scriptstyle{M\langle\cdot\rangle}\dfrac{\scriptstyle{dW}\dfrac{\mathbb{R}\dfrac{*}{R \vdash (t \neq t_0 \rightarrow \neg P)}}{\vdash [x' = f(x)\,\&\,R](t \neq t_0 \rightarrow \neg P)}}{\langle x' = f(x)\,\&\,R\rangle\circ \vdash \langle x' = f(x)\,\&\,R\rangle\neg P}}{\langle x' = f(x)\,\&\,R\rangle\circ \vdash \langle x' = f(x)\,\&\,Q\rangle\neg P}
$$

Now, let ω be a state which falsifies the left premise of sAI&, i.e., $\omega \in I[\![t = t_0 \land P \land Q \land \dot{Q}^{(*)}]\!]$, but $\omega \notin I[\![\dot{P}^{(*)}]\!]$. By unfolding the semantics, we have $\omega \in I[\![\neg(\dot{P}^{(*)})]\!]$, and therefore, since ① is valid in all states, we have $\omega \in I[\![\langle x' = f(x)\,\&\,Q\rangle\neg P]\!]$. In other words, ω

falsifies the conclusion of sAI&. Hence, the left premise of sAI& is necessary.

Similarly, let ν be a state which falsifies the right premise of sAI&, i.e., $\nu \in I[\![t = t_0, \neg P, Q, \dot{Q}^{(-*)}]\!]$, but $\nu \notin I[\![(\dot{\neg P})^{(-*)}]\!]$. By a similar argument with ① (appropriately instantiated), we have:

$$\nu \in I[\![\langle x' = -f(x) \,\&\, Q\rangle P]\!]$$

This does not immediately falsify the conclusion of sAI&. Instead, by definition, there is a solution $\varphi : [0,T] \to \mathbb{S}$, of the system $x' = -f(x)$, with $\varphi(0) = \nu$ except on $\{x'\}^\complement$, where $\varphi(T) \in I[\![P]\!]$.

We claim that $\varphi(T)$ falsifies the conclusion of sAI&. Let us consider the time-reversed solution ψ:

$$\psi(\tau)(z) \overset{\text{def}}{=} \begin{cases} \varphi(T-\tau)(z) & z \in \{x'\}^\complement \\ -\varphi(T-\tau)(z) & z \in \{x'\} \end{cases}$$

Notice that $\psi(0)$ agrees with $\varphi(T)$ except on $\{x'\}^\complement$. Moreover, it solves the system $x' = f(x)$ and stays in evolution domain Q for its entire duration. Finally, $\psi(T)$ agrees with ν, except on $\{x'\}^\complement$, which, by coincidence for formulas [15, Lemma 11], implies that $\psi(T) \in I[\![\neg P]\!]$ (recall, that P only depends on x). Therefore, ψ is a witness for $\varphi(T) \in I[\![\langle x' = f(x) \,\&\, Q\rangle \neg P]\!]$. Hence, $\varphi(T)$ falsifies the conclusion of sAI&, and so the right premise is also necessary. ◻

C Completed Proofs

We give full proofs for all remaining lemmas and theorems that have not already been proved in previous appendices where we developed the axiomatization (Appendix A) or derived the complete proof rule for semialgebraic invariants (Appendix B).

C.1 Darboux Inequalities

We derive the dbx$\gtrsim$ rule. Its proof is similar to the one for dbx.

Proof of Lemma 3.3. Let ① denote the use of the premise of dbx$\gtrsim$, and ② abbreviate the right premise in the following derivation.

$$\dfrac{\dfrac{\dfrac{p \gtrsim 0,\, y>0 \vdash [x' = f(x),\, y' = -gy \,\&\, Q \wedge y>0] py \gtrsim 0 \quad ②}{p \gtrsim 0,\, y>0 \vdash [x' = f(x),\, y' = -gy \,\&\, Q](y>0 \wedge py \gtrsim 0)}\,\text{dC}}{p \gtrsim 0 \vdash \exists y\, [x' = f(x),\, y' = -gy \,\&\, Q] p \gtrsim 0}\,\text{M[}\cdot\text{]},\exists\text{R}}{p \gtrsim 0 \vdash [x' = f(x) \,\&\, Q] p \gtrsim 0}\,\text{dG}$$

Note the minor variation in the proof: the last step above uses dC instead of $[\cdot]\wedge$, which introduces $y > 0$ into the evolution domain constraint in the left premise. This sign condition on y is crucially used when we apply ① in the proof for the left premise:

$$\dfrac{\dfrac{\dfrac{*}{p \gtrsim 0,\, y>0 \vdash py \gtrsim 0}\,\mathbb{R} \qquad \dfrac{① \quad \dfrac{*}{\dot{p} \geq gp,\, y>0 \vdash \dot{p}y - gyp \geq 0}\,\mathbb{R}}{Q,\, y>0 \vdash \dot{p}y - gyp \geq 0}\,\text{cut}}{}}{p \gtrsim 0,\, y>0 \vdash [x' = f(x),\, y' = -gy \,\&\, Q \wedge y>0] py \gtrsim 0}\,\text{dI}$$

The choice of the differential ghost $y' = -gy$ is obtained by solving the top condition for y'. The right premise ② is:

$$y > 0 \vdash [x' = f(x), y' = -gy \,\&\, Q] y > 0$$

Its proof continues using a second ghost $z' = \frac{g}{2}z$. This allows us to prove $yz^2 = 1$ invariant, which implies $y > 0$ in the postcondition:

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{Q \vdash -(gy)z^2 + y(2z(\frac{g}{2}z)) = 0}\,\mathbb{R}}{yz^2 = 1 \vdash [x' = f(x),\, y' = -gy,\, z' = \frac{g}{2}z \,\&\, Q] yz^2 = 1}\,\text{dI}}{y > 0 \vdash \exists z\, [x' = f(x),\, y' = -gy,\, z' = \frac{g}{2}z \,\&\, Q] y > 0}\,\text{M[}\cdot\text{]},\exists\text{R}}{y > 0 \vdash [x' = f(x),\, y' = -gy \,\&\, Q] y > 0}\,\text{dG}$$

◻

C.2 Differential Radical Invariants

We derive the dRI proof rule.

Proof of Theorem 4.2. Let p be a polynomial satisfying both premises of the dRI proof rule, and let

$$\mathbf{p} \overset{\text{def}}{=} \begin{pmatrix} p \\ \dot{p}^{(1)} \\ \vdots \\ \dot{p}^{(N-1)} \end{pmatrix}$$

We have $\mathbf{p}_i \overset{\text{def}}{=} \dot{p}^{(i-1)}$ for $i = 1, 2, \ldots, N$. If we take the component-wise Lie derivative of $\mathbf{p}$, we have: $(\dot{\mathbf{p}})_i = \mathcal{L}_{f(x)}(\mathbf{p}_i) = \dot{p}^{(i)}$.

We start by setting up for a proof by vdbx. On the left premise after the cut, we used the arithmetic equivalence $\bigwedge_{i=0}^{N-1} \dot{p}^{(i)} = 0 \leftrightarrow \mathbf{p} = 0$, to rewrite the succedent to the left premise of dRI.

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

We continue on the right premise by applying vdbx with the following special choice of G, with 1 on its superdiagonal, and the g_i cofactors in the last row:

$$\dfrac{Q \vdash \dot{\mathbf{p}} = \overbrace{\begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \ldots & 0 & 1 \\ g_0 & g_1 & \ldots & g_{N-2} & g_{N-1} \end{pmatrix}}^{G} \mathbf{p}}{\mathbf{p} = 0 \vdash [x' = f(x) \,\&\, Q]\mathbf{p} = 0}\,\text{vdbx}$$

The succedent of the open premise requires us to prove a component-wise equality on two vectors, i.e., $(\dot{\mathbf{p}})_i = (G\mathbf{p})_i$ for $1 \leq i \leq N$. For $1 \leq i < N$, explicit matrix multiplication yields:

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

Therefore, all but the final component-wise equality prove trivially by $\mathbb{R}$. The remaining premise is:

$$Q \vdash (\dot{\mathbf{p}})_N = (G\mathbf{p})_N$$

The LHS of this equality simplifies to:

$$(\dot{\mathbf{p}})_N = \dot{p}^{(N)}$$

The RHS simplifies to:

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

Therefore, by an arithmetic step, we equivalently reduce the remaining open premise to the right premise of dRI. ◻

C.3 Semialgebraic Case

We prove local progress for the general case where P is a semialgebraic formula in normal form (2).

Proof of Lemma 6.5. Throughout this proof, we will collapse similar premises in derivations and index them by i, j. We first decompose the outermost conjunction in P with $\wedge$L for the antecedents, and

&∧ for the evolution domain constraint. We write P_i for the i-th conjunct of P.

$$\frac{\Gamma, P, P_i \vdash \langle x' = f(x) \,\&\, P_i \rangle \circ}{\Gamma, P \vdash \langle x' = f(x) \,\&\, P \rangle \circ}\ {\scriptstyle \&\wedge,\wedge\text{L}}$$

Each P_i is a disjunctive formula: $\bigvee_{j=0}^{m(i)} p_{ij} = 0 \vee \bigvee_{j=0}^{n(i)} q_{ij} > 0$. It will be sufficient for us to show local progress for just one of these disjuncts, and then use $\langle\cdot\rangle$dRW to conclude local progress for P_i.

We continue by case splitting on P_i in the antecedent with ∨L. For the case with $\bigvee_{j=0}^{n(i)} q_{ij} > 0$, we close using cont^o. This leaves the $\bigvee_{j=0}^{m(i)} p_{ij} = 0$ cases abbreviated by ①.

$$\frac{① \qquad \dfrac{*}{\bigvee_{j=0}^{n(i)} q_{ij} > 0 \vdash \langle x' = f(x) \,\&\, P_i \rangle \circ}\ {\scriptstyle \text{cont}^o,\langle\cdot\rangle\text{dRW}}}{\Gamma, P, P_i \vdash \langle x' = f(x) \,\&\, P_i \rangle \circ}\ {\scriptstyle \vee\text{L}}$$

We continue on ① by cutting in the corresponding i-th conjunct of the premise of lpℝ, and then case splitting on the cut premise. In the $\dot{p_{ij}}^{(*)} = 0$ cases, we use $\langle\cdot\rangle$dRI. The cases for $\dot{q_{ij}}^{(*)} > 0$ are abbreviated with ②:

$$\frac{\dfrac{\dfrac{*}{\dot{p_{ij}}^{(*)} = 0 \vdash \langle x' = f(x) \,\&\, P_i \rangle \circ}\ {\scriptstyle \langle\cdot\rangle\text{dRI},\langle\cdot\rangle\text{dRW}} \qquad ②}{\bigvee_{j=0}^{m(i)} p_{ij} = 0, \bigvee_{j=0}^{m(i)} \dot{p_{ij}}^{(*)} = 0 \vee \bigvee_{j=0}^{n(i)} \dot{q_{ij}}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, P_i \rangle \circ}\ {\scriptstyle \vee\text{L}}}{\Gamma, P, \bigvee_{j=0}^{m(i)} p_{ij} = 0 \vdash \langle x' = f(x) \,\&\, P_i \rangle \circ}\ {\scriptstyle \text{cut}}$$

Finally, for ②, we rewrite the antecedents and domain constraint with $\bigvee_{j=0}^{m(i)} p_{ij} = 0 \leftrightarrow \prod_{j=0}^{m(i)} p_{ij} = 0$ which is a valid real arithmetic equivalence. We then complete the proof with lp$_{=\vee>}$.

$$\frac{\dfrac{\dfrac{*}{\prod_{j=0}^{m(i)} p_{ij} = 0, \dot{q_{ij}}^{(*)} > 0 \vdash \left\langle x' = f(x) \,\&\, \prod_{j=0}^{m(i)} p_{ij} = 0 \vee q_{ij} > 0 \right\rangle \circ}\ {\scriptstyle \text{lp}_{=\vee>}}}{\prod_{j=0}^{m(i)} p_{ij} = 0, \dot{q_{ij}}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, P_i \rangle \circ}\ {\scriptstyle \langle\cdot\rangle\text{dRW},\mathbb{R}}}{\bigvee_{j=0}^{m(i)} p_{ij} = 0, \dot{q_{ij}}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, P_i \rangle \circ}\ {\scriptstyle \text{cut},\mathbb{R}}$$

□