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 then 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 results are purely axiomatic, and so the axiomatization is suitable for sound implementation in foundational theorem provers.

CCS Concepts • **Mathematics of computing → Ordinary differential equations**; • **Theory of computation → Proof theory**; **Modal and temporal logics**; **Program reasoning**;

Keywords differential equation axiomatization, differential dynamic logic, differential ghosts

ACM Reference Format:
André Platzer and Yong Kiam Tan. 2018. Differential Equation Axiomatization: The Impressive Power of Differential Ghosts. In *LICS '18: LICS '18: 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, July 9–12, 2018, Oxford, United Kingdom.* ACM, New York, NY, USA, 25 pages. https://doi.org/10.1145/3209108.3209147

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) [12, 14]. dL is a logic for deductive verification of hybrid systems that are modeled by hybrid programs combining discrete computation (e.g., assignments, tests and loops), and continuous dynamics specified using systems of ordinary differential equations (ODEs). By the continuous relative completeness theorem for dL [12, 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 following the ODEs. The three basic dL axioms for reasoning about such invariants are: (1) *differential invariants*, which prove simple invariants by locally analyzing their 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 by analyzing the loop body, (2) corresponds to progressive refinement of the loop guards, and (3) corresponds to adding discrete ghost variables to remember intermediate program states. At first glance, differential ghosts seem counter-intuitive: they increase the dimension of the system, 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 [13].

This paper has the following contributions:

LICS '18, July 9–12, 2018, Oxford, United Kingdom

ACM ISBN 978-1-4503-5583-4/18/07.
https://doi.org/10.1145/3209108.3209147

[1] In fact, this analogy can be made precise: dL also has a converse relative completeness theorem [12, Theorem 2] that reduces ODEs to discrete Euler approximation loops.

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 axioms outlined above.
2. We introduce 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 dL calculus *decides* all real arithmetic invariants of differential equations.
4. Our completeness results are axiomatic, enabling disproofs.

Just as discrete ghosts can make a program logic relatively complete [11], our first completeness result shows that differential ghosts achieve completeness for algebraic invariants in dL. We extend the 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 [6, 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 identify the underlying aspects of differential equations that are needed for sound invariance reasoning. Our axiomatization is *not limited* to proving invariance properties, but also completely axiomatizes disproofs and other qualitative properties such as local progress.

The parsimony of our axiomatization makes it amenable to sound implementation and verification in foundational theorem provers [2, 5] using dL's uniform substitution calculus [14], and is in stark contrast to previous highly schematic procedures [6, 9].

All proofs are in the appendices A and B.

2 Background: Differential Dynamic Logic

This section briefly reviews the relevant continuous fragment of dL, and establishes the notational conventions used in this paper. The reader is referred to the literature [12, 14] 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:

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

Formulas can be normalized such that $e_1 \sim e_2$ has 0 on the right-hand side. We write $p \succcurlyeq 0$ if there is a free choice between $\geq$ or $>$. Further, $p \preccurlyeq 0$ is $-p \succcurlyeq 0$, where $\preccurlyeq$ stands for $\leq$ or $<$, and $\succcurlyeq$ is correspondingly chosen. Other logical connectives, e.g., $\rightarrow, \leftrightarrow$ are definable. For the formula $\mathbf{p} = \mathbf{q}$ where both $\mathbf{p}, \mathbf{q}$ have dimension n, equality is understood *component-wise* as $\bigwedge_{i=1}^{n} \mathbf{p}_i = \mathbf{q}_i$ and $\mathbf{p} \neq \mathbf{q}$ as $\neg(\mathbf{p} = \mathbf{q})$. 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.

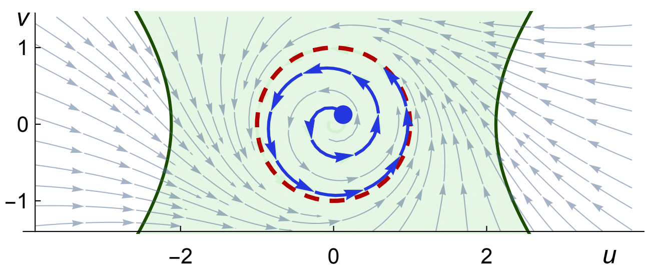

Figure 1. The red dashed circle $u^2 + v^2 = 1$ is approached by solutions of α_e from all points except the origin, e.g., the blue trajectory from $(\frac{1}{8}, \frac{1}{8})$ spirals towards the circle. The circle, green region $u^2 \leq v^2 + \frac{9}{2}$, and the origin are invariants of the system.

Hybrid programs α allow us to express both discrete and continuous dynamics. This paper focuses on the continuous fragment[2]:

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

We write $x' = f(x) \,\&\, Q$ for an autonomous vectorial differential equation 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. We write $x' = f(x)$ for $x' = f(x) \,\&\, \mathit{true}$. We use a running example (Fig. 1):

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

Following our analogy in Section 1, solutions of $x' = f(x)$ must continuously (locally) follow its RHS, $f(x)$. Figure 1 visualizes this 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. Figure 1 suggests, e.g., that all points (except the origin) globally evolve towards the unit circle.

2.2 Semantics

A state $\omega : \mathbb{V} \rightarrow \mathbb{R}$ assigns a real value to each variable in $\mathbb{V}$. We may let $\mathbb{V} = \{x_1, \ldots, x_n\}$ since we only need to consider the variables that occur[3]. 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.

The value of term e in state ω is written $\omega[\![e]\!]$ and defined as usual. The semantics of comparison operations and logical connectives 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 $\omega \in [\![\phi_1 \wedge \phi_2]\!]$ 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. The semantics of an ODE is the set of all pairs of states that can be connected by a solution of the ODE:

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

[2]We only consider weak-test dL, where Q is a first-order formula of real arithmetic.
[3]Variables v that do not have an ODE $v' = \ldots$ also do not change (similar to $v' = 0$).

The $\varphi \models x' = f(x) \,\&\, Q$ condition checks that φ is a solution of $x' = f(x)$, and that $\varphi(\zeta) \in [\![Q]\!]$ for all $\zeta \in [0, T]$. For any solution φ, the truncation $\varphi|_\zeta : [0, \zeta] \to \mathbb{R}^n$ defined as $\varphi|_\zeta(\tau) = \varphi(\tau)$ is also a solution. Thus, $(\omega, \varphi(\zeta)) \in [\![x' = f(x) \,\&\, Q]\!]$ for all $\zeta \in [0, T]$.

Finally, $\omega \in [\![[\alpha]\phi]\!]$ iff $\nu \in [\![\phi]\!]$ for all ν such that $(\omega, \nu) \in [\![\alpha]\!]$. Also, $\omega \in [\![\langle\alpha\rangle\phi]\!]$ iff there is a ν such that $(\omega, \nu) \in [\![\alpha]\!]$ and $\nu \in [\![\phi]\!]$. A formula ϕ is *valid* iff it is true in all states, i.e., $\omega \in [\![\phi]\!]$ for all ω.

If formula $P \to [x' = f(x) \,\&\, Q]P$ is valid, then P is called an *invariant* of $x' = f(x) \,\&\, Q$. By the semantics, that is, from any initial state $\omega \in [\![P]\!]$, any solution φ starting in ω, which does not leave the evolution domain $[\![Q]\!]$, stays in $[\![P]\!]$ for its *entire duration*.

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

2.3 Differentials and Lie Derivatives

The study of invariants relates to the study of time derivatives of the quantities that the invariants involve. Directly using time derivatives leads to numerous subtle sources of unsoundness, because they are not well-defined in arbitrary contexts (e.g., in isolated states). dL, instead, provides differential terms $(e)'$ that have a local semantics in every state, can be used in any context, and can soundly be used for arbitrary logical manipulations [14]. Along an ODE $x' = f(x)$, the value of the differential term $(e)'$ coincides with the time derivative $\frac{d}{dt}$ of the value of e [14, Lem. 35].

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

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

Unlike time derivatives, Lie derivatives can be written down syntactically. Unlike differentials, they still depend on the ODE context in which they are used. Along an ODE $x' = f(x)$, however, the value of Lie derivative $\mathcal{L}_{f(x)}(p)$ coincides with that of the differential $(p)'$, and dL allows transformation between the two by proof. For this paper, we shall therefore directly use Lie derivatives, relying under the hood on dL's axiomatic proof transformation from differentials [14]. The operator $\mathcal{L}_{f(x)}(\cdot)$ inherits the familiar sum and product rules of differentiation from corresponding axioms of differentials.

We reserve the notation $\mathcal{L}_{f(x)}(\cdot)$ when used as an operator and simply write $\dot{p}$ for $\mathcal{L}_{f(x)}(p)$, because $x' = f(x)$ will be clear from the context. 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. Since polynomials are closed under Lie derivation w.r.t. polynomial ODEs, all 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 [14, 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,$\wedge$R, and cut. The semantics of sequent $\Gamma \vdash \phi$ is equivalent to $(\bigwedge_{A \in \Gamma} A) \to \phi$. When we use an implicational or equivalence axiom, we omit the usual sequent manipulation steps and instead directly label the proof step with the axiom, giving the resulting premises accordingly [14]. Because first-order real arithmetic is decidable [1], we assume access to such a decision procedure, and label steps with $\mathbb{R}$ whenever they follow as a consequence of first-order real arithmetic. We use the $\exists$R rule over the reals, which allows us to supply a real-valued witness to an existentially quantified succedent. We mark with $*$ the completed branches of sequent proofs. A proof rule is *sound* iff the validity of all its premises (above the rule bar) imply the validity of its conclusion (below rule bar).

Theorem 2.1 (Differential equation axiomatization [14])**.** *The following sound proof rules derive from the axioms of* dL*:*

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

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

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

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

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

Differential invariants (dI) reduce questions about invariance of $p = 0, p \succcurlyeq 0$ (globally along solutions of the ODE) to local questions about their respective Lie derivatives. We only show the two instances ($\text{dI}_=$,$\text{dI}_\succcurlyeq$) of the more general dI rule [14] that will be used here. They internalize the mean value theorem[4] (see Appendix A.2). These *derived rules* are schematic because $\dot{p}$ in their premises are dependent on the ODEs $x' = f(x)$. This exemplifies our point in Section 2.3: differentials allow the principles underlying $\text{dI}_=$,$\text{dI}_\succcurlyeq$ to be stated as axioms [14] rather than complex, schematic proof rules.

Differential cut (dC) expresses that if we can separately prove that the system 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 drop the ODEs, and prove the postcondition P directly from the evolution domain constraint Q. Similarly, 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[·] monotonicity rule allows us to strengthen the postcondition to ϕ_2 if it implies ϕ_1. The derived axiom $[\cdot]\wedge$ allows us to prove conjunctive postconditions separately, e.g., $\text{dI}_=$ derives from $\text{dI}_\succcurlyeq$ using $[\cdot]\wedge$ with the equivalence $p = 0 \leftrightarrow p \geq 0 \wedge -p \geq 0$.

Even if dC increases the deductive power over dI, the deductive power increases even further [13] with the *differential ghosts* rule (dG). It allows us to add a *fresh* variable y to the system of equations.

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

The main soundness restriction of dG is that the new ODE must be linear[5] 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 the new vector of variables $\mathbf{y}$. In this setting, $a(x)$ (resp. $b(x)$) is a matrix (resp. vector) of polynomials in x.

Adding differential ghost variables by dG for the sake of the proof 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 dL 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 [4]. A polynomial p is a *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

As in algebra, $\mathbb{R}[x]$ is the ring of polynomials in indeterminates x.

Definition 3.1 (Ideal [1])**.** The *ideal* generated by the polynomials $p_1, \ldots, p_s \in \mathbb{R}[x]$ is defined as the set of polynomials:

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

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

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

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

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

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 above intuition motivates the following proof rule for invariance of $p = 0$:

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

Although we can derive dbx directly, we opt for a detour through a proof rule for Darboux *in*equalities instead. The resulting proof rule for invariant inequalities is crucially used in later sections.

3.2 Darboux Inequalities

Assume that p satisfies a Darboux *inequality* $\dot{p} \geq gp$ for some cofactor polynomial g. Semantically, in an initial state ω where $\omega[\![p]\!] \geq 0$, an application of Grönwall's lemma [8, 18, §29.VI] allows us to conclude that $p \geq 0$ stays invariant along solutions starting at ω. Indeed, if p is a Darboux polynomial with cofactor g, then it satisfies both Darboux inequalities $\dot{p} \geq gp$ and $\dot{p} \leq gp$, which yields an alternative semantic argument for the invariance of $p = 0$.

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

[6]This requires the solution to be an analytic function of time, which is the case here.

In our derivations below, we show that these Darboux invariance properties can be proved purely syntactically using dG.

Lemma 3.2 (Darboux (in)equalities are differential ghosts)**.** *The proof rules for Darboux equalities (dbx) and inequalities (dbx$\succcurlyeq$) derive from dG (and dI,dC):*

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

Proof. We first derive dbx$\succcurlyeq$, let ① denote the use of its premise, and ② abbreviate the right premise in the following derivation.

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

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 $y > 0$. We then observe that in order to prove $p \succcurlyeq 0$, it suffices to prove the stronger invariant $y > 0 \land py \succcurlyeq 0$, so we use the monotonicity rule M[·] to strengthen the postcondition. Next, we use dC to first prove $y > 0$ in ②, and assume it in 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:

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

We use dI to prove the inequational invariant $py \succcurlyeq 0$; 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:

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

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

We continue on premise ② with a second ghost $z' = \frac{g}{2}z$:

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

This derivation is analogous to the one for the previous premise. In the M[·],∃R step, we observe that if $y > 0$ initially, then there exists z such that $yz^2 = 1$. Moreover, $yz^2 = 1$ is sufficient to imply $y > 0$ in the postcondition. The differential ghost $z' = \frac{g}{2}z$ is constructed so that $yz^2 = 1$ can be proved invariant *along the differential equation.*

The dbx proof rule derives from rule dbx$\succcurlyeq$ using the equivalence $p = 0 \leftrightarrow p \geq 0 \land -p \geq 0$ and derived axiom $[\cdot]\land$:

$$\text{M}[\cdot],\mathbb{R}\ \dfrac{[\cdot]\land,\land\text{R}\ \dfrac{\text{dbx}_{\succcurlyeq}\ \dfrac{\mathbb{R}\ \dfrac{Q \vdash \dot{p} = gp}{Q \vdash \dot{p} \geq gp}}{p \geq 0 \vdash [x' = f(x)\,\&\,Q]p \geq 0} \qquad \text{dbx}_{\succcurlyeq}\ \dfrac{\mathbb{R}\ \dfrac{Q \vdash \dot{p} = gp}{Q \vdash \dot{(-p)} \geq -gp}}{-p \geq 0 \vdash [x' = f(x)\,\&\,Q]{-p} \geq 0}}{p \geq 0 \land -p \geq 0 \vdash [x' = f(x)\,\&\,Q](p \geq 0 \land -p \geq 0)}}{p = 0 \vdash [x' = f(x)\,\&\,Q]p = 0}$$

□

Example 3.3 (Proving continuous properties in dL)**.** In the running example, dbx$\succcurlyeq$ directly proves that the open disk $1 - u^2 - v^2 > 0$

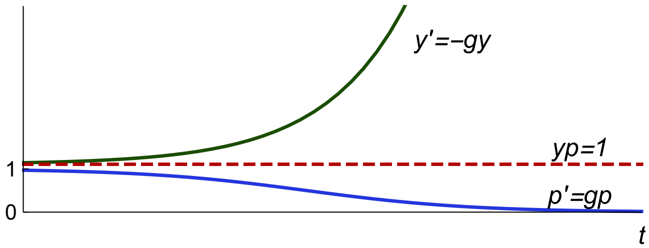

Figure 2. The differential ghost $y' = -gy$ (in green) balances out $p' = gp$ (in blue) so that the value of yp (the red dashed line) remains constant at 1. The horizontal axis tracks the evolution of time t.

is an invariant for α_e using cofactor $g = -\frac{1}{2}(u^2 + v^2)$:

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

Figure 1 indicated that trajectories in the open disk spiral towards $1-u^2-v^2 = 0$, i.e., they evolve towards leaving the invariant region. Intuitively, this makes a direct proof of invariance difficult. The proof of dbx$\succcurlyeq$ instead introduces the differential ghost $y' = -gy$. Its effect for our example is illustrated in Fig. 2, which plots the value of $p = 1 - u^2 - v^2$ and ghost y along the solution starting from the point $(\frac{1}{8}, \frac{1}{8})$. Although p decays towards 0, the ghost y balances this by growing away from 0 so that yp remains constant at its initial value 1, which implies that p never reaches 0.

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 [13]. It is a simple consequence of dbx$\succcurlyeq$, since the polynomial y satisfies the Darboux equality $\dot{y} = -y$ with cofactor -1. For brevity, we showed the same derivation for both $\geq$ and $>$ cases of dbx$\succcurlyeq$ even though the latter case only needs one ghost. Similarly, dbx derives directly using two ghosts rather than the four ghosts incurred using $[\cdot]\wedge$. All of these cases, however, only introduce one differential ghost at a time. In the next section, we exploit the full power of *vectorial* dG.

4 Algebraic Invariants

We now consider polynomials that are not Darboux for the given differential equations, but instead satisfy a *differential radical property* [6] with respect to its higher Lie derivatives. Let g_i be cofactor polynomials, $N \geq 1$, assume that p satisfies the polynomial identity:

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

With the same intuition, again take Lie derivatives on both sides:

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

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 higher Lie derivatives*) must stay invariant along (analytic) 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 $\mathbf{p}$. If all components of $\mathbf{p}$ start at 0, then they stay 0 along $x' = f(x)$.

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

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

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 $\mathbf{y}' = -G^T\mathbf{y}$ such that the vanishing of the scalar product, i.e., $\mathbf{p} \cdot \mathbf{y} = 0$, is invariant. In the derivation below, we suppress the initial choice of values for $\mathbf{y}$ till later. 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:

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

So far, the proof is similar to the first ghost step for dbx$\succcurlyeq$. 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 independent 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 $\mathbf{p} = 0$. The matrix Y is obtained by repeating the derivation above on premise ②, using dG to add n copies of the ghost vectors, $\mathbf{y}_1, \ldots, \mathbf{y}_n$, each satisfying the ODE system $\mathbf{y}_i' = -G^T\mathbf{y}_i$. By the derivation above, each $\mathbf{y}_i$ satisfies the provable invariant $\mathbf{y}_i \cdot \mathbf{p} = 0$, or more concisely:

$$\overbrace{\begin{pmatrix} y_{11} & y_{12} & \cdots & y_{1n} \\ y_{21} & y_{22} & \cdots & y_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ y_{n1} & y_{n2} & \cdots & y_{nn} \end{pmatrix}}^{Y} \overbrace{\begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix}}^{\mathbf{p}} = 0$$

[7] For a square matrix of polynomials Y, $\det(Y)$ is its determinant, $\mathrm{tr}(Y)$ its trace, and, of course, Y^T is its transpose.

Streamlining the proof, we first perform the dG steps that add the n ghost vectors $\mathbf{y}_i$, before combining $[\cdot]\wedge$,dI to prove:

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

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 prove 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 by dG, 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.

In order to show that $\det(Y) > 0$ is an invariant, we use rule dbx$\succcurlyeq$ with the critical polynomial identity $\dot{\det(Y)} = -\operatorname{tr}(G)\det(Y)$ that follows from Liouville's formula [18, §15.III], where the Lie derivatives are taken with respect to the extended system of equations $x' = f(x), Y' = -YG$. For completeness, we give an arithmetic proof of Liouville's formula in Appendix B.3. Thus, $\det(Y)$ is a Darboux polynomial over the variables y_{ij}, with polynomial cofactor $-\operatorname{tr}(G)$:

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

Combining ③ and ④ completes the derivation for the invariance of $\mathbf{p} = 0$. We start with the dG step and abbreviate the ghost matrix.

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

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

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

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

Since $\det(Y) \neq 0$ is invariant, the $n \times n$ ghost matrix Y in this proof corresponds to a basis 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, a variation of step ③ in the proof shows 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 continuously evolving change of basis Y^{-1}. This generalizes the intuition illustrated in Fig. 2 to the n-dimensional case. Crucially, differential ghosts let us soundly express this time-varying change of basis purely axiomatically.

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

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 (Appendix B.3). Rule dRI derives from rule vdbx with:

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

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, but, over $\mathbb{R}$, can be normalized to a single equation $p = 0$ 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 polynomial ODE $x' = f(x)$, there is a smallest natural number[9] $N{\geq}1$ called *rank* [6, 10] such that p satisfies the polynomial identity (1) for some cofactors g_i. This N is computable by successive ideal membership checks [6].

Thus, some suitable rank at which the right premise of dRI proves exists for any polynomial p.[10] The succedent in the remaining left premise of dRI entails that *all* Lie derivatives evaluate to zero.

Definition 4.3 (Differential radical formula)**.** The *differential radical formula* $\dot{p}^{(*)} = 0$ of a polynomial p with rank $N{\geq}1$ from (1) and Lie derivatives with respect to $x' = f(x)$ is defined to be:

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

The completeness of dRI can be proved semantically [6]. However, using the extensions developed in Section 5, we derive the following characterization for algebraic invariants axiomatically.

Theorem 4.4 (Algebraic invariant completeness)**.** *The following is a derived axiom in* dL *when Q characterizes an open set:*

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

Proof Summary (Appendix B.3). The "←" direction follows by an application of dRI (whose right premise closes by (1) for any Q). The "→" direction relies on existence and uniqueness of solutions to

[9] The only polynomial satisfying (1) for $N = 0$ is the 0 polynomial, which gives correct but trivial invariants $0 = 0$ for any system (and 0 can be considered to be of rank 1).

[10] Theorem 4.2 shows Q can be assumed when proving ideal membership of $\dot{p}^{(N)}$. A finite rank exists either way, but assuming Q may reduce the number of higher Lie derivatives of p that need to be considered.

differential equations, which are internalized as axioms in Section 5. □

For the proof of Theorem 4.4, we emphasize that additional axioms are *only required* for syntactically deriving the "$\rightarrow$" 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.

Corollary 4.5 (Decidability)**.** *For algebraic formulas P and hybrid programs α whose tests and domain constraints are negations of algebraic formulas (see Appendix B.3), it is possible to compute a polynomial q such that the equivalence $[\alpha]P \leftrightarrow q = 0$ is derivable in* dL.

Proof Summary (Appendix B.3). By structural induction on α analogous to [12, Thm. 1], using Theorem 4.4 for the differential equations case. □

5 Extended Axiomatization

In this section, we present the axiomatic extension that is used for the rest of this paper. The extension requires that the system $x' = f(x)$ locally evolves x, i.e., it has no fixpoint at which $f(x)$ is the 0 vector. This can be ensured syntactically, e.g., by requiring that the system contains a clock variable $x_1' = 1$ that tracks the passage of time, which can always first be added using dG if necessary.

5.1 Existence, Uniqueness, and Continuity

The differential equations considered in this paper have polynomial right-hand sides. Hence, the Picard-Lindelöf theorem [18, §10.VI] guarantees that for any initial state $\omega \in \mathbb{R}^n$, a *unique* solution of the system $x' = f(x)$, i.e., $\varphi : [0, T] \rightarrow \mathbb{R}^n$ with $\varphi(0) = \omega$, *exists* for some duration $T > 0$. The solution φ can be extended (uniquely) to its maximal open interval of existence [18, §10.IX] and $\varphi(\zeta)$ is differentiable, and hence continuous with respect to ζ.

Lemma 5.1 (Continuous existence, uniqueness, and differential adjoints)**.** *The following axioms are sound. In Cont and Dadj, y are fresh variables (not in $x' = f(x) \,\&\, Q(x)$ or p).*

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

$$\text{Cont}\quad x = y \rightarrow (p > 0 \rightarrow \langle x' = f(x) \,\&\, p > 0\rangle x \neq y)$$

$$\text{Dadj}\quad \langle x' = f(x) \,\&\, Q(x)\rangle\, x = y \leftrightarrow \langle y' = -f(y) \,\&\, Q(y)\rangle\, y = x$$

Proof Summary (Appendix A.3). Uniq internalizes uniqueness, Cont internalizes continuity of the values of p and existence of solutions, and Dadj internalizes the group action of time on ODE solutions, which is another consequence of existence and uniqueness. □

The *uniqueness axiom* Uniq can be intuitively read as follows. If we have 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 both evolution domains so $Q_1 \land Q_2$ and satisfies $P_1 \lor P_2$ at its endpoint.

Continuity axiom Cont expresses a notion of *local progress* for differential equations. It says that from an initial state satisfying $x = y$, the system can locally evolve to another state satisfying $x \neq y$ while staying in the *open set* of states characterized by $p > 0$. This uses the assumption that the system locally evolves x at all.

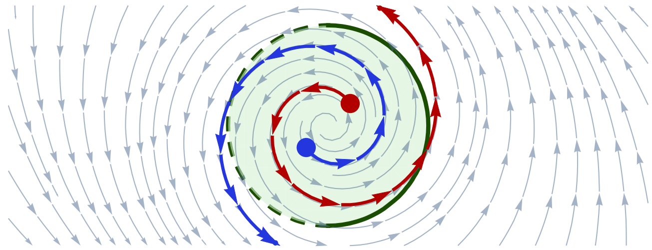

Figure 3. The half-open disk $u^2+v^2 < \frac{1}{4} \lor u^2+v^2 = \frac{1}{4} \land u \geq 0$ is not invariant for α_e because the red and blue trajectories spiral out of it towards the unit circle at a closed or open boundary, respectively.

The *differential adjoints* axiom Dadj expresses that x can flow forward to y iff y can flow backward to x along an ODE. It is at the heart of the "there and back again" axiom that equivalently expresses properties of differential equations with evolution domain constraints in terms of properties of forwards and backwards differential equations without evolution domain constraints [12].

To make use of these axioms, it will be useful to derive rules and axioms that allow us to work directly in the diamond modality, rather than the box modality.

Corollary 5.2 (Derived diamond modality rules and axioms)**.** *The following derived axiom and derived rule are provable in* dL*:*

$$\text{DR}\langle\cdot\rangle\quad \begin{aligned}&[x' = f(x) \,\&\, R]Q\\ &\rightarrow (\langle x' = f(x) \,\&\, R\rangle P \rightarrow \langle x' = f(x) \,\&\, Q\rangle P)\end{aligned}$$

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

Proof Summary (Appendix A.4). Axiom DR$\langle\cdot\rangle$ is the diamond version of the dL refinement axiom that underlies dC; if we never leave Q when staying in R (first assumption), then any solution staying in R (second assumption) must also stay in Q (conclusion). The rule dRW$\langle\cdot\rangle$ derives from DR$\langle\cdot\rangle$ using dW on its first assumption. □

5.2 Real Induction

Our final axiom is based on the real induction principle [3]. It internalizes the topological properties of solutions. For space reasons, we only present the axiom for systems without evolution domain constraints, leaving the general version to Appendix A.3.

Lemma 5.3 (Real induction)**.** *The real induction axiom is sound, where y is fresh in $[x' = f(x)]P$.*

$$\text{RI}\quad \begin{aligned}&[x' = f(x)]P \leftrightarrow\\ &\forall y\, [x' = f(x) \,\&\, P \lor x = y](x = y \rightarrow P \land \langle x' = f(x) \,\&\, P\rangle x \neq y)\end{aligned}$$

Proof Summary (Appendix A.3). The RI axiom follows from the real induction principle [3] and the Picard-Lindelöf theorem [18, §10.VI]. □

To see the topological significance of RI, recall the running example and consider a set of points that is *not invariant.* Figure 3 illustrates two trajectories that leave the candidate invariant disk S. These trajectories must stay in S before leaving it through its boundary, and only in one of two ways: either at a point which is also in S (red trajectory exiting right) or is not (the blue trajectory).

Real induction axiom RI can be understood as $\forall y\,[\dots]\big(x = y \rightarrow \dots\big)$ quantifying over all final states ($x = y$) reachable by trajectories still within P except possibly at the endpoint $x = y$. The left conjunct under the modality expresses that P is still true at such an endpoint, while the right conjunct expresses that the ODE still remains in P locally. The left conjunct rules out trajectories like the blue one exiting left in Fig. 3, while the right conjunct rules out trajectories like the red trajectory exiting right.

The right conjunct suggests a way to use RI: it reduces invariants to local progress properties under the box modality. This motivates the following syntactic modality abbreviations for *progress within a domain* Q (with the initial point) or *progress into* Q (without):

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

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

All remaining proofs in this paper only use these two modalities with an initial assumption $x = y$. In this case, where $\omega[\![x]\!] = \omega[\![y]\!]$, the $\bigcirc$ modality has the following semantics:

$\omega \in [\![\langle x' = f(x) \,\&\, Q\rangle\bigcirc]\!]$ iff there is a function $\varphi : [0, T] \rightarrow \mathbb{R}^n$ with $T > 0$, $\varphi(0) = \omega$, φ is a solution of the system $x' = f(x)$, and $\varphi(\zeta) \in [\![Q]\!]$ for all ζ in the half-open interval $(0, T]$

For $\langle x' = f(x) \,\&\, Q\rangle\circ$ it is the closed interval $[0, T]$ instead of $(0, T]$. Both $\bigcirc$ and $\circ$ resemble continuous-time versions of the next modality of temporal logic with the only difference being whether the initial state already needs to start in Q. Both coincide if $\omega \in [\![Q]\!]$.

The motivation for separating these modalities is topological: $\langle x' = f(x) \,\&\, Q\rangle\circ$ is uninformative (trivially true) if the initial state $\omega \in [\![Q]\!]$ and Q describes an open set, because existence and continuity already imply local progress. Excluding the initial state as in $\langle x' = f(x) \,\&\, Q\rangle\bigcirc$ makes this an insightful question, because it allows the possibility of starting on the topological boundary before entering the open set.

For brevity, we leave the $x = y$ assumption in the antecedents and axioms implicit in all subsequent derivations. For example, we shall elide the implicit $x = y$ assumption and write axiom Cont as:

$$\text{Cont}\ p > 0 \rightarrow \langle x' = f(x) \,\&\, p > 0\rangle\circ$$

Corollary 5.4 (Real induction rule)**.** *This rule derives from RI,Dadj.*

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

Proof Summary (Appendix A.4). The rule derives from RI, where we have used Dadj to axiomatically flip the signs of its second premise. □

Rule rI shows what our added axioms buys us: RI reduces global invariance properties of ODEs to local progress properties. These properties will be provable with Cont,Uniq and existing dL axioms. Both premises of rI allow us to assume that the formula we want to prove local progress for is true initially. Thus, we could have equivalently stated the succedent with $\circ$ modalities instead of $\bigcirc$ in both premises. The choice of $\bigcirc$ will be better for strict inequalities.

6 Semialgebraic Invariants

From now on, we simply assume domain constraint $Q \equiv \mathit{true}$ since Q is not fundamental [12] and not central to our discussion.[11] Any first-order formula of real arithmetic, P, characterizes a *semialgebraic set*, and by quantifier elimination [1] may equivalently be written as a finite, quantifier-free formula with polynomials p_{ij}, q_{ij}:

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

P is also called a *semialgebraic* formula, and the first step in our invariance proofs for semialgebraic P will be to apply rule rI, yielding premises of the form $P \vdash \langle x' = f(x) \,\&\, P\rangle\bigcirc$ (modulo sign changes and negation). The key insight then is that local progress can be completely characterized by a finite formula of real arithmetic.

6.1 Local Progress

Local progress was implicitly used previously for semialgebraic invariants [7, 9]. Here, we show how to derive the characterization syntactically in the dL calculus, starting from atomic inequalities. We observe interesting properties, e.g., self-duality, along the way.

6.1.1 Atomic Non-strict Inequalities

Let P be $p \geq 0$. Intuitively, since we only want to show *local progress*, it is sufficient to locally consider the *first* (significant) Lie derivative of p. This is made precise with the following key lemma.

Lemma 6.1 (Local progress step)**.** *The following axiom derives from Cont in* dL*.*

$$\text{LPi}_{\geq}\ \begin{array}{l} p \geq 0 \land \big(p = 0 \rightarrow \langle x' = f(x) \,\&\, \dot{p} \geq 0\rangle\circ\big) \\ \rightarrow \langle x' = f(x) \,\&\, p \geq 0\rangle\circ \end{array}$$

Proof. The proof starts with a case split since $p \geq 0$ is equivalent to $p > 0 \lor p = 0$. In the $p > 0$ case, Cont and dRW$\langle\cdot\rangle$ close the premise. The premise from the $p = 0$ case is abbreviated with ①.

$$\mathbb{R},\lor\text{L}\ \dfrac{\text{dRW}\langle\cdot\rangle\ \dfrac{\text{Cont}\ \dfrac{*}{p > 0 \vdash \langle x' = f(x) \,\&\, p > 0\rangle\circ}}{p > 0 \vdash \langle x' = f(x) \,\&\, p \geq 0\rangle\circ} \qquad ①}{p \geq 0,\ p = 0 \rightarrow \langle x' = f(x) \,\&\, \dot{p} \geq 0\rangle\circ \vdash \langle x' = f(x) \,\&\, p \geq 0\rangle\circ}$$

We continue on ① with DR$\langle\cdot\rangle$ and finish the proof using dI:

$$\rightarrow\text{L}\ \dfrac{\text{DR}\langle\cdot\rangle\ \dfrac{\text{dI}\ \dfrac{*}{p = 0 \vdash [x' = f(x) \,\&\, \dot{p} \geq 0]p \geq 0}}{p = 0,\ \langle x' = f(x) \,\&\, \dot{p} \geq 0\rangle\circ \vdash \langle x' = f(x) \,\&\, p \geq 0\rangle\circ}}{p = 0,\ p = 0 \rightarrow \langle x' = f(x) \,\&\, \dot{p} \geq 0\rangle\circ \vdash \langle x' = f(x) \,\&\, p \geq 0\rangle\circ}$$

□

Observe that $\text{LPi}_{\geq}$ allows us to pass from reasoning about local progress for $p \geq 0$ to local progress for its Lie derivative $\dot{p} \geq 0$ whilst accumulating $p = 0$ in the antecedent. Furthermore, this can be iterated for higher Lie derivatives, as in the following derivation:

$$\text{LPi}_{\geq}\ \dfrac{\Gamma \vdash p \geq 0 \qquad \text{LPi}_{\geq}\ \dfrac{\Gamma, p = 0 \vdash \dot{p} \geq 0 \qquad \text{LPi}_{\geq}\ \dfrac{\Gamma, p = 0, \dots \vdash \langle x' = f(x) \,\&\, \dot{p}^{(k)} \geq 0\rangle\circ}{\dots}}{\Gamma, p = 0 \vdash \langle x' = f(x) \,\&\, \dot{p} \geq 0\rangle\circ}}{\Gamma \vdash \langle x' = f(x) \,\&\, p \geq 0\rangle\circ}$$

Indeed, if we could prove $\dot{p}^{(k)} > 0$ from the antecedent, Cont,dRW$\langle\cdot\rangle$ finish the proof, because we must then locally enter $\dot{p}^{(k)} > 0$:

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

This derivation repeatedly examines higher Lie derivatives when lower ones are indeterminate ($p = 0, \dots, \dot{p}^{(k-1)} = 0$), until we

[11] We provide the case of arbitrary semialgebraic evolution domain Q in Appendix B.

find the *first* significant derivative with a definite sign ($\dot{p}^{(k)} > 0$). Fortunately, we already know that this terminates: when N is the rank of p, then once we gathered $p = 0, \ldots, \dot{p}^{(N-1)} = 0$, i.e., $\dot{p}^{(*)} = 0$ in the antecedents, dRI proves the invariant $p = 0$, and ODEs always locally progress in invariants. The following definition gathers the open premises above to obtain the *first significant Lie derivative.*

Definition 6.2 (Progress formula)**.** The *progress formula* $\dot{p}^{(*)} > 0$ for a polynomial p with rank $N{\geq}1$ is defined as the following formula, where Lie derivatives are with respect to $x' = f(x)$:

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

We define $\dot{p}^{(*)} \geq 0$ as $\dot{p}^{(*)} > 0 \lor \dot{p}^{(*)} = 0$. We write $\dot{p}^{-(*)} > 0$ (or $\dot{p}^{-(*)} \geq 0$) when taking Lie derivatives w.r.t. $x' = -f(x)$.

Lemma 6.3 (Local progress $\geq$)**.** *This axiom derives from LPi$_\geq$:*

$$\text{LP}_{\geq^*}\ \dot{p}^{(*)} \geq 0 \rightarrow \langle x' = f(x) \,\&\, p \geq 0 \rangle \circ$$

Proof Summary (Appendix B.2). This follows by the preceding discussion with iterated use of derived axioms LPi$_\geq$ and dRI. ◻

In order to prove $\langle x' = f(x) \,\&\, p \geq 0\rangle\circ$, it is not always necessary to consider the entire progress formula for p. The iterated derivation shows that once the antecedent $(\Gamma, p = 0, \ldots, \dot{p}^{(k-1)} = 0)$ implies that the next Lie derivative is significant ($\dot{p}^{(k)} > 0$), the proof can stop early without considering the remaining higher Lie derivatives.

6.1.2 Atomic Strict Inequalities

Let P be $p > 0$. Unlike the above non-strict cases, where $\bigcirc$ and $\circ$ were equivalent, we now exploit the $\bigcirc$ modality. The reason for this difference is that the set of states satisfying $p > 0$ is topologically open and, as mentioned earlier, it is possible to *locally enter* the set from an initial point on its boundary. This becomes important when we generalize to the case of semialgebraic P in normal form (2) because it allows us to move between its outer disjunctions.

Lemma 6.4 (Local progress $>$)**.** *This axiom derives from LPi$_\geq$:*

$$\text{LP}_{>^*}\ \dot{p}^{(*)} > 0 \rightarrow \langle x' = f(x) \,\&\, p > 0 \rangle \bigcirc$$

Proof Summary (Appendix B.2). We start by unfolding the syntactic abbreviation of the $\bigcirc$ modality, and observing that we can reduce to the non-strict case with dRW$\langle\cdot\rangle$ and the real arithmetic fact[12] $p \geq |x - y|^{2N} \rightarrow p > 0 \lor x = y$, where $N{\geq}1$ is the rank of p. The appearance of N in this latter step corresponds to the fact that we only need to inspect the first $N-1$ Lie derivatives of p with $\dot{p}^{(*)} > 0$. We further motivate this choice in the full proof (see Appendix B.2).

$$\dfrac{\dfrac{\overset{*}{\overline{p \geq |x-y|^{2N} \vdash p > 0 \lor x = y}}\ \mathbb{R} \qquad \Gamma \vdash \langle x' = f(x) \,\&\, p \geq |x-y|^{2N}\rangle\circ}{\Gamma \vdash \langle x' = f(x) \,\&\, p > 0 \lor x = y\rangle\circ}\ \text{dRW}\langle\cdot\rangle}{\Gamma \vdash \langle x' = f(x) \,\&\, p > 0\rangle\bigcirc}$$

We continue on the remaining open premise with iterated use of LPi$_\geq$, similar to the derivation for Lemma 6.3. ◻

[12] Here, $|x - y|^2$ is the squared Euclidean norm $(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2$

6.1.3 Semialgebraic Case

We finally lift the progress formulas for atomic inequalities to the general case of an arbitrary semialgebraic formula in normal form.

Definition 6.5 (Semialgebraic progress formula)**.** The *semialgebraic progress formula* $\dot{P}^{(*)}$ for a semialgebraic formula P written in normal form (2) is defined as follows:

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

We write $\dot{P}^{-(*)}$ when taking Lie derivatives w.r.t. $x' = -f(x)$.

Lemma 6.6 (Semialgebraic local progress)**.** *Let P be a semialgebraic formula in normal form* (2)*. The following axiom derives from* dL *extended with Cont,Uniq.*

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

Proof Summary (Appendix B.2). We decompose $\dot{P}^{(*)}$ according to its outermost disjunction, and accordingly decompose P in the local progress succedent with dRW$\langle\cdot\rangle$. We then use Uniq,$[\cdot]\land$ to split the conjunctive local progress condition in the resulting succedents of open premises, before finally utilizing LP$_{\geq^*}$ or LP$_{>^*}$, respectively. ◻

Lemma 6.6 implies that the implication in LP$\mathbb{R}$ can be strengthened to an equivalence. It also justifies our syntactic abbreviation $\bigcirc$, recalling that the $\bigcirc$ modality of temporal logic is self-dual.

Corollary 6.7 (Local progress completeness)**.** *Let P be a semialgebraic formula in normal form* (2)*. The following axioms derive from* dL *extended with Cont,Uniq.*

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

$$\neg\bigcirc\ \ \langle x' = f(x) \,\&\, P \rangle \bigcirc \leftrightarrow \neg\langle x' = f(x) \,\&\, \neg P \rangle \bigcirc$$

Proof Summary (Appendix B.2). Both follow because any P in normal form (2) has a corresponding normal form for $\neg P$ such that the equivalence $\neg(\dot{P}^{(*)}) \leftrightarrow (\dot{\neg P})^{(*)}$ is provable. Then apply Uniq,LP$\mathbb{R}$. ◻

In continuous time, there is no discrete next state, so unlike the $\bigcirc$ modality of discrete temporal logic, local progress is *idempotent*.

6.2 Completeness for Semialgebraic Invariants

We summarize our results with the following derived rule.

Theorem 6.8 (Semialgebraic invariants)**.** *For semialgebraic P with progress formulas $\dot{P}^{(*)}, (\dot{\neg P})^{-(*)}$ w.r.t. their respective normal forms* (2)*, this rule derives from the* dL *calculus with RI,Dadj,Cont,Uniq.*

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

Proof. Straightforward application of rI,LP. ◻

Completeness of sAI was proved semantically in [9] making crucial use of semialgebraic sets and analytic solutions to polynomial ODE systems. We showed that the sAI proof rule can be *derived* syntactically in the dL calculus and derive its completeness, too:

Theorem 6.9 (Semialgebraic invariant completeness)**.** *For semialgebraic P with progress formulas* $\dot{P}^{(*)}, \dot{(\neg P)}^{-(*)}$ *w.r.t. their respective normal forms* (2)*, this axiom derives from* dL *with RI,Dadj,Cont,Uniq.*

$$\text{SAI}\ \forall x\,(P \to [x' = f(x)]P) \leftrightarrow \forall x\,\big(P \to \dot{P}^{(*)}\big) \land \forall x\,\big(\neg P \to \dot{(\neg P)}^{-(*)}\big)$$

In Appendix B, we prove a generalization of Theorem 6.9 that handles semialgebraic evolution domains Q using LP and a corresponding generalization of axiom RI. Thus, dL decides invariance properties for all first-order real arithmetic formulas P, because quantifier elimination [1] can equivalently rewrite P to normal form (2) first. Unlike for Theorem 4.4, which can decide algebraic postconditions from any semialgebraic precondition, Theorem 6.9 (and its generalized version) are still limited to proving invariants, the search of which is the only remaining challenge.

Of course, sAI can be used to prove all the invariants considered in our running example. However, we had a significantly simpler proof for the invariance of $1 - u^2 - v^2 > 0$ with dbx$\succcurlyeq$. This has implications for implementations of sAI: simpler proofs help minimize dependence on real arithmetic decision procedures. Similarly, we note that if P is either topologically open (resp. closed), then the left (resp. right) premise of sAI closes trivially. Logically, this follows by the finiteness theorem [1, Theorem 2.7.2], which implies that formula $P \to \dot{P}^{(*)}$ is provable in real arithmetic for open semialgebraic P. Topologically, this corresponds to the fact that only one of the two exit trajectory cases in Section 5.2 can occur.

7 Related Work

We focus our discussion on work related to deductive verification of hybrid systems. Readers interested in ODEs [18], real analysis [3], and real algebraic geometry [1] are referred to the respective cited texts. Orthogonal to our work is the question of how invariants can be efficiently generated, e.g. [6, 9, 16].

Proof Rules for Invariants. There are numerous useful but incomplete proof rules for ODE invariants [15–17]. An overview can be found in [7]. The soundness and completeness theorems for dRI,sAI were first shown in [6] and [9] respectively.

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 [5]. 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 in *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. Our completeness results are axiomatic, so complete for disproofs.

Deductive Power and Proof Theory. The derivations shown in this paper are fully general, which is necessary for completeness of the resulting derived rules. The number of conjuncts in the progress and differential radical formulas, for example, are equal to the rank of p. Known upper bounds for the rank of p in n variables are doubly exponential in $n^2 \ln n$ [10]. Fortunately, 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 [7] 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 [13], 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 [12] 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 decide real arithmetic invariants syntactically.

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
Dadj	Group action on solutions
RI	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, but we leave further exploration of these issues to future work.

Acknowledgments

We thank Brandon Bohrer, Khalil Ghorbal, Andrew Sogokon, and the anonymous reviewers for their detailed feedback on this paper. This material is based upon work supported by the National Science Foundation under NSF CAREER Award CNS-1054246. The second author was also supported by A*STAR, Singapore.

References

[1] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. 1998. *Real Algebraic Geometry*. A Series of Modern Surveys in Mathematics, Vol. 36. Springer.
[2] 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.
[3] Pete L. Clark. 2012. The instructor's guide to real induction. (2012). arXiv:1208.0973
[4] 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.
[5] 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.
[6] 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.
[7] 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.

[8] Thomas H. Grönwall. 1919. Note on the derivative with respect to a parameter of the solutions of a system of differential equations. *Ann. Math.* 20, 4 (1919), 292–296.

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

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

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

[15] 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.

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

[17] 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.

[18] Wolfgang Walter. 1998. *Ordinary Differential Equations*. Springer.

A Differential Dynamic Logic Axiomatization

We work with dL's uniform substitution calculus presented in [14]. 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:

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

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

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

We refer readers to [14] 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. Differentials have a differential-form semantics [14] as the sum of all partial derivatives by all variables x multiplied by the corresponding values of x':

$$I\omega[\![(\theta)']\!] = \sum_x \omega(x') \frac{\partial I\omega[\![\theta]\!]}{\partial x}$$

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:

$(\omega, \nu) \in I[\![x' = f(x) \,\&\, Q]\!]$ 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 $\varphi(\zeta) \in I[\![x' = f(x) \wedge Q]\!]$, $\varphi(0) = \varphi(\zeta)$ 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 value of the RHS of the differential equations along the solution. We refer readers to [14, Definition 7] for further details.

The dL calculus allows all its axioms (cf. [14, 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. We shall directly use vectorial notation when presenting 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 [14].

A.1 Base Axiomatization

The following are the base axioms and axiomatic proof rules for dL from [14, Figure 2] where $\bar{x}$ is the vector of all variables.

Theorem A.1 (Base axiomatization [14]). *The following are sound axioms and proof rules for* dL.

$\langle\cdot\rangle$ $\langle a\rangle p(\bar{x}) \leftrightarrow \neg[a]\neg p(\bar{x})$

$[:=]$ $[x := f]p(x) \leftrightarrow p(f)$

$[?]$ $[?q]p \leftrightarrow (q \to p)$

$[\cup]$ $[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \wedge [b]p(\bar{x})$

$[;]$ $[a; b]p(\bar{x}) \leftrightarrow [a][b]p(\bar{x})$

$[^*]$ $[a^*]p(\bar{x}) \leftrightarrow p(\bar{x}) \wedge [a][a^*]p(\bar{x})$

K $[a](p(\bar{x}) \to q(\bar{x})) \to ([a]p(\bar{x}) \to [a]q(\bar{x}))$

I $[a^*]p(\bar{x}) \leftrightarrow p(\bar{x}) \wedge [a^*](p(\bar{x}) \to [a]p(\bar{x}))$

V $p \to [a]p$

G $\dfrac{p(\bar{x})}{[a]p(\bar{x})}$

In sequent calculus, these axioms (and axiomatic proof rules) are instantiated by uniform substitution and then used by congruence reasoning for equivalences (and equalities). All of the substitutions that we require are admissible [14, Definition 19]. We use weakening to elide assumptions from the antecedent without notice and, e.g., use Gödel's rule G directly as:

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

The $[\cdot]\wedge$ axiom derives from G,K [12]. The M$[\cdot]$ rule derives using G,K as well [14]. The loop induction rule derives from the induction axiom I using G on its right conjunct [12].

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

The presentation of the base axiomatization in Theorem A.1 follows [14], where $p(\bar{x})$ is used to indicate a predicate symbol which takes, $\bar{x}$, the vector of all variables. In the sequel, in order to avoid notational confusion with earlier parts of this paper, we return to using P for predicate symbols, reserving p for polynomial terms. Correspondingly, we return to using x for the vector of variables appearing in ODE $x' = f(x)$ when stating the dL axioms for differential equations.

A.2 Differential Equation Axiomatization

The following are axioms for differential equations and differentials from [14, Figure 3]. Note that when x is a vector of variables $x_1, x_2, \ldots, x_n$, then 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 [14]). *The following are sound axioms of* dL.

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

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

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

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

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

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

$$+'\quad (f(\bar{x}) + g(\bar{x}))' = (f(\bar{x}))' + (g(\bar{x}))'$$

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

We additionally use the Barcan axiom [12] specialized to ODEs in the diamond modality:

$$\text{B}'\quad \begin{aligned}&\langle x' = f(x)\,\&\,Q(x)\rangle \exists y P(x, y)\\ &\leftrightarrow \exists y\, \langle x' = f(x)\,\&\,Q(x)\rangle P(x, y)\end{aligned} \quad (y \notin x)$$

The ODE axiom B$'$ requires the variables y be fresh in x ($y \notin x$).

Syntactic differentiation under differential equations is performed using the DE axiom along with the axioms for working with differentials c',x',$+'$,$\cdot'$ [14, 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 $\succcurlyeq$:

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

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 $p_e \overset{\text{def}}{=} v^2 - u^2 + \frac{9}{2}$, unfolding the Lie derivative, we have:

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

In dL, we have the following derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdash [\alpha_e]\dot{p_e} \sim 0}{\vdash [\alpha_e]2v(u + \frac{v}{4}(1 - u^2 - v^2)) - 2u(-v + \frac{u}{4}(1 - u^2 - v^2)) \sim 0}\;\mathbb{R}}{\vdash [\alpha_e][u' := -v + \frac{u}{4}(1 - u^2 - v^2)][v' := u + \frac{v}{4}(1 - u^2 - v^2)]2vv' - 2uu' \sim 0}\;[:=]}{\vdash [\alpha_e][u' := -v + \frac{u}{4}(1 - u^2 - v^2)][v' := u + \frac{v}{4}(1 - u^2 - v^2)](p_e)' \sim 0}\;e'}{\vdash [\alpha_e](p_e)' \sim 0}\;\text{DE}$$

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 also use dL's coincidence lemmas [14, Lemma 10,11].

Lemma A.4 (Coincidence for terms and formulas [14])**.** *The following are coincidence properties of* dL*, where free variables $FV(e)$, $FV(\phi)$ are as defined in [14].*

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

We prove generalized versions of axioms from [14]. These are the vectorial differential ghost axioms (DG and DG$_\forall$)[13] which were proved only for the single variable case, and the differential modus ponens axiom, DMP, which was specialized for differential cuts.

Lemma A.5 (Generalized axiom soundness)**.** *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 an $m \times m$ matrix (resp. m-dimensional vector) of function symbols.*

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

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

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

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 ODEs that are (inhomogeneous) linear in $\mathbf{y}$. 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 $\omega_\mathbf{y}$ be identical to ω except where the values for variables $\mathbf{y}$ 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. 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 Lemma A.4, 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 $\varphi_\mathbf{y}(T)$ on x (since $\mathbf{y}$ is fresh), by Lemma A.4 we also have $\varphi_\mathbf{y}(T) \in I[\![P(x)]\!]$ 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

[13] We do not actually need DG$_\forall$ in this paper. We prove it for completeness, because [14] proves a similar axiom for single variable DG.

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 [14, 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:

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

By [18, §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 Lemma A.4,

$$I, \varphi_{\mathbf{y}} \models x' = f(x), \mathbf{y}' = a(x) \cdot \mathbf{y} + b(x) \,\&\, Q(x)$$

Thus, we have $\varphi_{\mathbf{y}}(T) \in I[\![P(x)]\!]$ from the RHS of DG. Since $\varphi(T)$ coincides with $\varphi_{\mathbf{y}}(T)$ on x, again by Lemma A.4 we have $\nu = \varphi(T) \in I[\![P(x)]\!]$ as required.

To prove soundness of DMP consider any initial state ω satisfying

① $\omega \in I[\![[x' = f(x) \,\&\, Q(x)](Q(x) \to R(x))]\!]$, 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 $\varphi : [0,T] \to \mathbb{S}$ 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 $\varphi(t) \in I[\![Q(x) \to R(x)]\!]$ 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.5, 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 By DMP we 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.

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

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

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

dI$_=$ The derivation is similar to dI$_{\succcurlyeq}$ using DI$_=$ instead of DI$_{\succcurlyeq}$. dI$_=$ also derives from dI$_{\succcurlyeq}$ using $[\cdot]\land$ with the equivalence $p = 0 \leftrightarrow p \geq 0 \land p \leq 0$.

dC We cut in a premise with postcondition $Q \to (Q \land C)$ and then reduce this postcondition to C by M$[\cdot]$ using the propositional tautology $C \to (Q \to (Q \land C))$. The right premise after the cut is abbreviated by ①.

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

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

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

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

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

◻

The soundness of DI$_{\succcurlyeq}$ is proved [14, Theorem 38] from the mean value theorem as follows. Briefly, consider any solution $\varphi : [0,T] \to \mathbb{S}$, and let $\varphi_p(t) \overset{\text{def}}{=} I\varphi(t)[\![p]\!]$ be the value of p along φ. We may, without loss of generality, assume $T > 0$, and $\varphi_p(0) \succcurlyeq 0$. By assumption on the left of the implication in DI$_{\succcurlyeq}$, $(p(x))' \geq 0$, which, by the differential lemma [14, Lemma 35], means $\frac{d\varphi_p(t)}{dt}(\zeta) \geq 0$ for $0 \leq \zeta \leq T$. The mean value theorem implies $\varphi_p(T) - \varphi_p(0) = \frac{d\varphi_p(t)}{dt}(\zeta)(T - 0)$ for some $0 < \zeta < T$. Since $\varphi_p(0) \succcurlyeq 0, T > 0$, and $\frac{d\varphi_p(t)}{dt}(\zeta) \geq 0$, we have $\varphi_p(T) \succcurlyeq 0$ as required. Conversely, a logical version of the mean value theorem derives from DI$_{\succcurlyeq}$:

Corollary A.6 (Mean value theorem)**.** *The following analogue of the mean value theorem derives from DI$_{\succcurlyeq}$:*

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

Proof. This follows immediately by taking contrapositives, dualizing with $\langle\cdot\rangle$, and then applying DI$_{\succcurlyeq}$. In the cut steps, we weakened the antecedents to implications since $P \to (Q \to P)$ is a propositional tautology for any formula P.

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

◻

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 prove the soundness of the axioms shown in Section 5 in uniform-substitution style after restating them as concrete dL formula instances. The axioms of Section 5 then derive as uniform substitution instances, because we only use them for concrete instances where the predicates involved (P, Q) mention all (proper) variables x changing in the respective system $x' = f(x)$.

For these proofs we will often need to take truncations of solutions $\varphi|_t$ (defined in Section 2.2). For any solution $\varphi : [0,T] \to \mathbb{S}$, 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 explained in Section 5, the soundness of the extended axioms require that the system $x' = f(x)$ always locally evolves x. In a uniform substitution formulation for Cont,RI&, the easiest syntactic check ensuring this condition is that the system contains an equation $x_1' = 1$. But our proofs are more general and only use the assumption that the system locally evolves x. The requirement that $x_1' = 1$ occurs is minor, since such a clock variable can always be added using DG if necessary before using the axioms. We elide these DG steps for subsequent derivations.

A.3.1 Existence, Uniqueness, and Continuity

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

Lemma A.7 (Continuous existence, uniqueness, and differential adjoints for Lemma 5.1)**.** *The following axioms are sound.*

$$\text{Uniq}\quad \big(\langle x' = f(x)\,\&\,Q_1(x)\rangle P_1(x)\big) \land \big(\langle x' = f(x)\,\&\,Q_2(x)\rangle P_2(x)\big) \rightarrow \langle x' = f(x)\,\&\,Q_1(x) \land Q_2(x)\rangle (P_1(x) \lor P_2(x))$$

$$\text{Cont}\quad x = y \rightarrow \big(g(x) > 0 \rightarrow \langle x' = f(x)\,\&\,g(x) > 0\rangle x \neq y\big)$$

$$\text{Dadj}\quad \langle x' = f(x)\,\&\,Q(x)\rangle\, x = y \leftrightarrow \langle y' = -f(y)\,\&\,Q(y)\rangle\, y = x$$

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 [18, §10.VI], from *any* state ω, there is an interval $[0, \tau)$, $\tau > 0$ on which there is a unique, continuous solution $\varphi : [0, \tau) \rightarrow \mathbb{S}$ with $\varphi(0) = \omega$ on $\{x'\}^{\complement}$. Moreover, the solution may be uniquely extended in time (to the right), up to its maximal open interval of existence [18, §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 exist two solutions $\varphi_1 : [0, T_1] \rightarrow \mathbb{S}$, $\varphi_2 : [0, T_2] \rightarrow \mathbb{S}$ from ω where $I, \varphi_1 \models x' = f(x)\,\&\,Q_1(x)$ and $I, \varphi_2 \models x' = f(x)\,\&\,Q_2(x)$, 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 $\varphi_1(T_1) \in I[\![P_1(x)]\!]$, which implies $\varphi_1(T_1) \in I[\![P_1(x) \lor P_2(x)]\!]$, 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 $\varphi_2(T_2) \in I[\![P_2(x)]\!]$. 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 $\omega \in I[\![x = y \land g(x) > 0]\!]$. By Picard-Lindelöf, there is a solution $\varphi : [0, \tau) \rightarrow \mathbb{S}$ with $\varphi(0) = \omega$ on $\{x'\}^{\complement}$ for some $\tau > 0$ such that $I, \varphi \models x' = f(x)$. Since $x' \notin g(x)$, coincidence (Lemma A.4) implies $I\varphi(0)[\![g(x)]\!] > 0$. As a composition of continuous evaluation [14, Definition 5] with the continuous solution φ, $I\varphi(t)[\![g(x)]\!]$ is a continuous function of time t. Thus, $I\varphi(0)[\![g(x)]\!] > 0$ implies $I\varphi(t)[\![g(x)]\!] > 0$ for all t in some interval $[0, T]$ with $0 < T < \tau$. Hence, the truncation $\varphi|_T$ satisfies

$$I, \varphi|_T \models x' = f(x)\,\&\,g(x) > 0$$

Since y is constant in the ODE but $x' = f(x)$ was assumed to locally evolve (for example with $x_1' = 1$), there is a time $0 < \epsilon \leq T$ at which $\varphi(\epsilon) \in I[\![x \neq y]\!]$. Thus, the truncation $\varphi|_\epsilon$ witnesses $\omega \in I[\![\langle x' = f(x)\,\&\,g(x) > 0\rangle x \neq y]\!]$.

Finally, we prove axiom Dadj. The "$\leftarrow$" direction follows immediately from the "$\rightarrow$" direction by swapping the names x, y, because $-(-f(x)) = f(x)$. Therefore, we only prove the "$\rightarrow$" direction. Consider an initial state ω where $\omega \in I[\![\langle x' = f(x)\,\&\,Q(x)\rangle\, x = y]\!]$. Unfolding the semantics, there is a solution $\varphi : [0, T] \rightarrow \mathbb{S}$, of the system $x' = f(x)$, with $\varphi(0) = \omega$ on $\{x'\}^{\complement}$, with $\varphi(t) \in I[\![Q(x)]\!]$ for all t, and $\varphi(T) \in I[\![x = y]\!]$.

Note that since the variables y do not appear in the differential equations, its value is held constant along the solution φ. Now, let us consider the time- and variable reversal $\psi : [0, T]$, where

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

By construction, $\psi(0)$ agrees with ω on $\{y'\}^{\complement}$, because $\varphi(T) \in I[\![x = y]\!]$. Moreover, we have explicitly negated the signs of the differential variables y_i' along ψ. By uniqueness, the solutions of $x' = -f(x)$ are exactly the time-reversed solutions of $x' = f(x)$. As we have constructed, ψ is the time-reversed solution for $x' = f(x)$ except we have replaced variables x by y instead. Moreover, since $\varphi([0, T]) \in I[\![Q(x)]\!]$, we also have $\psi([0, T]) \in I[\![Q(y)]\!]$ by construction and Lemma A.4. Therefore, $I, \psi \models y' = -f(y)\,\&\,Q(y)$. Finally, observe that $\psi(T)(y) = \varphi(0)(x)$, but ψ holds the values of x constant, thus $\psi(T)(x) = \varphi(0)(x)$ and so $\psi(T) \in I[\![y = x]\!]$. Therefore, ψ is a witness for

$$\omega \in I[\![\langle y' = -f(y)\,\&\,Q(y)\rangle y = x]\!] \qquad \square$$

A.3.2 Real Induction

For completeness, we state and prove a succinct version of the real induction principle that we use. This and other principles are in [3].

Definition A.8 (Inductive subset [3])**.** The subset $S \subseteq [a, b]$ is called an *inductive* subset of the compact interval $[a, b]$ iff for all $a \leq x \leq b$ and $[a, x) \subseteq S$,

① $x \in S$.
② If $x < b$ then $[x, x + \epsilon] \subseteq S$ for some $0 < \epsilon$.

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

Proposition A.9 (Real induction principle [3])**.** *The subset $S \subseteq [a, b]$ is inductive if and only if $S = [a, b]$.*

Proof. In the "$\Rightarrow$" direction, if $S = [a, b]$, then S is inductive by definition. For the "$\Leftarrow$" direction, let $S \subseteq [a, b]$ be inductive. Suppose that $S \neq [a, b]$, so that the complement set $S^{\complement} = [a, b] \setminus S$ is nonempty. Let x be the infimum of $S^{\complement}$, and note that $x \in [a, b]$ since $[a, b]$ is left-closed.

First, we note that $[a, x) \subseteq S$. Otherwise, x is not an infimum of $S^{\complement}$, because there would exist $a \leq y < x$, such that $y \in S^{\complement}$. By ①, $x \in S$. Next, if $x = b$, then $S = [a, b]$, contradiction. Thus, $x < b$, and by ②, $[x, x + \epsilon] \subseteq S$ for some $\epsilon > 0$. However, this implies that $x + \epsilon$ is a greater lower bound of $S^{\complement}$ than x, contradiction. $\square$

We now restate and prove a generalized, concrete version of the real induction axiom given in Lemma 5.3. This strengthened version includes the evolution domain constraint.

Lemma A.10 (Real induction for Lemma 5.3)**.** *The following real induction axiom is sound, where y is fresh in $[x' = f(x) \& Q(x)]P(x)$.*

$$\text{RI\&}\ [x' = f(x) \& Q(x)]P(x) \leftrightarrow$$
$$\forall y\, [x' = f(x) \& Q(x) \wedge (P(x) \vee x = y)]\Big(x{=}y \rightarrow P(x) \wedge \quad \text{(ⓐ)}$$
$$\big(\langle x' = f(x) \& Q(x)\rangle x \neq y \rightarrow \langle x' = f(x) \& P(x)\rangle x \neq y\big)\Big) \quad \text{(ⓑ)}$$

Proof. We label the two conjuncts on the RHS of RI& as ⓐ and ⓑ respectively, as shown above. Consider an initial state ω, we prove both directions of the axiom separately.

"$\rightarrow$" Assume that ⊛ $\omega \in I[\![[x' = f(x) \& Q(x)]P(x)]\!]$. Unfolding the quantification and box modality on the RHS, let ω_y be identical to ω except where the values for y are replaced with any initial values $d \in \mathbb{R}^n$. Consider any solution $\varphi_y : [0,T] \rightarrow \mathbb{S}$ of $x' = f(x) \& Q(x) \wedge (P(x) \vee x = y)$ where $\varphi_y(0) = \omega_y$ on $\{x'\}^{\complement}$, $\varphi_y(T) \in I[\![x{=}y]\!]$, and

$$I, \varphi_y \models x' = f(x) \& Q(x) \wedge (P(x) \vee x = y)$$

We construct a similar solution $\varphi : [0,T] \rightarrow \mathbb{S}$ that keeps y constant at their initial values in ω:

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

By construction, $\varphi(0)$ is identical to ω on $\{x'\}^{\complement}$. Since y is fresh in $x' = f(x) \& Q(x)$, by coincidence (Lemma A.4), we must have $I, \varphi \models x' = f(x) \& Q(x)$. By assumption ⊛, $\varphi(T) \in I[\![P(x)]\!]$, which implies that $\varphi_y(T) \in I[\![P(x)]\!]$ by coincidence since y is fresh in $P(x)$. This proves conjunct ⓐ. Unfolding the implication and diamond modality of conjunct ⓑ, we may assume that there is another solution $\psi_y : [0,\tau] \rightarrow \mathbb{S}$ starting from $\varphi_y(T)$ with $\psi_y(\tau) \in I[\![x \neq y]\!]$ and $I, \psi_y \models x' = f(x) \& Q(x)$. Note that $\psi_y(0) = \varphi_y(T)$ *exactly* rather than just on $\{x'\}^{\complement}$, because both of these states already have the same values for the differential variables. We need to show:

$$\varphi_y(T) \in I[\![\langle x' = f(x) \& P(x)\rangle x \neq y]\!]$$

We shall directly show:

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

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

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

As with φ, the solution Φ is constructed to keep y constant at their initial values in ω. Since ψ_y must uniquely extend φ_y [18, §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 by coincidence (Lemma A.4). Hence, by ⊛, $\Phi(T + \zeta) \in I[\![P(x)]\!]$, which implies $\psi_y(\zeta) \in I[\![P(x)]\!]$ by coincidence (Lemma A.4), as required.

"$\leftarrow$" We assume the RHS and prove the LHS in initial state ω. If $\omega \notin I[\![Q(x)]\!]$, then there is nothing to show, because there are no solutions that stay in $Q(x)$. Otherwise, consider an arbitrary solution $\varphi : [0,T] \rightarrow \mathbb{S}$ starting from ω such that $I, \varphi \models x' = f(x) \& Q(x)$. We prove $\varphi([0,T]) \in I[\![P(x)]\!]$ by showing that the subset $S \stackrel{\text{def}}{=} \{\zeta : \varphi(\zeta) \in I[\![P(x)]\!]\}$ is an inductive subset of $[0,T]$ i.e., satisfies properties ① and ② in Def. A.8. So, assume that $[0,\zeta) \subseteq S$ for some time $0 \leq \zeta \leq T$. Consider the state ω_y identical to ω, except where the values for variables y are replaced with the corresponding values of x in $\varphi(\zeta)$:

$$\omega_y(z) \stackrel{\text{def}}{=} \begin{cases} \varphi(\zeta)(x_i) & z = y_i \\ \omega(z) & \text{otherwise} \end{cases}$$

Correspondingly, consider the solution $\varphi_y : [0,\zeta] \rightarrow \mathbb{S}$ identical to φ but which keeps y constant at initial values in ω_y rather than in ω:

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

By coincidence (Lemma A.4), φ_y solves $x' = f(x) \& Q(x)$ from initial state ω_y. We still know $\varphi_y([0,\zeta)) \in I[\![P(x)]\!]$ by coincidence. Additionally, note that $\varphi_y(\zeta) \in I[\![x = y]\!]$ by construction. Therefore, $\varphi_y([0,\zeta]) \in I[\![Q(x) \wedge (P(x) \vee x = y)]\!]$. We now unfold the quantification, box modality and implication on the RHS to obtain:

$$\varphi_y(\zeta) \in I[\![ⓐ \wedge ⓑ]\!]$$

① We need to show $\varphi(\zeta) \in I[\![P(x)]\!]$, but by ⓐ, we have $\varphi_y(\zeta) \in I[\![P(x)]\!]$. By coincidence (Lemma A.4), this implies $\varphi(\zeta) \in I[\![P(x)]\!]$.

② We further assume that $\zeta < T$, and we need to show $\varphi([\zeta, \zeta + \epsilon]) \in I[\![P(x)]\!]$ for some $\epsilon > 0$. We shall first discharge the implication in ⓑ, i.e. we show:

$$\varphi_y(\zeta) \in I[\![\langle x' = f(x) \& Q(x)\rangle x \neq y]\!]$$

Observe that since $\zeta < T$, we may consider the solution that extends from state $\varphi(\zeta)$, i.e., $\psi : [0, T - \zeta] \rightarrow \mathbb{S}$, where $\psi(\tau) \stackrel{\text{def}}{=} \varphi(\tau + \zeta)$, and we have $I, \psi \models x' = f(x) \& Q(x)$. We correspondingly construct the solution that extends from state $\varphi_y(\zeta)$, $\psi_y : [0, T - \zeta] \rightarrow \mathbb{S}$ that keeps y constant instead:

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

We already know $\varphi_y(\zeta) \in I[\![x = y]\!]$. We also have $T - \zeta > 0$, and therefore, since the differential equation is assumed to always locally evolve (for example $x_1' = 1$), there must be some duration $0 < \epsilon < T - \zeta$ after which the value of x has changed from its initial value which is held constant in y, i.e., $\psi_y(\epsilon) \in I[\![x \neq y]\!]$. In other words, the truncation $\psi_y|_\epsilon$ witnesses:

$$\varphi_y(\zeta) \in I[\![\langle x' = f(x) \& Q(x)\rangle x \neq y]\!]$$

Discharging the implication in ⓑ, we obtain:

$$\varphi_y(\zeta) \in I[\![\langle x' = f(x) \& P(x)\rangle x \neq y]\!]$$

Unfolding the semantics gives us a solution, which by uniqueness, yields a truncation $\psi_y|_\epsilon$ of ψ_y, for some $\epsilon > 0$ which starts from $\varphi_y(\zeta)$ and satisfies $\psi_y|_\epsilon([0,\epsilon]) \in I[\![P(x)]\!]$. By construction, $\psi_y|_\epsilon(\tau)$ coincides with $\varphi(\tau+\zeta)$ on x for all $0 \le \tau \le \epsilon$, which implies $\varphi([\zeta,\zeta+\epsilon]) \in I[\![P(x)]\!]$ by Lemma A.4. ◻

A.4 Derived Rules and Axioms

We now derive several useful rules and axioms that we will use in subsequent derivations. Some of which were already proved in [12, 14] so their proofs are omitted.

A.4.1 Basic Derived Rules and Axioms

We start with basic derived rules and axioms of dL. The axiom K⟨·⟩ derives from K by dualizing its inner implication with ⟨·⟩ [12], and the rule M⟨·⟩ derives by G on the outer assumption of K⟨·⟩ [14].

$$\text{K}\langle\cdot\rangle \quad \begin{array}{l}[\alpha](\phi_2 \to \phi_1)\\ \to (\langle\alpha\rangle\phi_2 \to \langle\alpha\rangle\phi_1)\end{array} \qquad \text{M}\langle\cdot\rangle\ \frac{\phi_2 \vdash \phi_1 \qquad \Gamma \vdash \langle\alpha\rangle\phi_2}{\Gamma \vdash \langle\alpha\rangle\phi_1}$$

If $R(y)$ is true in an initial state and y has no differential equation in $x' = f(x)$, then it trivially continues to hold along solutions to the differential equations from that state because y remains constant along these solutions. Axiom V proves this for box modalities (and for diamond modalities in the antecedents):

$$\text{dC}\ \dfrac{\text{V}\ \dfrac{*}{R(y) \vdash [x' = f(x)\,\&\,Q]R(y)} \qquad \Gamma \vdash [x' = f(x)\,\&\,Q \land R(y)]P}{\Gamma, R(y) \vdash [x' = f(x)\,\&\,Q]P}$$

Conversely, if $R(y)$ is true in a final state reachable by an ODE $x' = f(x)$, then it must have trivially been true initially. In the derivation below, the open premise labelled ① closes because it leads to a domain constraint that contradicts the postcondition of the diamond modality.

$$\text{cut}\ \dfrac{\lor\text{L}\ \dfrac{\Gamma, R(y), \langle x' = f(x)\,\&\,Q\rangle(P \land R(y)) \vdash \phi \qquad ①}{\Gamma, R(y) \lor \neg R(y), \langle x' = f(x)\,\&\,Q\rangle(P \land R(y)) \vdash \phi}}{\Gamma, \langle x' = f(x)\,\&\,Q\rangle(P \land R(y)) \vdash \phi}$$

To prove premise ①, we use V,dC,⟨·⟩

$$\langle\cdot\rangle,\neg\text{L}\ \dfrac{\text{dC,V}\ \dfrac{\text{dW}\ \dfrac{*}{\vdash [x' = f(x)\,\&\,Q \land \neg R(y)]\neg(P \land R(y))}}{\neg R(y) \vdash [x' = f(x)\,\&\,Q]\neg(P \land R(y))}}{\neg R(y), \langle x' = f(x)\,\&\,Q\rangle(P \land R(y)) \vdash \mathit{false}}$$

In the sequel, we omit these routine steps and label proof steps that manipulate constant context assumptions with V directly.

We now prove Corollary 5.2, which provides tools for working with diamond modalities involving ODEs.

Proof of Corollary 5.2. Axiom DR⟨·⟩ derives from DMP by dualizing with the ⟨·⟩ axiom.

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

Rule dRW⟨·⟩ derives from DR⟨·⟩ by simplifying its left premise with rule dW. ◻

A.4.2 Extended Derived Rules and Axioms

We derive additional rules and axioms that make use of our axiomatic extensions.

Corollary A.11 (Extended diamond modality rules and axioms)**.** *The following are derived axioms in* dL *extended with Uniq,Dadj.*

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

$$\text{reflect}_{\langle\cdot\rangle} \quad \begin{array}{l}\exists x\,(P(x) \land \langle x' = f(x)\,\&\,Q(x)\rangle R(x))\\ \leftrightarrow \exists x\,(R(x) \land \langle x' = -f(x)\,\&\,Q(x)\rangle P(x))\end{array}$$

Proof. The equivalence ⟨&∧⟩ derives from dRW⟨·⟩ for the "→" direction, because of the propositional tautologies $Q \land R \to Q$ and $Q \land R \to R$. The "←" direction is an instance of Uniq by setting P_1, P_2 to P, and Q_1, Q_2 to Q, R respectively.

We prove reflect$_{\langle\cdot\rangle}$ from Dadj. Both implications are proved separately and the "←" direction follows by instantiating the proof of the "→" direction, since $-(-f(x)) = f(x)$.

In the derivation below, the succedent is abbreviated with $\phi \stackrel{\text{def}}{\equiv} \exists z\,(R(z) \land \langle z' = -f(z)\,\&\,Q(z)\rangle P(z))$, where we have renamed the variables for clarity. The first cut,M⟨·⟩ step introduces an existentially quantified z under the diamond modality using the provable first-order formula $R(y) \to \exists z\,(z = y \land R(z))$. Next, Barcan B′ moves the existentially quantified z out of the diamond modality.

$$\exists\text{L}\ \dfrac{\text{cut,M}\langle\cdot\rangle\ \dfrac{\text{B}'\ \dfrac{\exists\text{L}\ \dfrac{P(y), \langle y' = f(y)\,\&\,Q(y)\rangle(z = y \land R(z)) \vdash \phi}{P(y), \exists z\,\langle y' = f(y)\,\&\,Q(y)\rangle(z = y \land R(z)) \vdash \phi}}{P(y), \langle y' = f(y)\,\&\,Q(y)\rangle\exists z\,(z = y \land R(z)) \vdash \phi}}{P(y), \langle y' = f(y)\,\&\,Q(y)\rangle R(y) \vdash \phi}}{\exists x\,(P(x) \land \langle x' = f(x)\,\&\,Q(x)\rangle R(x)) \vdash \phi}$$

Continuing, since z is not bound in $y' = f(y)$, a V step allows us to move $R(z)$ out from under the diamond modality in the antecedents. We then use Dadj to flip the differential equations from evolving y forwards to evolving z backwards. The V,K⟨·⟩ step uses the fact that the (new) ODE does not modify y so that $P(y)$ remains true along the ODE, which allows its postcondition to be strengthened to $P(z)$, yielding a witness for the succedent.

$$\text{V}\ \dfrac{\text{Dadj}\ \dfrac{\text{V,K}\langle\cdot\rangle\ \dfrac{\exists\text{R}\ \dfrac{*}{R(z), \langle z' = -f(z)\,\&\,Q(z)\rangle P(z) \vdash \phi}}{P(y), R(z), \langle z' = -f(z)\,\&\,Q(z)\rangle z = y \vdash \phi}}{P(y), R(z), \langle y' = f(y)\,\&\,Q(y)\rangle z = y \vdash \phi}}{P(y), \langle y' = f(y)\,\&\,Q(y)\rangle(z = y \land R(z)) \vdash \phi}$$

◻

An invariant reflection principle derives from reflect$_{\langle\cdot\rangle}$: the negation of invariants $P(x)$ of the forwards differential equations $x' = f(x)$ are invariants of the backwards differential equations $x' = -f(x)$.

Corollary A.12 (Reflection)**.** *The invariant reflection axiom derives from axiom Dadj:*

$$\text{reflect} \quad \begin{array}{l}\forall x\,\big(P(x) \to [x' = f(x)\,\&\,Q(x)]P(x)\big)\\ \leftrightarrow \forall x\,\big(\neg P(x) \to [x' = -f(x)\,\&\,Q(x)]\neg P(x)\big)\end{array}$$

Proof. The axiom derives from reflect$_{\langle\cdot\rangle}$ by instantiating it with $R \stackrel{\text{def}}{\equiv} \neg P$ and negating both sides of the equivalence with ⟨·⟩. ◻

Finally, we derive the real induction rule corresponding to axiom RI&. We will use the ∘ abbreviation from Section 5 in the statement of the rule but explicitly include $x{=}y$ which was elided for brevity in Section 6.

Corollary A.13 (Real induction rule with domain constraints for Corollary 5.4)**.** *This rule (with two stacked premises) derives from RI&,Dadj,Uniq.*

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

Proof. We label the premises of rI& with ⓐ for the top premise and ⓑ for the bottom premise. The derivation starts by rewriting the succedent with RI&. We have abbreviated the second conjunct from this step with $R \stackrel{\text{def}}{\equiv} \langle x' = f(x) \,\&\, Q\rangle\circ \rightarrow \langle x' = f(x) \,\&\, P\rangle\circ$. The M[·] step rewrites the postcondition with the propositional tautology $(x{=}y \rightarrow P \land R) \leftrightarrow (x{=}y \rightarrow P) \land (x{=}y \rightarrow P \rightarrow R)$. We label the two premises after [·]∧,∧R with ① and ② respectively.

$$\dfrac{\dfrac{\dfrac{\dfrac{① \qquad ②}{P \vdash [x' = f(x) \,\&\, Q \land (P \lor x{=}y)]((x{=}y \rightarrow P) \land (x{=}y \rightarrow P \rightarrow R))}\,[\cdot]\land,\land R}{P \vdash [x' = f(x) \,\&\, Q \land (P \lor x{=}y)](x{=}y \rightarrow P \land R)}\,M[\cdot]}{P \vdash \forall y\, [x' = f(x) \,\&\, Q \land (P \lor x{=}y)](x{=}y \rightarrow P \land R)}\,\forall R}{P \vdash [x' = f(x) \,\&\, Q]P}\,RI\&$$

We continue from open premise ② with a dW step, which yields the premise ⓐ of rI& (by unfolding our abbreviation for R):

$$\dfrac{\dfrac{ⓐ}{Q \vdash (x{=}y \rightarrow P \rightarrow R)}\,\rightarrow R}{P \vdash [x' = f(x) \,\&\, Q \land (P \lor x{=}y)](x{=}y \rightarrow P \rightarrow R)}\,dW$$

We continue from the open premise ① by case splitting on the left with the provable real arithmetic formula $x{=}y \lor x \neq y$. This yields two further cases labelled ③ and ④.

$$\dfrac{\dfrac{③ \qquad ④}{x{=}y \lor x \neq y,\, P \vdash [x' = f(x) \,\&\, Q \land (P \lor x{=}y)](x{=}y \rightarrow P)}\,\lor L}{P \vdash [x' = f(x) \,\&\, Q \land (P \lor x{=}y)](x{=}y \rightarrow P)}\,cut,\mathbb{R}$$

For ③, since $x{=}y$ initially, we are trivially done, because $P(y)$ is true initially, and y is held constant by $x' = f(x)$. This is proved with an M[·] step followed by V.

$$\dfrac{\dfrac{*}{P(y) \vdash [x' = f(x) \,\&\, Q \land (P \lor x{=}y)]P(y)}\,V}{x{=}y,\, P \vdash [x' = f(x) \,\&\, Q \land (P \lor x{=}y)](x{=}y \rightarrow P)}\,cut,M[\cdot]$$

For ④, where $x \neq y$, we first use DW to assume Q in the postcondition. Abbreviate $S \stackrel{\text{def}}{\equiv} P \lor x{=}y$. We then move into the diamond modality, and use reflect$_{\langle\cdot\rangle}$. We cut the succedent of premise ⓑ. The resulting two open premises are labelled ⑤ and ⑥.

$$\dfrac{\dfrac{\dfrac{\dfrac{⑤ \qquad ⑥}{x{=}y \land Q \land \neg P,\, \langle x' = -f(x) \,\&\, Q \land S\rangle(x \neq y \land P) \vdash false}\,cut}{x \neq y \land P,\, \langle x' = f(x) \,\&\, Q \land S\rangle(Q \land x{=}y \land \neg P) \vdash false}\,reflect_{\langle\cdot\rangle}}{x \neq y,\, P \vdash [x' = f(x) \,\&\, Q \land S](Q \rightarrow x{=}y \rightarrow P)}\,\langle\cdot\rangle,\neg R}{x \neq y,\, P \vdash [x' = f(x) \,\&\, Q \land S](x{=}y \rightarrow P)}\,M[\cdot],DW$$

The premise ⑤ reduces to premise ⓑ, after we use M⟨·⟩,dRW⟨·⟩ to simplify the diamond modality assumption in the antecedents. The dRW⟨·⟩ step proves with the propositional tautology $Q \land S \rightarrow Q$.

$$\dfrac{\dfrac{\dfrac{ⓑ}{x{=}y,\, Q,\, \neg P,\, \langle x' = -f(x) \,\&\, Q\rangle x \neq y \vdash \langle x' = -f(x) \,\&\, \neg P\rangle\circ}}{x{=}y,\, Q,\, \neg P,\, \langle x' = -f(x) \,\&\, Q \land S\rangle x \neq y \vdash \langle x' = -f(x) \,\&\, \neg P\rangle\circ}\,dRW\langle\cdot\rangle}{x{=}y,\, Q,\, \neg P,\, \langle x' = -f(x) \,\&\, Q \land S\rangle(x \neq y \land P) \vdash \langle x' = -f(x) \,\&\, \neg P\rangle\circ}\,M\langle\cdot\rangle$$

Premise ⑥ uses the cut. The first dRW⟨·⟩ step unfolds the syntactic abbreviation in ∘, and drops Q from the domain constraint with the tautology $Q \land S \rightarrow S$. We then combine the two diamond modalities in the antecedents with Uniq and simplify its resulting domain constraint and postcondition with M⟨·⟩,dRW⟨·⟩, which respectively use the tautologies $x{\neq}y \lor x{\neq}y \land P \leftrightarrow x{\neq}y$ and $\neg P \land S \rightarrow x{=}y$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\langle x' = -f(x) \,\&\, x{=}y\rangle\, x{\neq}y \vdash false}{\langle x' = -f(x) \,\&\, \neg P \land S\rangle\, x{\neq}y \vdash false}\,dRW\langle\cdot\rangle}{\langle x' = -f(x) \,\&\, \neg P \land S\rangle(x{\neq}y \lor x{\neq}y \land P) \vdash false}\,M\langle\cdot\rangle}{\langle x' = -f(x) \,\&\, \neg P\rangle x{\neq}y,\, \langle x' = -f(x) \,\&\, S\rangle(x{\neq}y \land P) \vdash false}\,Uniq}{\langle x' = -f(x) \,\&\, \neg P\rangle\circ,\, \langle x' = -f(x) \,\&\, Q \land S\rangle(x{\neq}y \land P) \vdash false}\,dRW\langle\cdot\rangle$$

We complete the proof of ⑥ by dualizing and dW, since the domain constraint and postcondition of the diamond modality in the antecedents is contradictory.

$$\dfrac{\dfrac{*}{\vdash [x' = -f(x) \,\&\, x{=}y]x{=}y}\,dW}{\langle x' = -f(x) \,\&\, x{=}y\rangle x{\neq}y \vdash false}\,\langle\cdot\rangle,\neg L$$

□

The rule rI& discards any additional context in the antecedents of its premises. Intuitively, this is due to the use of RI& which focuses on particular states along trajectories of the ODE $x' = f(x)$; it would be unsound to keep any assumptions about the initial state that depend on x because we may not be at the initial state! On the other hand, assumptions that do not depend on x remain true along the ODE. They can be kept with uses of V throughout the derivation above or added into Q before using rI& by a dC that proves with V. We elide these additional steps, and directly use rule rI& while keeping these constant context assumptions around.

rI& is derived with the ∘ modality. However, it is easy to convert between the two modalities with the following derived axiom.

Corollary A.14 (Initial state inclusion)**.** *This is a derived axiom.*

$$\text{Init}\ x{=}y \land P \rightarrow \big(\langle x' = f(x) \,\&\, P\rangle\circ \leftrightarrow \langle x' = f(x) \,\&\, P\rangle\bigcirc\big)$$

Proof. We derive both directions of the equivalence by unfolding the syntactic abbreviations. In the "→" direction, a dRW⟨·⟩ step is sufficient, because $P \rightarrow P \lor x{=}y$ is a propositional tautology:

$$\dfrac{*}{x{=}y,\, P,\, \langle x' = f(x) \,\&\, P\rangle x \neq y \vdash \langle x' = f(x) \,\&\, P \lor x{=}y\rangle x \neq y}\,dRW\langle\cdot\rangle$$

In the "←" direction, we start with a DR⟨·⟩ step to reduce to the box modality. We then cut $P(y)$, which proves from antecedents $x = y, P$. This is then introduced in the domain constraint by V, which allows us to close the proof by dW.

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{\vdash [x' = f(x) \,\&\, (P \lor x{=}y) \land P(y)]P}\,dW}{P(y) \vdash [x' = f(x) \,\&\, P \lor x{=}y]P}\,V}{x{=}y,\, P \vdash [x' = f(x) \,\&\, P \lor x{=}y]P}\,cut}{x{=}y,\, P,\, \langle x' = f(x) \,\&\, P \lor x{=}y\rangle x \neq y \vdash \langle x' = f(x) \,\&\, P\rangle x \neq y}\,DR\langle\cdot\rangle$$

□

With Init, we may equivalently rewrite the premises of rI& with the ◯ modality, and so we will directly use it with ◯ instead of ∘. Similarly, rule rI from Corollary 5.4 derives from rI& with $Q \equiv true$.

Continuity (and local progress characterizations) generalize to open semialgebraic Q. Intuitively, the soundness of Cont only required that $p > 0$ characterized an open set. The derived axiom Cont^O builds on Cont to prove a stronger analogue for any formula characterizing an open semialgebraic set.

Corollary A.15 (Open continuity)**.** *Let Q be a formula characterizing an open semialgebraic set, this axiom derives from Cont,Uniq.*

$$\text{Cont}^O\ x{=}y \rightarrow \big(Q \rightarrow \langle x' = f(x) \,\&\, Q\rangle\circ\big)$$

Proof. Since Q characterizes an open, semialgebraic set, by the finiteness theorem [1, Theorem 2.7.2] for open semialgebraic sets, Q may be written as follows (q_{ij} are polynomials):

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

We may assume that Q is written in this form by an application of $\mathbb{R}$ (and congruence or DR⟨·⟩). Throughout this proof, we collapse similar premises in derivations and index them by i, j. We abbreviate the i-th disjunct of Q with $Q_i \stackrel{\text{def}}{\equiv} \bigwedge_{j=0}^{m(i)} q_{ij} > 0$.

We start by splitting on the outermost disjunction of Q with ∨L. For each resulting premise (indexed by i), we select the corresponding disjunct of Q to prove local progress. The domain change with dRW$\langle\cdot\rangle$ proves since $Q_i \to Q$ is a propositional tautology for each i.

$$\dfrac{\dfrac{x{=}y,\, Q_i \vdash \langle x' = f(x) \,\&\, Q_i \rangle\circ}{x{=}y,\, Q_i \vdash \langle x' = f(x) \,\&\, Q \rangle\circ}\,\mathrm{dRW}\langle\cdot\rangle}{x{=}y,\, Q \vdash \langle x' = f(x) \,\&\, Q \rangle\circ}\,\vee\mathrm{L}$$

Now, we only need to prove local progress in Q_i. We make use of $\langle\&\wedge\rangle$ to split up the conjunction in Q_i. This leaves premises (indexed by j) which are all closed by Cont.

$$\dfrac{\dfrac{*}{x{=}y,\, q_{ij} > 0 \vdash \langle x' = f(x) \,\&\, q_{ij} > 0 \rangle\circ}\,\mathrm{Cont}}{x{=}y,\, \bigwedge_{j=0}^{m(i)} q_{ij} > 0 \vdash \langle x' = f(x) \,\&\, Q_i \rangle\circ}\,\langle\&\wedge\rangle,\wedge\mathrm{R}$$

□

B Completeness

This appendix gives the full completeness arguments for the derived rules dRI and sAI (and the local progress conditions LP). We prove the completeness of dRI by showing that DRI is a derived axiom. We take a similar approach for sAI, although the precise form of the resulting derived axiom is more involved. We take syntactic approaches to proving completeness of dRI and sAI to demonstrate the versatility of the dL calculus and make it possible to disprove invariance properties (as opposed to just failing to apply a complete proof rule). We refer the readers to other presentations [6, 9] for purely semantical completeness arguments for invariants. Recall from Appendix A.3, that axioms Cont,RI& have an additional syntactic requirement, e.g. $x_1' = 1$. We assume that the syntactic requirement is met throughout this appendix, using DG if necessary, but elide the explicit proof steps.

The $\bigcirc$ and $\circ$ modalities have their corresponding semantic readings only when the assumption $x{=}y$ is true in the initial state Section 5. This additional assumption was elided in Section 6 for brevity, but is expanded in full in this appendix. For clarity, we re-state the derived axioms from Section 6 with this additional assumption where necessary. The ideas for these proofs are in the main paper.

B.1 Progress Formulas

We start with following useful observation on rearrangements of the progress formulas for polynomials:

Proposition B.1. *Let N be the rank of p. The following are provable equivalences on the progress and differential radical formulas.*

$$\begin{aligned}\dot{p}^{(*)} > 0 \leftrightarrow\; & p > 0 \vee (p = 0 \wedge \dot{p} > 0)\\ & \vee \ldots\\ & \vee \big(p = 0 \wedge \dot{p} = 0 \wedge \cdots \wedge \dot{p}^{(N-2)} = 0 \wedge \dot{p}^{(N-1)} > 0\big)\end{aligned} \tag{3}$$

$$\begin{aligned}\dot{p}^{(*)} \geq 0 \leftrightarrow\; & p \geq 0 \wedge \big(p = 0 \rightarrow \dot{p} \geq 0\big)\\ & \wedge \ldots\\ & \wedge \big(p = 0 \wedge \dot{p} = 0 \wedge \cdots \wedge \dot{p}^{(N-2)} = 0 \rightarrow \dot{p}^{(N-1)} \geq 0\big)\end{aligned} \tag{4}$$

$$\neg(\dot{p}^{(*)} > 0) \leftrightarrow (\dot{-p})^{(*)} \geq 0 \tag{5}$$

$$\neg(\dot{p}^{(*)} = 0) \leftrightarrow \dot{p}^{(*)} > 0 \vee (\dot{-p})^{(*)} > 0 \tag{6}$$

Proof. We prove the equivalences case by case, in order. We will use the following real arithmetic equivalences:

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

Note, also that Lie derivation is linear i.e. $(\dot{-p})^{(i)} = -(\dot{p}^{(i)})$ is provable in real arithmetic for any i.

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

$$p \geq 0 \wedge \Big((p = 0 \rightarrow \dot{p} \geq 0) \wedge \ldots\Big) \leftrightarrow$$
$$p > 0 \wedge \Big((p = 0 \rightarrow \dot{p} \geq 0) \wedge \ldots\Big) \vee$$
$$p = 0 \wedge \Big((p = 0 \rightarrow \dot{p} \geq 0) \wedge \ldots\Big)$$

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

$$\dot{p}^{(*)} > 0 \leftrightarrow p > 0 \vee p = 0 \wedge \Big(\dot{p} \geq 0 \wedge \ldots\Big)$$

The equivalence (3) follows by iterating this expansion for the conjuncts corresponding to higher Lie derivatives.

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

(5) This equivalence follows by negating both sides of the equivalence (3) and moving negations on the RHS inwards with propositional tautologies, yielding the provable equivalence:

$$\begin{aligned}\neg(\dot{p}^{(*)} > 0) \leftrightarrow \Big(& \neg(p > 0) \wedge (p = 0 \rightarrow \neg(\dot{p} > 0))\\ & \wedge \ldots\\ & \wedge \big(p{=}0 \wedge \dot{p}{=}0 \wedge \cdots \wedge \dot{p}^{(N-2)}{=}0 \rightarrow \neg(\dot{p}^{(N-1)}{>}0)\big)\Big)\end{aligned}$$

The desired equivalence proves by further rewriting the above RHS with real arithmetic and equivalence (4).

(6) By (5), we have the provable equivalence:

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

By rewriting with (4), the RHS of this equivalence is equivalent to the formula $\dot{p}^{(*)} = 0$ by real arithmetic. Negating both sides yields the provable equivalence (6). □

The equivalence (5) is particularly important, because it underlies the next proposition, from which all results about local progress will follow.

Proposition B.2. *Let P be in normal form:*

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

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

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

for which we additionally have the provable equivalence:

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

Proof. Throughout this proof, we will make use of the standard propositional tautologies:

$$\neg(A \land B) \leftrightarrow \neg A \lor \neg B$$
$$\neg(A \lor B) \leftrightarrow \neg A \land \neg B$$

We start by negating P (in normal form), and negating polynomials so that all inequalities have 0 on the RHS. We write ϕ for the resulting RHS:

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

The progress formula $\dot{P}^{(*)}$ for the normal form of P is:

$$\bigvee_{i=0}^{M} \Big(\bigwedge_{j=0}^{m(i)} \dot{p_{ij}}^{(*)} \geq 0 \land \bigwedge_{j=0}^{n(i)} \dot{q_{ij}}^{(*)} > 0 \Big)$$

Negating both sides of this progress formula for P proves:

$$\neg(\dot{P}^{(*)}) \leftrightarrow \bigwedge_{i=0}^{M} \Big(\bigvee_{j=0}^{m(i)} \neg(\dot{p_{ij}}^{(*)} \geq 0) \lor \bigvee_{j=0}^{n(i)} \neg(\dot{q_{ij}}^{(*)} > 0) \Big)$$

Rewriting the RHS with equivalence (5) from Proposition B.1 yields the following provable equivalence. We write ψ for the resulting RHS.

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

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

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

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

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

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

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

□

B.2 Local Progress

We first derive the properties about local progress stated in Section 6.1. These properties will be used in the completeness arguments for both algebraic and semialgebraic invariants.

B.2.1 Atomic Non-strict Inequalities

The $\mathrm{LPi}_{\geq}$ axiom derived in Section 6.1 has an implicit initial state assumption on the left of the implication for the $\circ$ modality:

$$\mathrm{LPi}_{\geq} \quad \begin{array}{l} x{=}y \land p \geq 0 \land \big(p = 0 \rightarrow \langle x' = f(x) \,\&\, \dot{p} \geq 0 \rangle \circ\big) \\ \rightarrow \langle x' = f(x) \,\&\, p \geq 0 \rangle \circ \end{array}$$

We start by completing the proof of Lemma 6.3 that was outlined in Section 6.1: we either iterate $\mathrm{LPi}_{\geq}$ until the first significant Lie derivative, or prove local progress in $p \geq 0$ using dRI immediately.

Proof of Lemma 6.3. We derive the following axiom:

$$\mathrm{LP}_{\geq^*} \quad x{=}y \land \dot{p}^{(*)} \geq 0 \rightarrow \langle x' = f(x) \,\&\, p \geq 0 \rangle \circ$$

Let N be the rank of p with respect to $x' = f(x)$. We unfold the definition of $\dot{p}^{(*)} \geq 0$ and handle both cases separately.

$$\dfrac{\scriptstyle\vee\mathrm{L}\;\dfrac{x{=}y, \dot{p}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, p \geq 0 \rangle \circ \quad x{=}y, \dot{p}^{(*)} = 0 \vdash \langle x' = f(x) \,\&\, p \geq 0 \rangle \circ}{x{=}y, \dot{p}^{(*)} > 0 \lor \dot{p}^{(*)} = 0 \vdash \langle x' = f(x) \,\&\, p \geq 0 \rangle \circ}}{x{=}y, \dot{p}^{(*)} \geq 0 \vdash \langle x' = f(x) \,\&\, p \geq 0 \rangle \circ}$$

The right premise by $\mathrm{DR}\langle\cdot\rangle$, because by dRI, $p = 0$ is invariant. The proof is completed with Cont using the trivial arithmetic fact $1 > 0$:

$$\scriptstyle\mathrm{DR}\langle\cdot\rangle\;\dfrac{\scriptstyle\mathrm{dRI}\;\dfrac{*}{\dot{p}^{(*)} = 0 \vdash [x' = f(x) \,\&\, 1 > 0] p = 0} \quad \scriptstyle\mathbb{R},\mathrm{Cont}\;\dfrac{*}{x{=}y \vdash \langle x' = f(x) \,\&\, 1 \geq 0 \rangle \circ}}{x{=}y, \dot{p}^{(*)} = 0 \vdash \langle x' = f(x) \,\&\, p \geq 0 \rangle \circ}$$

The left premise also closes, because it gathers all of the open premises obtained by iterating $\mathrm{LPi}_{\geq}$ for higher Lie derivatives. In this way, the derivation continues until we are left with the final open premise which is abbreviated here, and continued below.

$$\scriptstyle\mathrm{LPi}_{\geq}\;\dfrac{\scriptstyle\mathbb{R}\;\dfrac{*}{\dot{p}^{(*)} > 0 \vdash p \geq 0} \quad \scriptstyle\mathrm{LPi}_{\geq}\;\dfrac{\scriptstyle\mathbb{R}\;\dfrac{*}{\dot{p}^{(*)} > 0, p = 0 \vdash \dot{p} \geq 0} \quad \scriptstyle\mathrm{LPi}_{\geq}\;\dfrac{x{=}y, \dot{p}^{(*)} > 0, \ldots \vdash \ldots}{\ldots}}{x{=}y, \dot{p}^{(*)} > 0, p = 0 \vdash \langle x' = f(x) \,\&\, \dot{p} \geq 0 \rangle \circ}}{x{=}y, \dot{p}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, p \geq 0 \rangle \circ}$$

The open premise corresponds to the last conjunct of $\dot{p}^{(*)} > 0$. The implication in the conjunct is discharged with the gathered antecedents $p = 0, \ldots, \dot{p}^{(N-2)} = 0$.

$$\scriptstyle\mathrm{cut}\;\dfrac{\scriptstyle\mathrm{dRW}\langle\cdot\rangle\;\dfrac{\scriptstyle\mathrm{Cont}\;\dfrac{*}{x{=}y, \dot{p}^{(N-1)} > 0 \vdash \langle x' = f(x) \,\&\, \dot{p}^{(N-1)} > 0 \rangle \circ}}{x{=}y, \dot{p}^{(N-1)} > 0 \vdash \langle x' = f(x) \,\&\, \dot{p}^{(N-1)} \geq 0 \rangle \circ}}{x{=}y, \dot{p}^{(*)} > 0, p = 0, \ldots, \dot{p}^{(N-2)} = 0 \vdash \langle x' = f(x) \,\&\, \dot{p}^{(N-1)} \geq 0 \rangle \circ}$$

□

B.2.2 Atomic Strict Inequalities

Next, we prove Lemma 6.4. The essential idea is to reduce back to the non-strict case. We do so with the aid of the following proposition.

Proposition B.3. *Let $r = p^k$ for some $k \geq 1$, then $\dot{r}^{(i)} \in (p)$ for all $0 \leq i \leq k - 1$.*

Proof. We proceed by induction on k.

- For $k = 1$, we have $r = p^1$ so $\dot{r}^{(0)} = r \in (p)$ trivially.
- For $r = p^{k+1}$, we obtain an expression for the j-th Lie derivative of r by Leibniz's rule, where $0 \leq j \leq k$:

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

The induction hypothesis implies $(\dot{p^k})^{(j-i)} \in (p)$ for $1 \leq i \leq j$, and thus, each summand $\binom{j}{i} (\dot{p^k})^{(j-i)} \dot{p}^{(i)} \in (p)$ by Def. 3.1.

The final summand for $i = 0$ is:

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

Hence, $\dot{r}^{(j)} \in (p)$ as required. ∎

For $r = p^k, k \geq 1$, the formula $p = 0 \rightarrow \bigwedge_{i=0}^{k-1} \dot{r}^{(i)} = 0$, thus, is provable in real arithmetic. This enables a proof of Lemma 6.4.

Proof of Lemma 6.4. We derive the following axiom:

$$\mathrm{LP}_{>^*}\ x{=}y \land \dot{p}^{(*)} > 0 \rightarrow \langle x' = f(x) \,\&\, p > 0\rangle\bigcirc$$

Let N be the rank of p with respect to $x' = f(x)$. The rank bounds the number of higher Lie derivatives that we will need to consider. Recall $N \geq 1$ by (1).

We start by unfolding the syntactic abbreviation of the $\bigcirc$ modality, and observe that we can reduce to the non-strict case with dRW$\langle\cdot\rangle$ and the real arithmetic fact $p{-}r \geq 0 \rightarrow p > 0 \lor x = y$ for the abbreviation $r \overset{\text{def}}{\equiv} |x - y|^{2N}$, which is a polynomial term: $\big((x_1 - y_1)^2 + \cdots + (x_n - y_n)^2\big)^N$.

$$\dfrac{\dfrac{\dfrac{*}{p{-}r \geq 0 \vdash p > 0 \lor x = y}\,\mathbb{R} \qquad x{=}y,\, \dot{p}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, p{-}r \geq 0\rangle\circ}{x{=}y,\, \dot{p}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, p > 0 \lor x = y\rangle\circ}\,\mathrm{dRW}\langle\cdot\rangle}{x{=}y,\, \dot{p}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, p > 0\rangle\bigcirc}$$

Next, we make use of $x{=}y$ in the antecedents. The first cut proves because $x{=}y \rightarrow |x{-}y|^2 = 0$ is a provable formula of real arithmetic. As remarked, with $|x - y|^2 = 0$ and $N \geq 1$, by Proposition B.3, $|x - y|^2 = 0 \rightarrow \bigwedge_{i=0}^{N-1} \dot{r}^{(i)} = 0$ is a provable real arithmetic formula. The second cut proves using this fact. We call the resulting open premise ①.

$$\dfrac{\dfrac{x{=}y,\, \bigwedge_{i=0}^{N-1} \dot{r}^{(i)} = 0,\, \dot{p}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, p{-}r \geq 0\rangle\circ}{x{=}y,\, |x - y|^2 = 0,\, \dot{p}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, p{-}r \geq 0\rangle\circ}\,\mathrm{cut},\mathbb{R}}{x{=}y,\, \dot{p}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, p{-}r \geq 0\rangle\circ}\,\mathrm{cut},\mathbb{R}$$

To continue from ①, we observe for $0 \leq i \leq N - 1$,

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

Using the conjunction $\bigwedge_{i=0}^{N-1} \dot{r}^{(i)} = 0$ in the antecedents, the formula $(\dot{p{-}r})^{(i)} = \dot{p}^{(i)}$ proves by a cut and real arithmetic for $0 \leq i \leq N - 1$. This justifies the next real arithmetic step from ①, where we abbreviate $\Gamma_r \overset{\text{def}}{\equiv} \bigwedge_{i=0}^{N-1} (\dot{p{-}r})^{(i)} = \dot{p}^{(i)}$. Intuitively, Γ_r will allow us to locally consider higher Lie derivatives of p instead of higher Lie derivatives of $p - r$ in subsequent derivation steps.

$$\dfrac{\Gamma_r,\, x{=}y,\, \dot{p}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, p{-}r \geq 0\rangle\circ}{x{=}y,\, \bigwedge_{i=0}^{N-1} \dot{r}^{(i)} = 0,\, \dot{p}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, p{-}r \geq 0\rangle\circ}\,\mathrm{cut},\mathbb{R}$$

It remains for us to use the same technique of iterating LPi$_\geq$, as shown in the proof of Lemma 6.3. The following derivation starts with a single LPi$_\geq$ step. The left premise closes by real arithmetic because $\dot{p}^{(*)} > 0$ has the conjunct $p \geq 0$, and Γ_r provides $p - r = r$, which imply $p - r \geq 0$. The right premise is labeled ②:

$$\dfrac{\dfrac{*}{\Gamma_r,\, \dot{p}^{(*)} > 0 \vdash p{-}r \geq 0}\,\mathbb{R} \qquad ②}{\Gamma_r,\, x{=}y,\, \dot{p}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, p{-}r \geq 0\rangle\circ}\,\mathrm{LPi}_\geq$$

Continuing from ②, we now need to show local progress for the first Lie derivative of $p{-}r$. The first step simplifies formula $p{-}r = 0$ in the antecedents using Γ_r. We use LPi$_\geq$ again, use Γ_r to simplify and prove the left premise, abbreviating the right premise with ③.

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{p = 0 \rightarrow \dot{p} \geq 0,\, p = 0 \vdash \dot{p}^{(1)} \geq 0}\,\mathbb{R}}{\Gamma_r,\, \dot{p}^{(*)} > 0,\, p = 0 \vdash (\dot{p{-}r})^{(1)} \geq 0}\,\mathbb{R} \qquad ③}{\Gamma_r,\, x{=}y,\, \dot{p}^{(*)} > 0,\, p = 0 \vdash \langle x' = f(x) \,\&\, (\dot{p{-}r})^{(1)} \geq 0\rangle\circ}\,\mathrm{LPi}_\geq}{\Gamma_r,\, x{=}y,\, \dot{p}^{(*)} > 0,\, p{-}r = 0 \vdash \langle x' = f(x) \,\&\, (\dot{p{-}r})^{(1)} \geq 0\rangle\circ}\,\mathbb{R}$$

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

$$\dfrac{\dfrac{\dfrac{\Gamma_r,\, x{=}y,\, \dot{p}^{(*)}{>}0,\, p{=}0,\, \ldots,\, \dot{p}^{(N-2)}{=}0 \vdash \langle x' = f(x) \,\&\, (\dot{p{-}r})^{(N-1)} {\geq} 0\rangle\circ}{\cdots}\,\mathrm{LPi}_\geq}{\Gamma_r,\, x{=}y,\, \dot{p}^{(*)}{>}0,\, p = 0,\, \dot{p}^{(1)} \geq 0 \vdash \langle x' = f(x) \,\&\, (\dot{p{-}r})^{(2)} {\geq} 0\rangle\circ}\,\mathrm{LPi}_\geq}{\Gamma_r,\, x{=}y,\, \dot{p}^{(*)}{>}0,\, p{=}0,\, (\dot{p{-}r})^{(1)} \geq 0 \vdash \langle x' = f(x) \,\&\, (\dot{p{-}r})^{(2)} {\geq} 0\rangle\circ}\,\mathbb{R}$$

The gathered antecedents $p = 0, \ldots, \dot{p}^{(N-2)} = 0$ are respectively obtained from Γ_r by real arithmetic. The proof is closed with dRW$\langle\cdot\rangle$,Cont, similarly to Lemma 6.3.

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{x{=}y,\, (\dot{p{-}r})^{(N-1)}{>}0 \vdash \langle x' = f(x) \,\&\, (\dot{p{-}r})^{(N-1)} {>} 0\rangle\circ}\,\mathrm{Cont}}{\Gamma_r,\, x{=}y,\, \dot{p}^{(N-1)}{>}0 \vdash \langle x' = f(x) \,\&\, (\dot{p{-}r})^{(N-1)} {>} 0\rangle\circ}\,\mathrm{cut},\mathbb{R}}{\Gamma_r,\, x{=}y,\, \dot{p}^{(N-1)}{>}0 \vdash \langle x' = f(x) \,\&\, (\dot{p{-}r})^{(N-1)} {\geq} 0\rangle\circ}\,\mathrm{dRW}\langle\cdot\rangle}{\Gamma_r,\, x{=}y,\, \dot{p}^{(*)} > 0,\, p{=}0,\, ..,\, \dot{p}^{(N-2)}{=}0 \vdash \langle x' = f(x) \,\&\, (\dot{p{-}r})^{(N-1)} {\geq} 0\rangle\circ}\,\mathrm{cut}$$

∎

B.2.3 Semialgebraic Case

We now prove the main lemma for local progress.

Proof of Lemma 6.6. We derive the following axiom:

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

We assume that P is written in normal form (2). Throughout this proof, we will collapse similar premises in derivations and index them by i, j. We abbreviate the i-th disjunct of P with $P_i \overset{\text{def}}{\equiv} \bigwedge_{j=0}^{m(i)} p_{ij} \geq 0 \land \bigwedge_{j=0}^{n(i)} q_{ij} > 0$.

We start by splitting the outermost disjunction in $\dot{P}^{(*)}$ with $\lor$L. For each resulting premise (indexed by i), we select the corresponding disjunct of P to prove local progress. The domain change with dRW$\langle\cdot\rangle$ proves because $P_i \rightarrow P$ is a propositional tautology for each i.

$$\dfrac{\dfrac{x{=}y,\, \bigwedge_{j=0}^{m(i)} \dot{p_{ij}}^{(*)} \geq 0 \land \bigwedge_{j=0}^{n(i)} \dot{q_{ij}}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, P_i\rangle\bigcirc}{x{=}y,\, \bigwedge_{j=0}^{m(i)} \dot{p_{ij}}^{(*)} \geq 0 \land \bigwedge_{j=0}^{n(i)} \dot{q_{ij}}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, P\rangle\bigcirc}\,\mathrm{dRW}\langle\cdot\rangle}{x{=}y,\, \dot{P}^{(*)} \vdash \langle x' = f(x) \,\&\, P\rangle\bigcirc}\,\lor\mathrm{L}$$

Now, we only need to prove local progress in P_i. We make use of $\langle\&\land\rangle$ to split up the conjunct in P_i. This leaves premises (indexed by j) for the non-strict and strict inequalities of P_i respectively. These premises are abbreviated with ① and ② respectively.

$$\dfrac{① \qquad ②}{x{=}y,\, \bigwedge_{j=0}^{m(i)} \dot{p_{ij}}^{(*)} \geq 0 \land \bigwedge_{j=0}^{n(i)} \dot{q_{ij}}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, P_i\rangle\bigcirc}\,\langle\&\land\rangle,\land\mathrm{R}$$

For the non-strict inequalities (①), we use LP$_{\geq^*}$, after unfolding $\bigcirc$ and using dRW$\langle\cdot\rangle$, because $p_{ij} \geq 0 \rightarrow p_{ij} \geq 0 \lor x = y$ is a propositional tautology:

$$\dfrac{\dfrac{\dfrac{*}{x{=}y,\ \dot{p}_{ij}^{(*)} \geq 0 \vdash \langle x' = f(x)\,\&\,p_{ij} \geq 0\rangle\circ}\ \text{LP}_{\geq^*}}{x{=}y,\ \dot{p}_{ij}^{(*)} \geq 0 \vdash \langle x' = f(x)\,\&\,p_{ij} \geq 0 \lor x = y\rangle\circ}\ \text{dRW}\langle\cdot\rangle}{x{=}y,\ \dot{p}_{ij}^{(*)} \geq 0 \vdash \langle x' = f(x)\,\&\,p_{ij} \geq 0\rangle\bigcirc}$$

For the strict inequalities (②), we use $\text{LP}_{>^*}$ directly:

$$\dfrac{*}{x{=}y,\ \dot{p}_{ij}^{(*)} > 0 \vdash \langle x' = f(x)\,\&\,p_{ij} > 0\rangle\bigcirc}\ \text{LP}_{>^*}$$

Note that the $\bigcirc$ modality is not required for non-strict inequalities, but they are crucially used for the strict inequalities. ◻

Finally, we give a characterization of semialgebraic local progress.

Proof of Corollary 6.7. We derive the following axioms:

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

$$\neg\bigcirc\quad x{=}y \rightarrow \big(\langle x' = f(x)\,\&\,P\rangle\bigcirc \leftrightarrow \neg\langle x' = f(x)\,\&\,\neg P\rangle\bigcirc\big)$$

We assume that P is written in normal form (2). By Proposition B.2, there is a normal form for $\neg P$, i.e.,

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

where we additionally have the provable equivalence:

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

We first derive LP. The "$\leftarrow$" direction is LP$\mathbb{R}$. The proof for the "$\rightarrow$" direction (of the inner equivalence) starts by reducing to the contrapositive statement by logical manipulation. We then use the above normal form to rewrite the negation in the antecedents. By LP$\mathbb{R}$, we cut in the local progress formula for $\neg P$. We then move the negated succedent into the antecedents, and combine the two local progress antecedents with Uniq. This combines their respective domain constraints:

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

Observe that we now have $\neg P \land P$ in the domain constraints which is equivalent to *false*; but we cannot locally progress into an empty set of states. The proof is completed by unfolding the $\bigcirc$ syntactic abbreviation, and shifting to the box modality:

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{\neg P \land P \lor x = y \vdash x = y}\ \mathbb{R}}{\vdash [x' = f(x)\,\&\,\neg P \land P \lor x = y]x = y}\ \text{dW}}{\langle x' = f(x)\,\&\,\neg P \land P \lor x = y\rangle x \neq y \vdash \mathit{false}}\ \langle\cdot\rangle,\neg\text{L}}{\langle x' = f(x)\,\&\,\neg P \land P\rangle\bigcirc \vdash \mathit{false}}$$

The self-duality axiom $\neg\bigcirc$ derives from LP using the equivalence $\neg(\dot{P}^{(*)}) \leftrightarrow \dot{(\neg P)}^{(*)}$ from Proposition B.2. ◻

B.3 Algebraic Invariants

This section proves the completeness results for algebraic invariants. We first prove Liouville's formula which was used in Lemma 4.1 to derive vectorial Darboux from vectorial DG. We then complete the proof of dRI. This allows us to prove the completeness result and its corollary.

B.3.1 Liouville's Formula

We give an arithmetic proof of Liouville's formula, which holds for any derivation operator $(\cdot)'$, i.e., any operator satisfying the usual sum and product rules of differentiation. Derivation operators include Lie derivatives (which we will use Lemma B.4 for in the proof of Lemma 4.1), differentials, and time derivatives.

Lemma B.4 (Liouville). *Let the $n{\times}n$ matrix of polynomials A satisfy the equation $A' = BA$ for an $n \times n$ matrix B of cofactor polynomials. Then the following is a provable real arithmetic identity:*

$$(\det A)' = \operatorname{tr}(B) \det A$$

Proof. We consider the following expression for the determinant $\det A$, where $\sigma \in \operatorname{perm} n$ is a permutation on n indices and $\operatorname{sgn}(\sigma)$ denotes its sign:

$$\det(A) = \sum_{\sigma \in \operatorname{perm} n} (\operatorname{sgn}(\sigma) A_{1,\sigma_1} A_{2,\sigma_2} \dots A_{n,\sigma_n})$$

By the sum and product rules of derivation operators:

$$\begin{aligned}
(\det(A))' &= \sum_{\sigma \in \operatorname{perm} n} \operatorname{sgn}(\sigma)(A_{1,\sigma_1} A_{2,\sigma_2} \dots A_{n,\sigma_n})' \\
&= \sum_{\sigma \in \operatorname{perm} n} \operatorname{sgn}(\sigma) A'_{1,\sigma_1} A_{2,\sigma_2} \dots A_{n,\sigma_n} \\
&\quad + \sum_{\sigma \in \operatorname{perm} n} \operatorname{sgn}(\sigma) A_{1,\sigma_1} A'_{2,\sigma_2} \dots A_{n,\sigma_n} \\
&\quad + \cdots \\
&\quad + \sum_{\sigma \in \operatorname{perm} n} \operatorname{sgn}(\sigma) A_{1,\sigma_1} A_{2,\sigma_2} \dots A'_{n,\sigma_n}
\end{aligned}$$

Let us write:

$$A_{[i]'} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a'_{i1} & a'_{i2} & \dots & a'_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

Then

$$(\det(A))' = \sum_{i=1}^{n} \det(A_{[i]'})$$

Using $A' = BA$, and by row-reduction properties of determinants:

$$\begin{aligned}
\det(A_{[i]'}) &= \det \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{k=1}^{n} b_{ik} a_{k1} & \sum_{k=1}^{n} b_{ik} a_{k2} & \dots & \sum_{k=1}^{n} b_{ik} a_{kn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \\
&= \det \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{ii} a_{i1} & b_{ii} a_{i2} & \dots & b_{ii} a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \\
&= b_{ii} \det(A)
\end{aligned}$$

Therefore,

$$(\det(A))' = \sum_{i=1}^{n} b_{ii} \det(A) = \operatorname{tr}(B) \det(A)$$

◻

Lemma B.4 proves the arithmetic fact $(\det(Y))' = -\operatorname{tr}(G)\det(Y)$ used in the proof of Lemma 4.1 to derive rule vdbx. In that proof, $Y' = -YG$. Transposing yields $(Y^T)' = -G^T Y^T$, so:

$$(\det(Y))' = (\det(Y^T))' = -\operatorname{tr}(G^T)\det(Y^T) = -\operatorname{tr}(G)\det(Y)$$

B.3.2 Differential Radical Invariants

Next, we complete the derivation of rule dRI from derived rule vdbx. In this derivation, we use a DI$_=$ step which may be slightly unfamiliar since it differs from our usage in dI. Rewriting axiom DI$_=$ with [?], and abbreviating $R \stackrel{\text{def}}{\equiv} [x' = f(x) \,\&\, Q(x)](p(x))' = 0$ proves the following formula:

$$(Q \to R) \to \big([x' = f(x) \,\&\, Q]p = 0 \leftrightarrow (Q \to p = 0)\big)$$

Propositionally, if we only consider of the "$\leftarrow$" direction of the nested equivalence we have the provable formula:

$$(Q \to R) \to \big((Q \to p = 0) \to [x' = f(x) \,\&\, Q]p = 0\big)$$

Thus, the formula $\neg Q \to [x' = f(x) \,\&\, Q]p = 0$ proves propositionally from DI$_=$,[?], since $\neg Q$ implies both formulas on the left of the implication above. Intuitively, the formula states that if the domain constraint Q is false in an initial state, then the box modality in the conclusion is trivially true, because no trajectories stay in Q.

Therefore, as $Q \to [x' = f(x) \,\&\, Q]p = 0$ is propositionally equivalent to $\neg Q \vee [x' = f(x) \,\&\, Q]p = 0$ the following formula (which we use below) proves propositionally from DI$_=$,[?]:

$$(Q \to [x' = f(x) \,\&\, Q]p = 0) \to [x' = f(x) \,\&\, Q]p = 0$$

Proof of Theorem 4.2. Let p be a polynomial satisfying both premises of the dRI proof rule, and let $\mathbf{p}_i \stackrel{\text{def}}{=} \dot{p}^{(i-1)}$ for $i = 1, 2, \ldots, N$, i.e.

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

The component-wise Lie derivative of $\mathbf{p}$ is: $(\dot{\mathbf{p}})_i = \mathcal{L}_{f(x)}(\mathbf{p}_i) = \dot{p}^{(i)}$.

We start by setting up for a proof by vdbx. In the first step, we used DI$_=$,[?] to assume Q is true initially (see above). On the left premise after the cut, arithmetic equivalence $\bigwedge_{i=0}^{N-1} \dot{p}^{(i)} = 0 \leftrightarrow \mathbf{p} = 0$ is used to rewrite the succedent to the left premise of dRI.

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

The right premise continues by vdbx with the following choice of G, with 1 on its superdiagonal, and g_i cofactors in the last row:

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

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 $1 \le i \le N$. For $i < N$, explicit matrix multiplication yields:

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

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, real arithmetic equivalently reduces the remaining open premise to the right premise of dRI. ◻

B.3.3 Completeness for Algebraic Invariants

We now derive axiom DRI, which makes use of LP$\mathbb{R}$ from Lemma 6.6 and Cont^{O} from Corollary A.15.

Proof of Theorem 4.4. In the "$\leftarrow$" direction, we use dRI, by setting N to the rank 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 rank of p, it must, by definition satisfy the rank identity (1).

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

For the "$\to$" direction, we first reduce to the contrapositive statement by logical manipulation. An application of $\langle\cdot\rangle$ axiom turns the negated box modality in the succedent to a diamond modality. By (6) from Proposition B.1, we equivalently rewrite the negated differential radical formula in the antecedents to two progress formulas. We cut the first-order formula $\exists y\, x{=}y$ which proves trivially in real arithmetic to get an initial state assumption. Finally, we use Cont^{O} to cut local progress for Q because, by assumption, Q characterizes an open semialgebraic set. Splitting with $\vee$L yields two premises, which we label ① and ②.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{① \qquad ②}{x{=}y,\ \langle x' = f(x) \,\&\, Q\rangle\circ,\ \dot{p}^{(*)} > 0 \vee \dot{(-p)}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}\,\vee\mathrm{L}}{x{=}y,\ Q,\ \dot{p}^{(*)} > 0 \vee \dot{(-p)}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}\,\mathrm{cut,Cont}^{O}}{\exists y\, x{=}y,\ Q,\ \dot{p}^{(*)} > 0 \vee \dot{(-p)}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}\,\exists\mathrm{L}}{Q,\ \dot{p}^{(*)} > 0 \vee \dot{(-p)}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}\,\mathrm{cut}}{Q,\ \neg(\dot{p}^{(*)} = 0) \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}\,\mathbb{R}}{Q,\ \neg\langle x' = f(x) \,\&\, Q\rangle\neg p = 0 \vdash \dot{p}^{(*)} = 0}\,\neg\mathrm{L},\neg\mathrm{R}}{[x' = f(x) \,\&\, Q]p = 0 \vdash Q \to \dot{p}^{(*)} = 0}\,\to\mathrm{R},\langle\cdot\rangle$$

Continuing on ①, because we already have $\dot{p}^{(*)} > 0$ in the antecedents, LP$_{>^*}$ derives $\langle x' = f(x) \,\&\, p > 0\rangle\bigcirc$. Unfolding the $\bigcirc$ abbreviation, an application of $\langle\&\wedge\rangle$ allows us to combine the two local progress formulas in the antecedent.

$$\dfrac{\dfrac{\langle x' = f(x) \,\&\, Q \wedge (p > 0 \vee x = y)\rangle\circ \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}{\langle x' = f(x) \,\&\, Q\rangle\circ,\ \langle x' = f(x) \,\&\, p > 0\rangle\bigcirc \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}\,\langle\&\wedge\rangle}{x{=}y,\ \langle x' = f(x) \,\&\, Q\rangle\circ,\ \dot{p}^{(*)} > 0 \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}\,\mathrm{cut,LP}_{>^*}$$

We continue by removing the syntactic abbreviation for $\circ$. Since $\overbrace{Q \wedge (p > 0 \vee x = y)}^{R} \to Q$ is a propositional tautology, we use dRW$\langle\cdot\rangle$ to strengthen the evolution domain constraint in the succedent. This allows us to use Kripke axiom K$\langle\cdot\rangle$ which reduces our succedent to the box modality. We finish the proof with a dW step, because the formula $p > 0 \lor x = y$ in the domain constraint R implies the succedent by real arithmetic.

$$
{\scriptstyle \mathrm{dRW}\langle\cdot\rangle}\dfrac{{\scriptstyle \mathrm{K}\langle\cdot\rangle}\dfrac{{\scriptstyle \mathrm{dW}}\dfrac{{\scriptstyle \mathbb{R}}\dfrac{*}{R \vdash (x \neq y \rightarrow p \neq 0)}}{\vdash [x' = f(x) \,\&\, R](x \neq y \rightarrow p \neq 0)}}{\langle x' = f(x) \,\&\, R\rangle x \neq y \vdash \langle x' = f(x) \,\&\, R\rangle p \neq 0}}{\dfrac{\langle x' = f(x) \,\&\, R\rangle x \neq y \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}{x{=}y,\ \langle x' = f(x) \,\&\, R\rangle \circ \vdash \langle x' = f(x) \,\&\, Q\rangle p \neq 0}}
$$

The remaining premise ② follows similarly, except that the progress formula $(\dot{-p})^{(*)} > 0$ enables the cut $\langle x' = f(x) \,\&\, -p > 0\rangle \bigcirc$. 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. We shall consider the fragment of dL programs generated by the following grammar, where $\tilde{Q}$ denotes a first-order formula of real arithmetic that characterizes the *complement* of a real algebraic variety, or equivalently, a formula of the form $r \neq 0$ where r is a polynomial:

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

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, by real arithmetic, assume that it is written in this form. Similarly, we shall, by real arithmetic, assume that $\tilde{Q}$ already has the form $r \neq 0$.

We proceed by structural induction on the form of α following [12, Theorem 1], and show that for some (computable) polynomial q, we can derive the equivalence $[\alpha]p = 0 \leftrightarrow q = 0$ in dL.

- Case $x' = f(x) \,\&\, r \neq 0$. The set of states characterized by $r \neq 0$ is open. Thus, Theorem 4.4 derives the equivalence $[x' = f(x) \,\&\, r \neq 0]p = 0 \leftrightarrow (r \neq 0 \rightarrow \dot{p}^{(*)} = 0)$. Let N be the rank of p so that $\dot{p}^{(*)} = 0$ expands to $\bigwedge_{i=0}^{N-1} \dot{p}^{(i)} = 0$. Let $q \stackrel{\text{def}}{=} r(\sum_{i=0}^{N-1} (\dot{p}^{(i)})^2)$, giving the provable real arithmetic equivalence $(r \neq 0 \rightarrow \dot{p}^{(*)} = 0) \leftrightarrow q = 0$. Rewriting with this derives the equivalence,
$$[x' = f(x) \,\&\, r \neq 0]p = 0 \leftrightarrow q = 0$$
- Case $x := e$. By axiom [:=], $[x := e]p(x) = 0 \leftrightarrow p(e) = 0$. As a composition of polynomials, $p(e)$ is a polynomial.
- Case $?r \neq 0$. By axiom [?], $[?r \neq 0]p = 0 \leftrightarrow (r \neq 0 \rightarrow p = 0)$. Let $q \stackrel{\text{def}}{=} rp$, giving the provable real arithmetic equivalence $(r \neq 0 \rightarrow p = 0) \leftrightarrow q = 0$. Rewriting with this derived equivalence yields the derived equivalence:
$$[?r \neq 0]p = 0 \leftrightarrow q = 0$$
- Case $\alpha \cup \beta$. By [∪], $[\alpha \cup \beta]p = 0 \leftrightarrow [\alpha]p = 0 \land [\beta]p = 0$. By the induction hypothesis on α, β, we may derive $[\alpha]p = 0 \leftrightarrow q_1 = 0$ and $[\beta]p = 0 \leftrightarrow q_2 = 0$ 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 provable formula of real arithmetic. Rewriting with the derived equivalences yields the derived equivalence:
$$[\alpha \cup \beta]p = 0 \leftrightarrow q_1^2 + q_2^2 = 0$$
- Case $\alpha;\beta$. By [;], $[\alpha;\beta]p = 0 \leftrightarrow [\alpha][\beta]p = 0$. By the induction hypothesis on β, we derive $[\beta]p = 0 \leftrightarrow q_2 = 0$. By rewriting with this equivalence, we derive $[\alpha;\beta]p = 0 \leftrightarrow [\alpha]q_2 = 0$. Now, by the induction hypothesis on α, we derive $[\alpha]q_2 = 0 \leftrightarrow q_1 = 0$ for some q_1. Rewriting with the derived equivalences yields the derived equivalence:
$$[\alpha;\beta]p = 0 \leftrightarrow q_1 = 0$$
- 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, i.e., every ascending chain of ideals is finite. We first construct the following sequence of polynomials q_i:
$$q_0 \stackrel{\text{def}}{=} p, \quad q_{i+1} \stackrel{\text{def}}{=} f_i$$
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:
$$(q_0) \subset (q_0, q_1) \subset (q_0, q_1, q_2) \subset \ldots$$
Thus, there is some smallest k such that q_k satisfies the following polynomial identity, with polynomial cofactors g_i:
$$q_k = \sum_{i=0}^{k-1} g_i q_i \tag{7}$$
We claim that $\bigwedge_{i=0}^{k-1} q_i = 0 \leftrightarrow [\alpha^*]p = 0$ is derivable. Since the following real arithmetic equivalence is provable $\sum_{i=0}^{k-1} q_i^2 = 0 \leftrightarrow \bigwedge_{i=0}^{k-1} q_i = 0$, 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.

"←" This direction is straightforward using k times the iteration axiom [*] together with [·]∧. By construction, we may successively replace $[\alpha]q_i$ with q_{i+1}, which gives us the required implication.

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

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

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

The conjuncts for $0 \leq i < k-1$ close trivially because $q_{i+1} = 0$ is in the antecedent. The last conjunct for $i = k-1$ is $q_k = 0$, which follows from the antecedent using (7). ◻

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

The following generalized version of sAI for Theorem 6.8, which also handles the evolution domain constraints derives, from rI&,LP.

Theorem B.5 (Semialgebraic invariants for Theorem 6.8 with semialgebraic domain constraints)**.** *For semialgebraic Q, P, with progress formulas $\dot{Q}^{(*)}, \dot{P}^{(*)}, \dot{Q}^{-(*)}, \dot{(\neg P)}^{-(*)}$ w.r.t. their respective normal forms* (2)*, this rule derives from the* dL *calculus with RI&,Dadj,Cont,Uniq.*

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

Proof. Rule sAI& derives directly from rule rI& derived in Corollary A.13, Corollary A.14, and the characterization of semialgebraic local progress LP from Corollary 6.7. The $x{=}y$ assumptions provided by rI& are used to convert between the local progress modalities and the semialgebraic progress formulas by LP, but they do not need to remain in the premises of sAI& (by weakening). ◻

Recalling our earlier discussion for rule rI&, we may again use V to keep any additional context assumptions that do not depend on variables x for the ODEs $x' = f(x)$ in rule sAI&, because it immediately derives from rI&, which supports constant contexts.

We now prove a syntactic completeness theorem for sAI&, from which Theorem 6.9 follows as a special case (where $Q \equiv \mathit{true}$).

Theorem B.6 (Semialgebraic invariant completeness for Theorem 6.9 with semialgebraic domains)**.** *For semialgebraic Q, P, with progress formulas $\dot{Q}^{(*)}, \dot{P}^{(*)}, \dot{Q}^{-(*)}, \dot{(\neg P)}^{-(*)}$ w.r.t. their respective normal forms* (2)*, this axiom derives in* dL *with RI&,Dadj,Cont,Uniq.*

$$\text{SAI\&}\quad \begin{array}{l} \forall x\,(P \to [x' = f(x)\,\&\,Q]P) \\ \leftrightarrow \forall x\,\big(P \land Q \land \dot{Q}^{(*)} \to \dot{P}^{(*)}\big) \land \forall x\,\big(\neg P \land Q \land \dot{Q}^{-(*)} \to \dot{(\neg P)}^{-(*)}\big) \end{array}$$

In particular, the dL *calculus is complete for invariance properties of the following form with semialgebraic formulas P, Q:*

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

Proof. We abbreviate the left and right conjunct on the RHS of SAI& as ⓐ and ⓑ, respectively.

The "←" direction derives directly by an application of sAI&. The antecedents ⓐ and ⓑ are first-order formulas of real arithmetic which are quantified over x, the variables evolved by the ODE $x' = f(x)$. They may, therefore, be kept as constant context in the antecedents of the premises when applying rule sAI&.

$$\begin{array}{rc} & \text{∀L,→L}\dfrac{*}{ⓐ, P, Q, \dot{Q}^{(*)} \vdash \dot{P}^{(*)}} \qquad \text{∀L,→L}\dfrac{*}{ⓑ, \neg P, Q, \dot{Q}^{-(*)} \vdash \dot{(\neg P)}^{-(*)}} \\ \hline \text{sAI\&} & ⓐ, ⓑ, P \vdash [x' = f(x)\,\&\,Q]P \\ \hline \to\text{R} & ⓐ, ⓑ \vdash (P \to [x' = f(x)\,\&\,Q]P) \\ \hline \forall\text{R} & ⓐ, ⓑ \vdash \forall x\,(P \to [x' = f(x)\,\&\,Q]P) \end{array}$$

In the "→" direction, we show the contrapositive statement in both cases. For ⓑ, we use the derived invariant reflection axiom (reflect) to turn the invariance assumption for the forwards ODE to an invariance assumption for the backwards ODE. The open premises with ⓐ and ⓑ in the succedent are labeled ① and ② respectively.

$$\wedge\text{R}\ \dfrac{\forall x\,(P \to [x' = f(x)\,\&\,Q]P) \vdash ⓐ \qquad \text{reflect}\dfrac{\forall x\,(\neg P \to [x' = -f(x)\,\&\,Q]\neg P) \vdash ⓑ}{\forall x\,(P \to [x' = f(x)\,\&\,Q]P) \vdash ⓑ}}{\forall x\,(P \to [x' = f(x)\,\&\,Q]P) \vdash ⓐ \land ⓑ}$$

Continuing on ①, we expand ⓐ and dualize on both sides of the sequent. We choose x as our witness for the (then) existentially quantified succedent. The $\mathbb{R}$ two steps respectively introduce an initial state assumption, and replace $\neg(\dot{P}^{(*)})$ with $\dot{(\neg P)}^{(*)}$, by Proposition B.2. We continue by cutting in local progress for Q and $\neg P$ respectively in steps ③, ④. The open premise after both cuts is labeled ⑤. All three steps are continued below.

$$\begin{array}{rc} & ③ \qquad ④ \quad ⑤ \\ \hline \text{cut} & x{=}y, P, Q, \dot{Q}^{(*)}, \dot{(\neg P)}^{(*)} \vdash \langle x' = f(x)\,\&\,Q\rangle\neg P \\ \hline \mathbb{R} & x{=}y, P, Q, \dot{Q}^{(*)}, \neg(\dot{P}^{(*)}) \vdash \langle x' = f(x)\,\&\,Q\rangle\neg P \\ \hline \exists\text{L} & \exists y\, x{=}y, P, Q, \dot{Q}^{(*)}, \neg(\dot{P}^{(*)}) \vdash \langle x' = f(x)\,\&\,Q\rangle\neg P \\ \hline \text{cut} & P, Q, \dot{Q}^{(*)}, \neg(\dot{P}^{(*)}) \vdash \langle x' = f(x)\,\&\,Q\rangle\neg P \\ \hline \exists\text{R},\wedge\text{R} & P, Q, \dot{Q}^{(*)}, \neg(\dot{P}^{(*)}) \vdash \exists x\,(P \land \langle x' = f(x)\,\&\,Q\rangle\neg P) \\ \hline \exists\text{L} & \exists x\,\big(P \land Q \land \dot{Q}^{(*)} \land \neg(\dot{P}^{(*)})\big) \vdash \exists x\,(P \land \langle x' = f(x)\,\&\,Q\rangle\neg P) \\ \hline \langle\cdot\rangle,\neg\text{L},\neg\text{R} & \forall x\,(P \to [x' = f(x)\,\&\,Q]P) \vdash \forall x\,\big(P \land Q \land \dot{Q}^{(*)} \to \dot{P}^{(*)}\big) \end{array}$$

The proofs in ③, ④ are similar and they prove local progress conditions within Q and $\neg P$ from $\dot{Q}^{(*)}, \dot{(\neg P)}^{(*)}$ respectively. On ③, the first step uses Init to weaken to the $\bigcirc$ modality since we have $x{=}y$ and P in the antecedents, and y is constant along the ODE $x' = f(x)$. The proof for ③ completes with LP$\mathbb{R}$.

$$\begin{array}{rc} & * \\ \hline \text{LP}\mathbb{R} & x{=}y, Q, \dot{Q}^{(*)} \vdash \langle x' = f(x)\,\&\,Q\rangle\bigcirc \\ \hline \text{Init} & x{=}y, Q, \dot{Q}^{(*)} \vdash \langle x' = f(x)\,\&\,Q\rangle\circ \end{array}$$

The proof for ④ uses LP$\mathbb{R}$ directly.

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

The proof completes on ⑤ by unfolding the $\circ$ and $\bigcirc$ modalities and combining the two local progress modalities in the antecedents using $\langle\&\wedge\rangle$. A K$\langle\cdot\rangle$,dW step allows us to turn the postcondition of the diamond modality in the antecedent to $\neg P$ because at the endpoint where $x \neq y$ is satisfied the domain constraint must still be true which implies that $\neg P$ is true at that endpoint. Formally, the dW step proves with the tautology $Q \land (\neg P \lor x{=}y) \to x \neq y \to \neg P$. A dRW$\langle\cdot\rangle$ step completes the proof.

$$\begin{array}{rr} & * \\ \hline \wedge\text{L} & Q \land (\neg P \lor x{=}y) \vdash Q \\ \hline \text{dRW}\langle\cdot\rangle & \langle x' = f(x)\,\&\,Q \land (\neg P \lor x{=}y)\rangle\neg P \vdash \langle x' = f(x)\,\&\,Q\rangle\neg P \\ \hline \text{K}\langle\cdot\rangle,\text{dW} & \langle x' = f(x)\,\&\,Q \land (\neg P \lor x{=}y)\rangle x \neq y \vdash \langle x' = f(x)\,\&\,Q\rangle\neg P \\ \hline \langle\&\wedge\rangle & \langle x' = f(x)\,\&\,Q\rangle x \neq y, \langle x' = f(x)\,\&\,\neg P \lor x{=}y\rangle x \neq y \vdash \langle x' = f(x)\,\&\,Q\rangle\neg P \\ \hline & \langle x' = f(x)\,\&\,Q\rangle\circ, \langle x' = f(x)\,\&\,\neg P\rangle\bigcirc \vdash \langle x' = f(x)\,\&\,Q\rangle\neg P \end{array}$$

The remaining derivation from ② (with succedent ⓑ) is similar using local progress for the backwards differential equations instead.

For an invariance property $\forall x\,(P \to [x' = f(x)\,\&\,Q]P)$, we may, without loss of generality, assume that P, Q (and $\neg P, \neg Q$) are equivalently rewritten into appropriate normal forms when necessary with an application of rule $\mathbb{R}$. Therefore, by SAI&, the dL calculus reduces all such invariance questions to a first-order formula of real arithmetic which is decidable. ◻