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, 10 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 a companion report [15].

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 [15] 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.

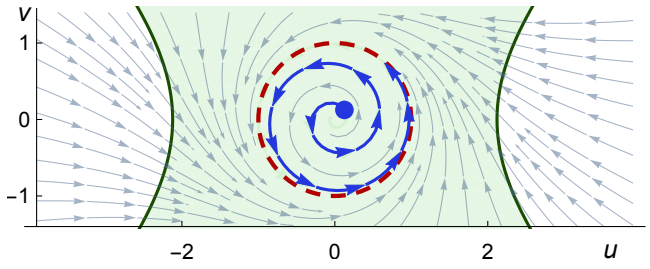

Figure 1. The red dashed circle $u^2 + v^2 = 1$ is approached by solutions of α_e from all points except the origin, e.g., the blue trajectory from $(\frac{1}{8}, \frac{1}{8})$ spirals towards the circle. The circle, green region $u^2 \leq v^2 + \frac{9}{2}$, and the origin are invariants of the system.

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 $x' = f(x) \,\&\, true$. We use a running example (Fig. 1):

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

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 $\omega : \mathbb{V} \to \mathbb{R}$ 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 $\varphi : [0, T] \to \mathbb{R}^n$ 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 $u^2 \le v^2 + \frac{9}{2}$ 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 $\frac{\mathrm{d}}{\mathrm{d}t}$ of the value of e [14, Lem. 35].

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

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

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.

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

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 [15].

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*:*

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

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

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

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

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

Differential invariants (dI) 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 (dI$_=$,dI$_{\succcurlyeq}$) of the more general dI rule [14] that will be used here. They internalize the mean value theorem[4] [15]. 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 dI$_=$,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 [·]$\wedge$ allows us to prove conjunctive postconditions separately, e.g., dI$_=$ derives from dI$_{\succcurlyeq}$ using [·]$\wedge$ with the equivalence $p = 0 \leftrightarrow p \ge 0 \wedge -p \ge 0$.

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. The main soundness restriction of dG is that the new ODE must be

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

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, 19, §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 $p = 0$. In our derivations below, we show that these Darboux invariance properties can be proved purely syntactically using dG.

[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.

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.

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

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 $y > 0 \wedge py \succcurlyeq 0$, 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:

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

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 $z' = \frac{g}{2}z$:

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

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 $p = 0 \leftrightarrow p \geq 0 \wedge -p \geq 0$ and derived axiom $[\cdot]\wedge$:

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

□

Example 3.3 (Proving continuous properties in dL)**.** In the running example, dbx$\succcurlyeq$ directly proves that the open disk $1 - u^2 - v^2 > 0$ is an invariant for α_e using cofactor $g = -\frac{1}{2}(u^2 + v^2)$:

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

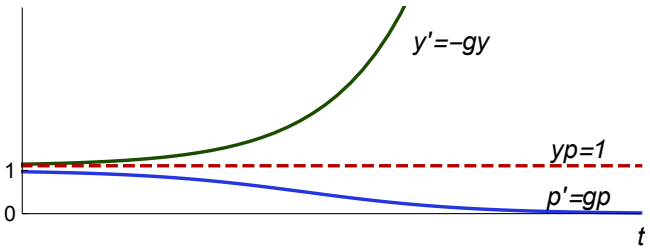

Figure 2. The differential ghost $y' = -gy$ (in green) balances out $p' = gp$ (in blue) so that the value of yp (the red dashed line) remains constant at 1. The horizontal axis tracks the evolution of time t.

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$\gtrcurlyeq$ 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$\gtrcurlyeq$, 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$\gtrcurlyeq$ 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:

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

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).*

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

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

First, we develop a proof that we will have occasion to use repeatedly. This proof adds an n-dimensional vectorial ghost $\mathbf{y}' = -G^T\mathbf{y}$ 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.

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

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$\gtrcurlyeq$. 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:

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

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:

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

[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.

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 [19, §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 [15]. Thus, $\det(Y)$ is a Darboux polynomial over the variables y_{ij}, with polynomial cofactor $-\operatorname{tr}(G)$:

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

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.

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

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

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

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.

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).*

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

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

Proof Summary [15]. Rule dRI derives from rule vdbx with:

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

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:*

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

Proof Summary [15]. 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 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 "→" direction (completeness) of DRI. Hence, the base dL axiomatization with differential ghosts is complete for proving properties of the form $[x' = f(x) \,\&\, Q]p = 0$ because dRI reduces all such questions to $Q \rightarrow \dot{p}^{(*)} = 0$, which is a formula of real arithmetic, and hence, decidable. The same applies for our next result, which is a corollary of Theorem 4.4, but applies beyond the continuous fragment of dL.

[9] 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.

Corollary 4.5 (Decidability). *For algebraic formulas P and hybrid programs α whose tests and domain constraints are negations of algebraic formulas [15], it is possible to compute a polynomial q such that the equivalence $[\alpha]P \leftrightarrow q = 0$ is derivable in* dL.

Proof Summary [15]. 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 [19, §10.VI] guarantees that for any initial state $\omega \in \mathbb{R}^n$, a *unique* solution of the system $x' = f(x)$, i.e., $\varphi : [0, T] \to \mathbb{R}^n$ with $\varphi(0) = \omega$, *exists* for some duration $T > 0$. The solution φ can be extended (uniquely) to its maximal open interval of existence [19, §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).*

Uniq $\big(\langle x' = f(x) \,\&\, Q_1\rangle P_1\big) \wedge \big(\langle x' = f(x) \,\&\, Q_2\rangle P_2\big) \to \langle x' = f(x) \,\&\, Q_1 \wedge Q_2\rangle(P_1 \vee P_2)$

Cont $x = y \to \big(p > 0 \to \langle x' = f(x) \,\&\, p > 0\rangle x \neq y\big)$

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

Proof Summary [15]. 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 $Q_1 \wedge Q_2$ and satisfies $P_1 \vee P_2$ 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.

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.

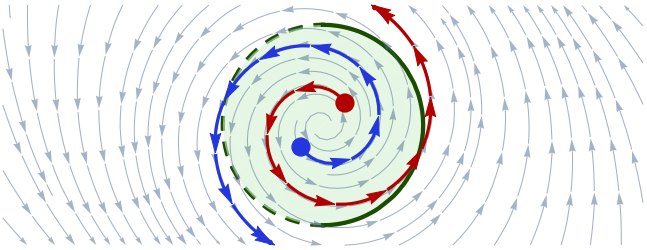

Figure 3. The half-open disk $u^2+v^2 < \frac{1}{4} \vee u^2+v^2 = \frac{1}{4} \wedge u \geq 0$ is not invariant for α_e because the red and blue trajectories spiral out of it towards the unit circle at a closed or open boundary, respectively.

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

DR$\langle\cdot\rangle$ $[x' = f(x) \,\&\, R]Q \to \big(\langle x' = f(x) \,\&\, R\rangle P \to \langle x' = f(x) \,\&\, Q\rangle P\big)$

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

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 the report [15].

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

RI $[x' = f(x)]P \leftrightarrow \forall y\, [x' = f(x) \,\&\, P \vee x = y]\big(x = y \to P \wedge \langle x' = f(x) \,\&\, P\rangle x \neq y\big)$

Proof Summary [15]. The RI axiom follows from the real induction principle [3] and the Picard-Lindelöf theorem [19, §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 $\forall y\, [\ldots]\big(x = y \to \ldots\big)$ 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):

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

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

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 $\varphi : [0,T] \to \mathbb{R}^n$ 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:

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

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

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

Proof Summary [15]. 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}:

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

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.

[11] We provide the case of arbitrary semialgebraic evolution domain Q in [15].

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.

$$\text{LPi}_{\geq}\ p \geq 0 \wedge \big(p = 0 \to \langle x' = f(x)\,\&\,\dot p \geq 0\rangle\circ\big) \to \langle x' = f(x)\,\&\,p \geq 0\rangle\circ$$

Proof. The proof starts with a case split since $p \geq 0$ is equivalent to $p > 0 \vee p = 0$. 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.

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

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

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

□

Observe that 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:

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

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 $\dot p^{(k)} > 0$:

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

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

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

We define $\dot p^{(*)} \geq 0$ as $\dot p^{(*)} > 0 \vee \dot p^{(*)} = 0$. 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 ≥). *This axiom derives from LPi$_{\geq}$:*

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

Proof Summary [15]. 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 ◯ and ∘ were equivalent, we now exploit the ◯ 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$_{\geq}$:*

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

Proof Summary [15]. We start by unfolding the syntactic abbreviation of the ◯ modality, and observing that we can reduce to the non-strict case with dRW$\langle\cdot\rangle$ and the real arithmetic fact[12] $p \geq |x-y|^{2N} \rightarrow p > 0 \vee x = y$, 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 [15].

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

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

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:

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

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.*

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

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

Proof Summary [15]. 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,[·]∧ 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 ◯, recalling that the ◯ 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.*

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

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

Proof Summary [15]. 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 ◯ 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.*

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

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.*

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

In [15], 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 [19], 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, 17].

Proof Rules for Invariants. There are numerous useful but incomplete proof rules for ODE invariants [16–18]. 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] André Platzer and Yong Kiam Tan. 2018. Differential Equation Axiomatization: The Impressive Power of Differential Ghosts. *CoRR* abs/1802.01226 (2018).
[16] 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.
[17] Sriram Sankaranarayanan, Henny B. Sipma, and Zohar Manna. 2008. Constructing invariants for hybrid systems. *Form. Methods Syst. Des.* 32, 1 (2008), 25–55.
[18] 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.
[19] Wolfgang Walter. 1998. *Ordinary Differential Equations.* Springer.