How to Prove "All" Differential Equation Properties

André Platzer **Yong Kiam Tan**

August 2017
CMU-CS-17-117

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work supported by the National Science Foundation under NSF CAREER Award CNS-1054246. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. The second author was supported by an A*STAR National Science Scholarship (PhD), Singapore.

Keywords: differential dynamic logic; algebraic and semialgebraic invariants

Abstract

This report shows that differential ghosts prove all algebraic invariants of algebraic differential equations by proving that differential radical invariants derive from differential ghosts. Differential ghosts add differential equations to a differential equation system, which, if cleverly chosen, simplify proofs, because they make it possible to relate the change in the quantities of interest to additional variables that can be chosen to evolve freely. A fractional generalization of Darboux's principle for proving invariance of (polynomial) equations along polynomial differential equations is shown to derive from differential ghosts. Differential adjoints are identified as the missing link to derive a vectorial formulation of Darboux's principle from vectorial differential ghosts, from which differential radical invariants follow. These ideas are subsequently generalized from equalities to inequalities, ultimately covering proofs of all true semialgebraic invariants.

1 Introduction

Hybrid systems combine both discrete and continuous dynamics. They may be used, for example, to model cyber-physical systems with discrete software controls and physical components that evolve along their continuous dynamics. Hence, methods used for the verification of hybrid systems must suitably handle both the discrete and continuous dynamics, as well as the intricate interactions between both dynamics. Differential Dynamic Logic (dL) [Pla08, Pla12b, Pla17a] is a logic for deductive reasoning about such systems, where the continuous dynamics are specified using a system of ordinary differential equations (ODEs). In fact, differential dynamic logic is complete relative to differential equations, so its calculus reduces all valid properties of hybrid systems to corresponding sub-questions about differential equations [Pla08, Pla12a, Pla17a]. This yields the question of how to best prove the remaining properties of differential equations.

One way to handle ODEs axiomatically is to introduce rules that replace them with their corresponding solutions [Pla08]. For example, the differential solution axiom for dL allows one to axiomatically replace a (constant) differential equation with its solution [Pla17a], which generalizes to any differential equation solvable in polynomial real arithmetic. However, such methods are not scalable for two reasons. Firstly, most differential equation systems do not have closed-form solutions. Secondly, even if solutions exist, they quickly involve undecidable real arithmetic [Ric69], making them difficult to reason about in a deductive proof.

An alternative approach is to reason about invariant sets of the differential equations [Bla99, Pla12b]. Informally, (positively) invariant sets are subsets of the state space from which the dynamics of the ODE under consideration cannot escape. Hence, if we start in such a set, then we are guaranteed to stay within the set no matter how long we follow the dynamics of the ODE system. The axiomatization of dL includes sound reasoning principles for proving invariance of formulas of first-order real arithmetic [Pla10, Pla12b, Pla17a]. However, it was not previously known if the existing axiomatization is complete, i.e. we can prove all true invariants of the ODEs under consideration.[1]

In this report, we investigate a proof rule for algebraic invariants DRI [GP14] and one for semialgebraic invariants LZZ [LZZ11]. Along the way, we identify three axioms internalizing the uniqueness, continuity and analyticity of solutions to systems of ODEs with polynomial right-hand sides.

We show that any instance of either proof rule can be soundly derived using these additional axioms together with a standard axiomatization of dL. In fact, most of the steps in our derivations make use of standard dL axioms, such as DI,DC,DG. Furthermore, both DRI and LZZ are complete for their respective types of invariants [GP14, LZZ11], which implies that our extended axiomatization is sound and complete for all invariants that are first-order formulas of real arithmetic.

In sharp contrast to previous approaches, the axioms we need can be stated as concrete formulas, rather than complex axiom schemata. Indeed, we shall see that both DRI and especially the LZZ proof rules require very complex side conditions governing when they can be applied. This

[1] A notable exception is the complete axiomatization of dL relative to discrete dynamics [Pla12a], which proves that valid properties of hybrid systems and differential equations reduce to discrete questions. Here we ask the complementary pragmatic question whether dL's differential equation axioms alone are sufficient.

advantage makes our axiomatization amenable to implementation in a theorem prover for hybrid systems, such as KeYmaera X [FMQ+15] which is built from a small axiomatic core based around uniform substitution [Pla17a], implementable in around 1,700 lines of code. Having a small soundness critical core minimizes the chance of implementation errors, and also allows for independent code inspection. Both of these are key to increasing trust in the correctness of the resulting proofs.

2 Related Work

Proof Rules for Invariants. An overview of proof rules for the invariance of algebraic and semi-algebraic sets can be found in [GSP17]. The soundness and completeness theorems for DRI,LZZ are shown in [GP14] and [LZZ11] respectively. An alternative derivation of DRI can also be found in [Bor17]. There are also other sound, but incomplete, proof rules for deductive verification along an ODE system [TT09, Tiw08, PJP07, PJ04]. We do not consider these alternative rules, but, e.g. barrier certificates [PJP07], are an easy consequence of the results in Section 6; see Appendix A for a derivation. The aforementioned works focus on the proof rules as stand-alone verification principles for checking invariance of a formula over the evolution of an ODE. As a result, they usually involve complex side conditions necessary for correctness. This makes them very difficult to implement soundly as part of a *small* axiomatic core, such as the implementation of dL in KeYmaera X [FMQ+15, Pla17a]. Our work thus focuses on *deriving* these rules directly from a small set of axiomatic principles.

Deductive Power and Proof Theory. The proof rules we study are sound and complete, but their generality also means that the premises could be more complex than necessary, especially for simpler invariants. This is where a study of the deductive power of various sound, but incomplete, proof rules [GSP17] 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 [Pla12c], which studies the relative deductive power of differential invariants (DI) and differential cuts (DC), two important reasoning principles in dL, that are both shown to increase the deductive power of the logic. Other proof theoretic studies of dL [Pla08, Pla12a] 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.

Generating Invariants. Our work focuses on *proving* the invariance of a formula – an orthogonal question is how we might *generate* these invariants in the first place. An effective approach, used, for example, in [PJ04, PJP07, SSM08, PC08, GP14, LZZ11], is to use templates for polynomials invariants. From a given template, the premises of a proof rule can be computed symbolically, resulting in constraints on template parameters.

3 Background

This section briefly reviews the relevant fragment of dL, and establishes the notational conventions that we will use in this report. We refer readers to [Pla08, Pla12b, Pla17a] for a more complete exposition of dL, including its discrete fragment.

3.1 Syntax and Semantics

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

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

These terms correspond to polynomials over the variables under consideration. For the purposes of this report, we write x to refer to a vector of variables $x_0, \cdots, x_n$, and we use $p(x), q(x)$ to stand for polynomial terms over these variables. When the variable context is clear, we also simply write p, q without arguments instead.

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

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

We assume that all the formulas of the form $e \sim e$ are normalized to have 0 on the right-hand side. We also write $p \succeq 0$ if there is a free choice of $\succeq$ between $\geq$ or $>$. We may define $p \preceq 0 \iff -p \succeq 0$, where $\preceq$ stands for $\leq$ or $<$, and $\succeq$ is correspondingly chosen.

Hybrid programs α allow one to express both discrete and continuous dynamics. We shall only be concerned with the continuous dynamics, where $\alpha := x' = f(x) \,\&\, Q$, i.e. an autonomous vectorial ODE system in variables $x_0, \cdots, x_n$, restricted to evolution domain Q. In fact, sound and complete calculi for hybrid systems exist relative to purely continuous dynamical systems [Pla12a].

Semantically, terms and comparison operations on terms are given the usual interpretation in first-order real arithmetic. The logical connectives are also defined in the standard way, for example, $u \in [\![\phi_1 \wedge \phi_2]\!]$ is true if and only if $u \in [\![\phi_1]\!]$ and $u \in [\![\phi_2]\!]$. Hybrid programs are interpreted as transition relations, $[\![\alpha]\!] \subseteq \mathbb{R}^n \times \mathbb{R}^n$, between states. In particular, the transition semantics of an ODE is defined as:

$$(u, v) \in [\![x' = f(x) \,\&\, Q]\!] \iff \exists \phi : [0, T] \to \mathbb{R}^n \phi(0) = u, \phi(T) = v, \phi \vDash x' = f(x) \,\&\, Q$$

Here, $\phi(t)$ is a solution starting in state u and ending at v. The $\phi \vDash x' = f(x) \,\&\, Q$ assertion checks that ϕ respects the ODE system $x' = f(x)$, and that it stays in Q for $t \in [0, T]$.

Finally, the modal formula $[\alpha]\phi$ is true in a state u iff for all states v such that $(u, v) \in [\![\alpha]\!]$, ϕ is also true in v. Dually, $\langle\alpha\rangle\phi$ holds in u iff there exists a state v, where $(u, v) \in [\![\alpha]\!]$ and ϕ holds in v.

Putting these definitions together, we shall consider formulas of the form:

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

where P is a first-order formula of real arithmetic generated by ϕ (i.e. not containing modal operators). Intuitively, this formula asserts that P is a (positive) invariant of the ODE system – if we start in a state satisfying P and follow the dynamics forwards in time, then we always remain in a state satisfying P.

3.2 Axiomatization

We assume a classical sequent calculus for dL, and we only present here the axiomatization for differential equations following [Pla17a, Figure 3].

Theorem 1 (Differential equation axiomatization)**.** *The following axioms are sound for* dL *[Pla17a]:*

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

$$\text{DC}\ ([x' = f(x)\,\&\,Q]P \leftrightarrow [x' = f(x)\,\&\,Q \wedge C]P) \leftarrow [x' = f(x)\,\&\,Q]C$$

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

$$\text{DI}\ ([x' = f(x)\,\&\,Q]P \leftrightarrow [?Q]P) \leftarrow (Q \to [x' = f(x)\,\&\,Q](P)')$$

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

Differential weakening (DW), asserts that we may assume that the evolution domain holds while proving a post-condition. Differential cut (DC) asserts that if we separately prove that C is an invariant of the ODE system, then we may assume that the ODE under consideration additionally never leaves C.

The differential effect axiom (DE) asserts that solutions obey the RHS of the differential equations. This is typically used to assert that the differential symbols take their corresponding values when reasoning about the post-condition.

The differential induction axiom (DI) reduces questions about a invariant P to a question about its differential $(P)'$. A particular instance of DI is the following:

$$\text{DI}_{\geq}\ [x' = f(x)\,\&\,Q](p)' \geq 0 \to \big(p \geq 0 \to [x' = f(x)\,\&\,Q]p \geq 0\big)$$

Intuitively, if the differential of p stays positive throughout the evolution of an ODE, then if we start in $p \geq 0$, we must stay in $p \geq 0$ because p can only be increasing. Therefore, $p \geq 0$ is an invariant. We note that $\text{DI}_{\geq}$ is equivalent to a version of the mean value theorem[2]:

Corollary 2 (Mean value theorem)**.** *The following analogue of the mean value theorem is a derived axiom:*

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

Proof. By taking contrapositives in $\text{DI}_{\geq}$. □

[2]This is unsurprising, because the proof of soundness for $\text{DI}_{\geq}$ relies on the mean value theorem.

Finally, the differential ghosts axiom (DG) allows one to add a fresh variable y to the system of equations. The main soundness restriction of this rule is that the RHS must be linear in y. For our purposes, we will let y be vectorial, i.e. we allow the existing differential equations to be extended by a system that is linear in a vector of variables y. This axiom is known to increase the deductive power over a calculus with only DI,DC [Pla12c]. Indeed, we shall see in the upcoming section that making clever choices of differential ghosts will allow us to prove complicated properties beyond the reach of DI,DC. We will exploit this increased deductive power in full in later sections.

3.3 Extensions

For the rest of this report, we will use two mild extensions to the standard grammar of dL terms given above.

- We add terms of the form: $\frac{e_1}{e_2}$. This extends terms from polynomials to rational functions. We assume that the denominators are non-zero in the domain of interest wherever such terms appear in order for the term to have well-defined semantics. For example, if $\frac{1}{e}$ appears on the RHS of an ODE, then the evolution domain must imply that $e \neq 0$.
- We also need terms of the form: $\max(p,q), \min(p,q)$. Unlike polynomials, such terms are not smooth, and so we treat them as a separate syntactic class. In particular, they are not allowed to appear on the right-hand sides of an ODE, and we do not allow arithmetic operations on these terms. For formulas, this does not result in an extension in expressivity because we may equivalently rewrite them with:

$$\max(p,q) \succeq e \iff p \succeq e \vee q \succeq e$$

$$\min(p,q) \succeq e \iff p \succeq e \wedge q \succeq e$$

3.4 Notation

We write $(p)^{(i)}$ for the i-th differential [Pla17a] of the term p and $\mathcal{L}^{(i)}_{f(x)}(p)$ for the i-th Lie derivative of p along $x' = f(x)$. Following convention, we let $(p)^{(0)} = p = \mathcal{L}^{(0)}_{f(x)}(p)$. By the differential lemma [Pla17a, Lemma 35], these two notions coincide along an ODE. This is internalized in dL by the differential effect axiom DE, and a set of axioms for computing the syntactic derivations c',x',$+'$,$\cdot'$,$\circ'$ [Pla17a, Lemmas 36-37]. Syntactically, this means that $\mathcal{L}^{(i)}_{f(x)}(p)$ is equivalent to $(p)^{(i)}$ after an i-fold application of differential assignment $[':=]$ and some arithmetic manipulation. More formally, we can use the following derivation to convert between the two notions under an ODE (assuming p is a polynomial). We omit the full derivation and freely swap the two notions for the rest of this report.

$$\text{DE}\ \frac{[':=],c',x',+',\cdot',\circ',\mathbb{R}\ \dfrac{*}{\vdash [x'=f(x)\,\&\,Q][x':=f(x)](p)' = \mathcal{L}_{f(x)}(p)}}{\vdash [x'=f(x)\,\&\,Q](p)' = \mathcal{L}_{f(x)}(p)}$$

Note that for polynomial vector fields and polynomials p, $\mathcal{L}_{f(x)}(p)$ is also a polynomial, which means that we can iterate the above derivation for any higher Lie derivative. This also allows us to swap $(p)^{(i)}$ for $\mathcal{L}^{(i)}_{f(x)}(p)$ under an ODE freely.

Since we work with autonomous ODE systems, it will also be convenient to assume that a clock variable with $x_0' = 1$ exists in the system. Such a clock can always be introduced using DG if not already present.

4 Darboux Polynomials

This section considers proof rules that directly derive in dL without additional axioms. Although these proof rules are not complete on their own, they provide crucial intuition for the subsequent sections. A generalization of the techniques presented here will be used in Section 5, where we derive a complete proof rule for algebraic invariants.

4.1 Fractional Darboux are Ghosts of Differential Invariants

A polynomial $p(x)$ is a Darboux polynomial [Dar78] for the system $x' = f(x)$ iff we have $\mathcal{L}_{f(x)}(p(x)) = g(x)p(x)$ for some polynomial cofactor $g(x)$. Correspondingly, $p(x)$ is a fractional Darboux polynomial if $q(x)\mathcal{L}_{f(x)}(p(x)) = g(x)p(x)$ for some cofactor polynomials $g(x), q(x)$.

Our first derivation shows a proof of invariance for $p(x) = 0$, assuming it is a (fractional) Darboux polynomial.

Lemma 3 (Darboux are ghosts of differential invariants)**.** *Fractional Darboux polynomials derive with differential ghosts from differential invariants. The following is a derived proof rule*[3]*:*

$$\text{FDbx}\ \frac{Q \land q(x) \neq 0 \vdash [x':=f(x)]q(x)(p(x))' = g(x)p(x)}{p(x) = 0 \vdash [x' = f(x)\,\&\,Q \land q(x) \neq 0]p(x) = 0}$$

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

$$\cfrac{\cfrac{\cfrac{}{p(x)=0 \vdash [x' = f(x), y' = -\frac{g(x)}{q(x)}y\,\&\,Q \land q(x) \neq 0]p(x)y=0}\ ②}{p(x) = 0, y \neq 0 \vdash [x' = f(x), y' = -\frac{g(x)}{q(x)}y\,\&\,Q \land q(x) \neq 0](y \neq 0 \land p(x)y = 0)}\,[]\land}{\cfrac{p(x) = 0 \vdash \exists y\,[x' = f(x), y' = -\frac{g(x)}{q(x)}y\,\&\,Q \land q(x) \neq 0]p(x) = 0}{p(x) = 0 \vdash [x' = f(x)\,\&\,Q \land q(x) \neq 0]p(x) = 0}\,\text{DG}}\,\text{M}[\cdot],\exists\text{R}$$

Note that the assumption $q(x) \neq 0$ is required in order for the application of DG to be sound. The

[3]The proof rule with $q(x) = 1$ is also called polynomial scale consecution in [SSM08].

proof of the left premise continues as follows (after a simple cut with real arithmetic):

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\textcircled{1} \qquad \overset{*}{\overline{{}^{\mathbb{R}}Q \wedge q(x) \neq 0 \vdash \frac{g(x)}{q(x)}p(x)y - \frac{g(x)}{q(x)}yp(x) = 0}}}}{Q \wedge q(x) \neq 0 \vdash [x'{:=}f(x)](p(x))'y - \frac{g(x)}{q(x)}yp(x) = 0}\,\text{cut}}{Q \wedge q(x) \neq 0 \vdash [x'{:=}f(x)][y'{:=} - \frac{g(x)}{q(x)}y](p(x))'y + y'p(x) = 0}\,[']}{p(x)y = 0 \vdash [x' = f(x), y' = -\frac{g(x)}{q(x)}y \,\&\, Q \wedge q(x) \neq 0]p(x)y = 0}\,\text{DI}}{p(x) = 0 \vdash [x' = f(x), y' = -\frac{g(x)}{q(x)}y \,\&\, Q \wedge q(x) \neq 0]p(x)y = 0}\,\text{cut,}\mathbb{R}$$

In fact, the choice of the differential ghost $y' = -\frac{g(x)}{q(x)}y$ is obtained by solving the remaining condition for y'. The right premise ② is:

$$y \neq 0 \vdash [x' = f(x), y' = -\frac{g(x)}{q(x)}y \,\&\, Q \wedge q(x) \neq 0]y \neq 0$$

Its proof continues using a second ghost:

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\overset{*}{\overline{Q \wedge q(x) \neq 0 \vdash [x'{:=}f(x)]0 = 0}}}{Q \wedge q(x) \neq 0 \vdash [x'{:=}f(x)] - z\frac{g(x)}{q(x)}y + y\frac{g(x)}{q(x)}z = 0}\,\mathbb{R}}{Q \wedge q(x) \neq 0 \vdash [x'{:=}f(x)][y'{:=} - \frac{g(x)}{q(x)}y][z'{:=}\frac{g(x)}{q(x)}z]zy' + yz' = 0}\,[']}{yz = 1 \vdash [x' = f(x), y' = -\frac{g(x)}{q(x)}y, z' = \frac{g(x)}{q(x)}z \,\&\, Q \wedge q(x) \neq 0]yz = 1}\,\text{DI}}{y \neq 0 \vdash \exists z\, [x' = f(x), y' = -\frac{g(x)}{q(x)}y, z' = \frac{g(x)}{q(x)}z \,\&\, Q \wedge q(x) \neq 0]y \neq 0}\,\text{M}[\cdot],\exists\mathbb{R}}{y \neq 0 \vdash [x' = f(x), y' = -\frac{g(x)}{q(x)}y \,\&\, Q \wedge q(x) \neq 0]y \neq 0}\,\text{DG}$$

□

By inspection of the derivation above, it is easy to see the following generalization to fractional Darboux inequalities, where $q(x)\mathcal{L}_{f(x)}(p(x)) \succeq g(x)p(x)$.

Lemma 4 (Darboux inequalities are ghosts of differential invariants)**.** *Fractional Darboux polynomial inequalities derive with differential ghosts from differential invariants. The following is a derived proof rule:*

$$\text{FDbx}_{\succeq}\ \frac{Q \wedge q(x){>}0 \vdash [x'{:=}f(x)]q(x)(p(x))' \geq g(x)p(x)}{p(x) \succeq 0 \vdash [x' = f(x) \,\&\, Q \wedge q(x) > 0]p(x) \succeq 0}$$

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

$$\cfrac{\cfrac{\cfrac{p(x){\succeq}0, y{>}0 \vdash [x' = f(x), y' = -\frac{g(x)}{q(x)}y \,\&\, Q \wedge q(x){>}0 \wedge y > 0]p(x)y \succeq 0 \quad \textcircled{2}}{p(x) \succeq 0, y > 0 \vdash [x' = f(x), y' = -\frac{g(x)}{q(x)}y \,\&\, Q \wedge q(x){>}0](y > 0 \wedge p(x)y \succeq 0)}\,\text{DC}}{p(x) \succeq 0 \vdash \exists y\, [x' = f(x), y' = -\frac{g(x)}{q(x)}y \,\&\, Q \wedge q(x){>}0]p(x) \succeq 0}\,\text{M}[\cdot],\exists\mathbb{R}}{p(x) \succeq 0 \vdash [x' = f(x) \,\&\, Q \wedge q(x){>}0]p(x) \succeq 0}\,\text{DG}$$

Note the minor variation in the proof: the last step above uses DC instead of $[]\wedge$ so that $y > 0$ is available in the left premise. This allows the proof of the left premise to continue in a similar fashion:

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\textcircled{1} \qquad \overset{*}{\overline{Q \wedge q(x){>}0 \wedge y > 0 \vdash \frac{g(x)}{q(x)}p(x)y - \frac{g(x)}{q(x)}yp(x) \geq 0}}^{\mathbb{R}}}{Q \wedge q(x){>}0 \wedge y > 0 \vdash [x'{:=}f(x)](p(x))'y - \frac{g(x)}{q(x)}yp(x) \geq 0}\,\text{cut}}{Q \wedge q(x){>}0 \wedge y > 0 \vdash [x'{:=}f(x)][y'{:=} -\frac{g(x)}{q(x)}y](p(x))'y + y'p(x) \geq 0}\,[':=]}{p(x)y{\succeq}0 \vdash [x' = f(x), y' = -\frac{g(x)}{q(x)}y \,\&\, Q \wedge q(x){>}0 \wedge y > 0]p(x)y \succeq 0}\,\text{DI}}{p(x){\succeq}0, y{>}0 \vdash [x' = f(x), y' = -\frac{g(x)}{q(x)}y \,\&\, Q \wedge q(x){>}0 \wedge y > 0]p(x)y \succeq 0}\,\text{cut,}\mathbb{R}$$

Again, the choice of the differential ghost $y' = -\frac{g(x)}{q(x)}y$ is obtained by solving the remaining condition for y'. The right premise ② is:

$$y > 0 \vdash [x' = f(x), y' = -\frac{g(x)}{q(x)}y \,\&\, Q \wedge q(x) > 0]y > 0$$

Its proof continues using a second ghost:

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\overset{*}{\overline{}}}{Q \wedge q(x){>}0 \vdash [x'{:=}f(x)]0 = 0}\,\text{G,}\mathbb{R}}{Q \wedge q(x){>}0 \vdash [x'{:=}f(x)]{-}z^2\frac{g(x)}{q(x)}y + 2yz\frac{g(x)}{2q(x)}z = 0}\,\mathbb{R}}{Q \wedge q(x){>}0 \vdash [x'{:=}f(x)][y'{:=} -\frac{g(x)}{q(x)}y][z'{:=}\frac{g(x)}{2q(x)}z]z^2y' + 2yzz' = 0}\,[':=]}{yz^2 = 1 \vdash [x' = f(x), y' = -\frac{g(x)}{q(x)}y, z' = \frac{g(x)}{2q(x)}z \,\&\, Q \wedge q(x){>}0]yz^2 = 1}\,\text{DI}}{y > 0 \vdash \exists z\,[x' = f(x), y' = -\frac{g(x)}{q(x)}y, z' = \frac{g(x)}{2q(x)}z \,\&\, Q \wedge q(x){>}0]y > 0}\,\text{M[}\cdot\text{],}\exists\text{R}}{y > 0 \vdash [x' = f(x), y' = -\frac{g(x)}{q(x)}y \,\&\, Q \wedge q(x){>}0]y > 0}\,\text{DG}$$

For the case where $\succeq$ is $>$, the equivalence $p(y) > 0 \leftrightarrow \exists y\,(y > 0 \wedge p(x)y > 0)$ is used in the M[·],∃R step. □

A minor variation leads to the following result with an equational premise (proof omitted):

Lemma 5 (Darboux inequalities are ghosts of differential invariants)**.** *Fractional Darboux polynomial inequalities derive with differential ghosts from differential invariants. The following is a derived proof rule:*

$$\text{FDbx}'_{\succeq}\ \frac{Q \wedge q(x){\neq}0 \vdash [x'{:=}f(x)]q(x)(p(x))' = g(x)p(x)}{p(x) \succeq 0 \vdash [x' = f(x) \,\&\, Q \wedge q(x) \neq 0]p(x) \succeq 0}$$

One simple consequence of this derived rule is the following analogue of the intermediate value theorem, asserting that we can always reach a zero-crossing. Note that we will see stronger versions in Section 6.

Corollary 6 (Intermediate value theorem)**.** *The following are derived axioms:*

$$\text{IVT}\quad p(x)\geq 0\land\langle x'=f(x)\,\&\,Q\rangle\, p(x)\leq 0\to\langle x'=f(x)\,\&\,Q\rangle\, p(x)=0$$

$$\text{IVT}_{[]\geq}\quad p(x)\geq 0\to[x'=f(x)\,\&\,Q\land p(x)\neq 0]\, p(x)\geq 0$$

$$\text{IVT}_{[]>}\quad p(x)>0\to[x'=f(x)\,\&\,Q\land p(x)\neq 0]\, p(x)>0$$

Proof. $\text{IVT}_{[]\geq}$ and $\text{IVT}_{[]>}$ derive from each other by DW (and DI in case $p(x)=0$). IVT derives from $\text{IVT}_{[]\geq}$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{p(x)\geq 0\vdash[x'=f(x)\,\&\,Q\land p(x)\neq 0]\,p(x)\geq 0}\text{DC}}{p(x)\geq 0,[x'=f(x)\,\&\,Q]p(x)\neq 0\vdash[x'=f(x)\,\&\,Q]\,p(x)\geq 0}\langle\cdot\rangle,\neg\text{L},\neg\text{R}}{p(x)\geq 0,\langle x'=f(x)\,\&\,Q\rangle p(x)<0\vdash\langle x'=f(x)\,\&\,Q\rangle\, p(x)=0}\lor\text{L},\text{id}}{p(x)\geq 0,\langle x'=f(x)\,\&\,Q\rangle p(x)=0\lor\langle x'=f(x)\,\&\,Q\rangle p(x)<0\vdash\langle x'=f(x)\,\&\,Q\rangle\, p(x)=0}\text{K}}{p(x)\geq 0,\langle x'=f(x)\,\&\,Q\rangle(p(x)=0\lor p(x)<0)\vdash\langle x'=f(x)\,\&\,Q\rangle\, p(x)=0}\text{CE},\land\text{L}}{p(x)\geq 0\land\langle x'=f(x)\,\&\,Q\rangle\, p(x)\leq 0\vdash\langle x'=f(x)\,\&\,Q\rangle\, p(x)=0}$$

$\text{IVT}_{[]\geq}$ in turn proves by $\text{FDbx}'_{\geq}$ with $q(x)\overset{\text{def}}{=}p(x)$ and $g(x)\overset{\text{def}}{=}(p(x))'$:

$$\dfrac{\dfrac{*}{Q\land p(x)\neq 0\vdash[x':=f(x)]p(x)(p(x))'=(p(x))'p(x)}\mathbb{R},\text{G}}{p(x)\geq 0\vdash[x'=f(x)\,\&\,Q\land p(x)\neq 0]\,p(x)\geq 0}\text{FDbx}'_{\geq}$$

□

5 Algebraic Invariants

In this section, we show that we can derive the following sound and complete proof rule, DRI, for algebraic invariants [GP14].

$$\text{DRI}\quad\dfrac{p=0\to\bigwedge_{i=1}^{N-1}\mathcal{L}^{(i)}_{f(x)}(p)=0}{p=0\to[x'=f(x)]p=0}\quad(\mathcal{L}^{(N)}_{f(x)}(p)=\textstyle\sum_{i=0}^{N-1}g_i\mathcal{L}^{(i)}_{f(x)}(p))$$

The side condition of this rule, $\mathcal{L}^{(N)}_{f(x)}(p)=\sum_{i=0}^{N-1}g_i\mathcal{L}^{(i)}_{f(x)}(p)$, asserts that $\mathcal{L}^{(N)}_{f(x)}(p)$ is contained in the ideal generated by lower Lie derivatives of p, where g_i are cofactor polynomials witnessing ideal membership. The (equational) Darboux proof rule is a special case of DRI with $N=1$.

Note that it is sufficient for us to consider an invariant of the form $p=0$ since any algebraic invariant defined by finite conjunctions and disjunctions of equations may be reduced to this form with the following real arithmetic equivalences:

$$p=0\land q=0\iff p^2+q^2=0$$
$$p=0\lor q=0\iff pq=0$$

The following definition is central to the soundness and completeness of DRI [GP14]:

Definition 1 (Differential rank)**.** The *differential rank* of a polynomial p in a vector field $f(x)$ is the smallest N such that:

$$\mathcal{L}^{(N)}_{f(x)}(p) = \sum_{i=0}^{N-1} g_i \mathcal{L}^{(i)}_{f(x)}(p)$$

The proof that the differential rank is well-defined can be found in [NY99, GP14, LZZ11]. It relies on the fact that the polynomial ring $\mathbb{R}[x]$ is Noetherian, which implies that the (ascending) chain of ideals:

$$\langle p \rangle \subset \langle p, \mathcal{L}_{f(x)}(p) \rangle \subset \cdots$$

terminates. In addition, N is computable by successively checking for ideal membership of $\mathcal{L}^{(N)}_{f(x)}(p)$ in $\langle p, \mathcal{L}_{f(x)}(p), \cdots, \mathcal{L}^{(N-1)}_{f(x)}(p) \rangle$ for $N = 1, 2, \cdots$. An upper bound on the length of the chain, and hence, N, is given in [NY99, Theorem 4].

5.1 Vectorial Disequational Darboux

We start by deriving a vectorial generalization of the Darboux-style proof rules in the previous section. The derivation requires the ability to simultaneously add a vector of fresh variables to the ODE under consideration with differential ghosts.

Lemma 7 (Vectorial disequational Darboux are differential ghosts)**.** *Vectorial DG proves:*

$$\text{VDbx}_{\neq} \quad \frac{Q \vdash [x' := f(x)](\vec{p}(x))' = G(x)\vec{p}(x)}{\vec{p}(x) \cdot \vec{p}(x) > 0 \vdash [x' = f(x) \,\&\, Q]\vec{p}(x) \cdot \vec{p}(x) > 0}$$

where $G(x)$ is an $M \times M$ matrix of polynomials, and $\vec{p}(x)$ is an M dimensional vector.

Proof. The $\exists$R step uses $\vec{p}(x)$ as witness for $\vec{y}$ since $\vec{p}(x) \cdot \vec{p}(x) > 0$ implies $\vec{p}(x) \cdot \vec{y} > 0$ then (conversely $\vec{p}(x) \cdot \vec{y} > 0$ also necessitates $\vec{p}(x) \cdot \vec{p}(x) > 0$ in step M$[\cdot]$):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{Q \vdash [x' := f(x)]G(x)\vec{p}(x) \cdot \vec{y} - G(x)\vec{p}(x) \cdot \vec{y} \geq 0}\,{}^{*}\,\text{G},\mathbb{R} \quad \textcircled{1}}{Q \vdash [x' := f(x)]G(x)\vec{p}(x) \cdot \vec{y} - \vec{p}(x) \cdot G(x)^T\vec{y} \geq 0}\,\mathbb{R}}{Q \vdash [x' := f(x)](\vec{p}(x))' \cdot \vec{y} - \vec{p}(x) \cdot G(x)^T\vec{y} \geq 0}\,\text{cut}}{Q \vdash [x' := f(x)][y' := -G(x)^T\vec{y}](\vec{p}(x))' \cdot \vec{y} + \vec{p}(x) \cdot (\vec{y})' \geq 0}\,[':=]}{\vec{p}(x) \cdot \vec{y} > 0 \vdash [x' = f(x), \vec{y}' = -G(x)^T\vec{y} \,\&\, Q]\vec{p}(x) \cdot \vec{y} > 0}\,\text{DI}}{\vec{p}(x) \cdot \vec{p}(x) > 0 \vdash \exists \vec{y}\, [x' = f(x), \vec{y}' = -G(x)^T\vec{y} \,\&\, Q]\vec{p}(x) \cdot \vec{p}(x) > 0}\,\text{M}[\cdot],\exists\text{R}}{\vec{p}(x) \cdot \vec{p}(x) > 0 \vdash [x' = f(x) \,\&\, Q]\vec{p}(x) \cdot \vec{p}(x) > 0}\,\text{DG}$$

□

For notational simplicity, we used matrix and vector notation to express the proof rule and derivation. However, instances of the rule at any dimension M can be derived using our term language (without matrices and vectors) using vectorial DG. Note also that as a simple consequence of real arithmetic, we may replace the invariant formula with $\vec{p}(x) \cdot \vec{p}(x) > 0 \iff \bigvee_{i=0}^{M-1} p_i(x) \neq 0$.

5.2 Differential Adjoints

Differential adjoints express that x can flow to y forward iff y can flow to x backwards along an ODE. They are 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 [Pla12a, Pla15].

Lemma 8 (Differential adjoints)**.** *The differential adjoint axiom is sound:*

$$'^{*}\ \langle x' = f(x) \,\&\, Q(x)\rangle\, x = y \leftrightarrow \langle y' = -f(y) \,\&\, Q(y)\rangle\, y = x$$

Proof. Both implications are proved separately. Consider any state ω in which one side is true and prove the other.

"$\rightarrow$" Assume that there is a transition $(\omega, \nu) \in [\![x' = f(x) \,\&\, Q(x)]\!]$ of duration r such that $\nu \in [\![x = y]\!]$. By uniqueness, the solutions of $x' = -f(x) \,\&\, Q(x)$ are exactly the reverse of solutions of $x' = f(x) \,\&\, Q(x)$. Thus, $(\nu, \omega) \in [\![x' = -f(x) \,\&\, Q(x)]\!]$. Since $\nu \in [\![x = y]\!]$, the solutions of $x' = -f(x) \,\&\, Q(x)$ starting in ν directly correspond to the solutions of $y' = -f(y) \,\&\, Q(y)$ starting in ν, just with the values of x and y swapped. That is, the two respective solutions φ of $x' = -f(x) \,\&\, Q(x)$ and ϑ of $y' = -f(y) \,\&\, Q(y)$ agree with ν and ω except that $\varphi(t)(x) = \vartheta(t)(y)$ and $\varphi(t)(y) = \vartheta(t)(x) = \nu(x) = \nu(y)$ for all times t. Consequently, $\omega(x) = \varphi(r)(x) = \vartheta(r)(y)$. Let μ denote the state reached from ω along $y' = -f(y) \,\&\, Q(y)$ after duration r. Then $(\omega, \mu) \in [\![y' = -f(y) \,\&\, Q(y)]\!]$ and $\mu \in [\![x = y]\!]$, because $\mu(y) = \vartheta(r)(y) = \omega(x)$ by coincidence lemma since ω and ν agree on the free variables of $y' = -f(y) \,\&\, Q(y)$ by bound effect lemma as $(\omega, \nu) \in [\![x' = f(x) \,\&\, Q(x)]\!]$ of duration r such that $\nu \in [\![x = y]\!]$ implies that both agree except on x, x'.

"$\leftarrow$" This direction follows from direction "$\rightarrow$" by swapping the names x and y, because $-(-f(x)) = f(x)$. □

5.3 Reflections

The differential adjoint axiom yields predicate reflection under $\langle\cdot\rangle$. Intuitively, if we can start in a state u satisfying P and reach a state v satisfying R following the ODE, then we may follow the ODE backwards starting at v and ending at u.

Corollary 9 ($\langle\cdot\rangle$Reflection)**.** *The following predicate reflection axiom derives from $'^{*}$:*

$$\text{reflect}_{\langle\cdot\rangle}\ \exists x\,(P(x) \wedge \langle x' = f(x) \,\&\, Q(x)\rangle R(x)) \leftrightarrow \exists x\,(R(x) \wedge \langle x' = -f(x) \,\&\, Q(x)\rangle P(x))$$

Proof. Both implications are proved separately and the "$\leftarrow$" direction follows by instantiating the

proof of the "$\rightarrow$" direction, since $-(-f(x)) = f(x)$.

$$
\begin{array}{rl}
 & \ast \\
\exists\text{R} & \dfrac{}{R(z), \langle z' = -f(z)\,\&\,Q(z)\rangle P(z) \vdash \exists x\,(R(x) \wedge \langle x' = -f(x)\,\&\,Q(x)\rangle P(x))} \\
\text{CE} & \dfrac{}{P(y), R(z), \langle z' = -f(z)\,\&\,Q(z)\rangle z = y \vdash \exists x\,(R(x) \wedge \langle x' = -f(x)\,\&\,Q(x)\rangle P(x))} \\
{}'{}^{*} & \dfrac{}{P(y), R(z), \langle y' = f(y)\,\&\,Q(y)\rangle z = y \vdash \exists x\,(R(x) \wedge \langle x' = -f(x)\,\&\,Q(x)\rangle P(x))} \\
\text{B},\exists\text{L} & \dfrac{}{P(y), \langle y' = f(y)\,\&\,Q(y)\rangle \exists z\,(z = y \wedge R(z)) \vdash \exists x\,(R(x) \wedge \langle x' = -f(x)\,\&\,Q(x)\rangle P(x))} \\
\text{CE} & \dfrac{}{P(y), \langle y' = f(y)\,\&\,Q(y)\rangle R(y) \vdash \exists x\,(R(x) \wedge \langle x' = -f(x)\,\&\,Q(x)\rangle P(x))} \\
\exists\text{L} & \dfrac{}{\exists x\,(P(x) \wedge \langle x' = f(x)\,\&\,Q(x)\rangle R(x)) \vdash \exists x\,(R(x) \wedge \langle x' = -f(x)\,\&\,Q(x)\rangle P(x))}
\end{array}
$$

□

Consequently, we have the following invariant reflection principle: $\neg P$ must have been always true if it ever is true, if P remains always true (and vice versa).

Corollary 10 (Reflection)**.** *The invariant reflection axiom is sound, and derives from* $'^{*}$*:*

$$\text{reflect}\quad \forall x\,(P \rightarrow [x' = f(x)\,\&\,Q]P) \leftrightarrow \forall x\,(\neg P \rightarrow [x' = -f(x)\,\&\,Q]\neg P)$$

Proof. This follows immediately from $\text{reflect}_{\langle\cdot\rangle}$ by instantiating it with $R \overset{\text{def}}{=} \neg P$ and negating both sides of the equivalence. □

5.4 Vectorial Darboux

Combining invariant reflection and $\text{VDbx}_{\neq}$, yields the following:

Lemma 11 (Vectorial Darboux are vectorial ghosts)**.** *VDbx derives from vectorial DG by* $'^{*}$.

$$\text{VDbx}\quad \frac{Q \vdash [x'{:=}f(x)](\vec{p}(x))' = G(x)\vec{p}(x)}{\vec{p}(x) = 0 \vdash [x' = f(x)\,\&\,Q]\vec{p}(x) = 0}$$

Proof.

$$
\begin{array}{rl}
\mathbb{R} & \dfrac{Q \vdash [x'{:=}f(x)](\vec{p}(x))' = G(x)\vec{p}(x)}{Q \vdash [x'{:=}-f(x)](\vec{p}(x))' = -G(x)\vec{p}(x)} \\
\text{VDbx}_{\neq} & \dfrac{}{\vec{p}(x)\cdot\vec{p}(x) > 0 \vdash [x' = -f(x)\,\&\,Q]\vec{p}(x)\cdot\vec{p}(x) > 0} \\
\mathbb{R} & \dfrac{}{\vec{p}(x)\cdot\vec{p}(x) \neq 0 \vdash [x' = -f(x)\,\&\,Q]\vec{p}(x)\cdot\vec{p}(x) \neq 0} \\
\text{reflect} & \dfrac{}{\vec{p}(x)\cdot\vec{p}(x) = 0 \vdash [x' = f(x)\,\&\,Q]\vec{p}(x)\cdot\vec{p}(x) = 0} \\
\mathbb{R} & \dfrac{}{\vec{p}(x) = 0 \vdash [x' = f(x)\,\&\,Q]\vec{p}(x) = 0}
\end{array}
$$

The arithmetic on top of axiom reflect uses the fact that $\vec{p}(x)\cdot\vec{p}(x) \neq 0$ is equivalent to $\vec{p}(x)\cdot\vec{p}(x) > 0$, because $\vec{p}(x)\cdot\vec{p}(x) < 0$ is equivalent to false. The arithmetic in the final step holds because the Lie derivative satisfies $\mathcal{L}_f^{(i)}(p) = \nabla p \cdot f = -\nabla p \cdot -f = -\mathcal{L}_{-f}^{(i)}(p)$. □

5.5 Differential Radical Invariants

We now derive DRI as a special case of VDbx using a clever choice of the cofactor matrix $G(x)$.

Lemma 12 (Differential radical invariants are vectorial Darboux)**.** *DRI derives from VDbx, which in turn derives from $'^*$ and vectorial DG.*

$$\text{DRI}\ \frac{p=0 \to \bigwedge_{i=1}^{N-1} \mathcal{L}^{(i)}_{f(x)}(p)=0}{p=0 \to [x'=f(x)]p=0} \quad (\mathcal{L}^{(N)}_{f(x)}(p) = \textstyle\sum_{i=0}^{N-1} g_i \mathcal{L}^{(i)}_{f(x)}(p))$$

Proof. Let N be the rank of a use of the DRI proof rule, i.e. such that its side condition proves. We start by setting up for a proof by VDbx.

$$\text{cut}\ \frac{p=0 \vdash \bigwedge_{i=1}^{N-1} \mathcal{L}^{(i)}_{f(x)}(p)=0 \qquad \text{M}[\cdot]\ \frac{\begin{pmatrix} \mathcal{L}^{(N-1)}_{f(x)}(p) \\ \vdots \\ \mathcal{L}_{f(x)}(p) \\ p \end{pmatrix} = 0 \vdash [x'=f(x)\,\&\,Q] \begin{pmatrix} \mathcal{L}^{(N-1)}_{f(x)}(p) \\ \vdots \\ \mathcal{L}_{f(x)}(p) \\ p \end{pmatrix} = 0}{\begin{pmatrix} \mathcal{L}^{(N-1)}_{f(x)}(p) \\ \vdots \\ \mathcal{L}_{f(x)}(p) \\ p \end{pmatrix} = 0 \vdash [x'=f(x)\,\&\,Q]p=0}}{p=0 \vdash [x'=f(x)\,\&\,Q]p=0}$$

The left open premise is the premise of DRI. The cut proves because of the following simple fact of arithmetic:

$$p=0 \wedge \left(\bigwedge_{i=1}^{N-1} \mathcal{L}^{(i)}_{f(x)}(p)=0\right) \leftrightarrow \begin{pmatrix} \mathcal{L}^{(N-1)}_{f(x)}(p) \\ \vdots \\ \mathcal{L}_{f(x)}(p) \\ p \end{pmatrix} = 0$$

We then apply VDbx, with a proper choice of $G(x)$:

$$\text{VDbx}\ \frac{\mathbb{R}\ \dfrac{Q \vdash [x':=f(x)](\mathcal{L}^{(N-1)}_{f(x)}(p))' = g_{N-1}\mathcal{L}^{(N-1)}_{f(x)}(p) + \cdots + g_1\mathcal{L}_{f(x)}(p) + g_0 p}{Q \vdash [x':=f(x)]\left(\begin{pmatrix} \mathcal{L}^{(N-1)}_{f(x)}(p) \\ \vdots \\ \mathcal{L}_{f(x)}(p) \\ p \end{pmatrix}'\right) = \begin{pmatrix} g_{N-1} & \cdots & g_1 & g_0 \\ 1 & \cdots & 0 & 0 \\ & & & \\ 0 & \ddots & 0 & 0 \\ 0 & \cdots & 1 & 0 \end{pmatrix} \begin{pmatrix} \mathcal{L}^{(N-1)}_{f(x)}(p) \\ \vdots \\ \mathcal{L}_{f(x)}(p) \\ p \end{pmatrix}}}{\begin{pmatrix} \mathcal{L}^{(N-1)}_{f(x)}(p) \\ \vdots \\ \mathcal{L}_{f(x)}(p) \\ p \end{pmatrix} = 0 \vdash [x'=f(x)\,\&\,Q] \begin{pmatrix} \mathcal{L}^{(N-1)}_{f(x)}(p) \\ \vdots \\ \mathcal{L}_{f(x)}(p) \\ p \end{pmatrix} = 0}$$

The last proof step on the right premise uses that $Q \vdash [x'{:=}f(x)](\mathcal{L}_{f(x)}(p))' = 1\mathcal{L}^{(2)}_{f(x)}(p)$ is valid, or more generally for all $i < N-1$ that the following proves by construction of $\mathcal{L}^{(i+1)}_{f(x)}(p)$:

$$Q \vdash [x'{:=}f(x)](\mathcal{L}^{(i)}_{f(x)}(p))' = 1\mathcal{L}^{(i+1)}_{f(x)}(p)$$

Consequently from Q it is possible to directly prove all but the first row of:

$$[x'{:=}f(x)]\left(\begin{pmatrix} \mathcal{L}^{(N-1)}_{f(x)}(p) \\ \vdots \\ \mathcal{L}^{(2)}_{f(x)}(p) \\ \mathcal{L}_{f(x)}(p) \\ p \end{pmatrix}'\right) = \begin{pmatrix} g_{N-1} & \dots & g_2 & g_1 & g_0 \\ 1 & \dots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \dots & 1 & 0 & 0 \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \mathcal{L}^{(N-1)}_{f(x)}(p) \\ \vdots \\ \mathcal{L}^{(2)}_{f(x)}(p) \\ \mathcal{L}_{f(x)}(p) \\ p \end{pmatrix}$$

The first row leaves an open premise, which is the side condition of DRI. □

By the soundness and completeness theorem for DRI [GP14], our derivation shows that all algebraic invariants are provable by vectorial DG and the differential adjoints axiom $'^*$. However, not all first-order formulas of real arithmetic can be represented by algebraic sets. Additionally, we have not considered the effects of the evolution domain Q.

Using predicate reflection again, we may slightly extend the reach of DRI to simple inequalities with the following:

Corollary 13 (Backwards DDC signs)**.** *The following axiom is sound, and derives from $'^*$,IVT$_{[]>}$:*

$$\text{ddc}\quad \begin{array}{l} \forall x \left(p = 0 \to [x' = \pm f(x) \,\&\, Q]p = 0\right) \\ \leftrightarrow \forall x \left(p > 0 \to [x' = \mp f(x) \,\&\, Q]p > 0\right) \wedge \forall x \left(p < 0 \to [x' = \mp f(x) \,\&\, Q]p < 0\right) \end{array}$$

where $\pm$ and $\mp$ indicate that the sign of the ODE is flipped across the equivalence.

Proof. Using reflect directly derives:

$$\forall x \left(p = 0 \to [x' = f(x) \,\&\, Q]p = 0\right) \leftrightarrow \forall x \left(p \neq 0 \to [x' = -f(x) \,\&\, Q]p \neq 0\right)$$

Thus, it is sufficient for us to show: $\forall x \left(p \neq 0 \to [x' = -f(x) \,\&\, Q]p \neq 0\right)$ is equivalent to:

$$\forall x \left(p > 0 \to [x' = -f(x) \,\&\, Q]p > 0\right) \wedge \forall x \left(p < 0 \to [x' = -f(x) \,\&\, Q]p < 0\right)$$

"$\to$" We show the derivation for $p > 0$ since the one for $p < 0$ is symmetric.

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{p{>}0, [x' = -f(x) \,\&\, Q]p{\neq}0 \vdash [x' = -f(x) \,\&\, Q]p{>}0}\,\text{DC,IVT}_{[]>}}{p{>}0, \forall x \left(p{\neq}0 \to [x' = -f(x) \,\&\, Q]p{\neq}0\right) \vdash [x' = -f(x) \,\&\, Q]p{>}0}\,\forall\text{L},{\to}\text{L}}{\forall x \left(p{\neq}0 \to [x' = -f(x) \,\&\, Q]p{\neq}0\right) \vdash \forall x \left(p{>}0 \to [x' = -f(x) \,\&\, Q]p{>}0\right)}\,\forall\text{R},{\to}\text{R}}{\forall x \left(p{=}0 \to [x' = f(x) \,\&\, Q]p{=}0\right) \vdash \forall x \left(p{>}0 \to [x' = -f(x) \,\&\, Q]p{>}0\right)}\,\text{reflect}$$

"←" The idea is to case split on whether we start at $p > 0$ or $p < 0$, and then apply the assumptions directly. The open premise ① is symmetric, and it is closed using the corresponding assumption hidden by $\cdots$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{p{>}0, [x' = -f(x)\,\&\,Q]p{>}0, \cdots \vdash [x' = -f(x)\,\&\,Q]p{\neq}0}\,\mathbb{R},\mathrm{M}[\cdot]}{p{>}0, \forall x\,\big(p{>}0 \to [x' = -f(x)\,\&\,Q]p{>}0\big), \cdots \vdash [x' = -f(x)\,\&\,Q]p{\neq}0}\,\forall\mathrm{L},{\to}\mathrm{L} \quad ①}{p{>}0 \lor p{<}0, \forall x\,\big(p{>}0 \to [x' = -f(x)\,\&\,Q]p{>}0\big), \cdots \vdash [x' = -f(x)\,\&\,Q]p{\neq}0}\,\lor\mathrm{L}}{p{\neq}0, \forall x\,\big(p{>}0 \to [x' = -f(x)\,\&\,Q]p{>}0\big), \cdots \vdash [x' = -f(x)\,\&\,Q]p{\neq}0}\,\mathbb{R}}{\forall x\,\big(p{>}0 \to [x' = -f(x)\,\&\,Q]p{>}0\big), \cdots \vdash \forall x\,\big(p{\neq}0 \to [x' = -f(x)\,\&\,Q]p{\neq}0\big)}\,\forall\mathrm{R},{\to}\mathrm{R}}{\forall x\,\big(p{>}0 \to [x' = -f(x)\,\&\,Q]p{>}0\big), \cdots \vdash \forall x\,\big(p{=}0 \to [x' = f(x)\,\&\,Q]p{=}0\big)}\,\text{reflect}$$

□

Thus, to prove the invariance of $p > 0$, we could instead try to prove that $p = 0$ is invariant. However, this is not complete in general, and it also does not generalize to invariants involving conjunctions and disjunctions of inequalities, except when they are individually invariant.

6 Semialgebraic Invariants

By quantifier elimination, the set of points satisfying a first-order formula of real arithmetic P is semialgebraic, and can be characterized by a quantifier-free, finite formula of the form:

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

where p_{ij}, q_{ij} are polynomials, and $M, m(i), n(i)$ are finite indexes.

This section shows that the following sound and complete proof rule, due to [LZZ11], for semialgebraic invariants with a semialgebraic evolution domain constraint Q is a derived rule. We follow the simplified notation used in [GSP17] in our exposition of the rule.

$$\text{LZZ}\ \frac{\neg P \land Q \to \mathrm{In}_{-f(x)}(\neg P) \lor \mathrm{In}_{-f(x)}(\neg Q) \quad P \land Q \to \mathrm{In}_{f(x)}(P) \lor \mathrm{In}_{f(x)}(\neg Q)}{P \to [x' = f(x)\,\&\,Q]P}$$

Here, let $\Phi : \mathbb{R}^n \times [0, T] \to \mathbb{R}^n$ be the generic solution of the ODE system $x' = f(x)$ parameterized by both time and initial conditions. We define:

$$\mathrm{In}_{f(x)}(P)(x) \stackrel{\text{def}}{=} x \in \{y \mid \exists \varepsilon > 0\, \forall 0 < t < \varepsilon\, P(\Phi(y, t))\}$$

In other words, it is true at those points y where the solution of the ODE system $x' = f(x)$ starting at $x = y$ immediately enters and stays in P for $\varepsilon > 0$ time.

For simplicity, we will first focus on deriving the following simpler proof rule without the evolution domain constraints before generalizing to LZZ at the end of this section:

$$\text{In}\ \frac{\neg P \to \mathrm{In}_{-f(x)}(\neg P) \quad P \to \mathrm{In}_{f(x)}(P)}{P \to [x' = f(x)\,\&\,Q]P}$$

As stated, the LZZ proof rule is a *semantic* proof rule, because it refers to the generic solution Φ in its premises. This is awkward to implement in a proof calculus because it requires us to have the generic solution Φ, and also be able to correctly calculate $\text{In}_{f(x)}(P)$ from it.

6.1 Properties of $\text{In}_{f(x)}(P)$

The primary result of [LZZ11] is if $P \iff \bigvee_{i=0}^{M} \left(\bigwedge_{j=0}^{m(i)} p_{ij} \geq 0 \wedge \bigwedge_{j=0}^{n(i)} q_{ij} > 0 \right)$ is semialgebraic, then there is a semialgebraic formula that characterizes $\text{In}_{f(x)}(P)$.

In particular, the operator $\text{In}_{f(x)}(\cdot)$ is homomorphic across the usual logical connectives, and we have:

$$\text{In}_{f(x)}(P) \iff \bigvee_{i=0}^{M} \left(\bigwedge_{j=0}^{m(i)} \text{In}_{f(x)}(p_{ij} \geq 0) \wedge \bigwedge_{j=0}^{n(i)} \text{In}_{f(x)}(q_{ij} > 0) \right)$$

The formulas $\text{In}_{f(x)}(p > 0)$ and $\text{In}_{f(x)}(p \geq 0)$ for arbitrary polynomials p can also be characterized by finite formulas.

Let us first consider $\text{In}_{f(x)}(p > 0)$. For any given point in $y \in \mathbb{R}^n$, there are three possible scenarios:

- If $p(y) > 0$, then because solutions of the ODE are continuous, the solution must locally stay in the set of points satisfying $p > 0$. Therefore, we have $p > 0 \to \text{In}_{f(x)}(p > 0)$
- If $p(y) < 0$, then for the same continuity reasons, the solution cannot immediately enter $p > 0$. Thus, $p < 0 \to \neg\text{In}_{f(x)}(p > 0)$.
- If $p(y) = 0$, then we must look to the higher Lie derivatives of p. For example, if additionally $\mathcal{L}_{f(x)}(p(y)) > 0$, then the solution locally enters $y > 0$, while if $\mathcal{L}_{f(x)}(p(y)) < 0$, then it locally enters $y < 0$. In general, as long as the first non-zero Lie derivative of p at y is positive, then we will locally enter $p > 0$.

We define notation for the local Lie derivative condition recursively:

Definition 2 (First positive non-zero Lie derivative)**.**

$$\gamma_{f(x)}^{=n}(p) > 0 \equiv \mathcal{L}_{f(x)}^{(n)}(p) > 0 \wedge \bigwedge_{i=0}^{n-1} \mathcal{L}_{f(x)}^{(i)}(p) = 0$$
$$\gamma_{f(x)}^{\leq 0}(p) > 0 \equiv p > 0$$
$$\gamma_{f(x)}^{\leq n+1}(p) > 0 \equiv \gamma_{f(x)}^{\leq n}(p) > 0 \vee \gamma_{f(x)}^{=n+1}(p) > 0$$

The formula $\text{In}_{f(x)}(p > 0)$ is exactly true whenever $\gamma_{f(x)}^{\leq n}(p) > 0$ holds for any n:

$$\text{In}_{f(x)}(p > 0) \iff \gamma_{f(x)}^{\leq \infty}(p) > 0$$

Moreover, if N_p is the differential rank of p along $x' = f(x)$, then it is equivalent to the following finite disjunction:

$$\text{In}_{f(x)}(p > 0) \iff \gamma_{f(x)}^{\leq N_p - 1}(p) > 0$$

The reasoning for $\text{In}_{f(x)}(p \geq 0)$ is largely similar, since if a solution locally enters $p > 0$ it must also locally enter $p \geq 0$. However, we must additionally account for the possibility that $p = 0$ itself is invariant. Here, we have:

$$\text{In}_{f(x)}(p \geq 0) \iff \gamma_{f(x)}^{\leq N_p - 1}(p) > 0 \vee \bigwedge_{i=0}^{N_p - 1} \mathcal{L}_{f(x)}^{(i)}(p) = 0$$

Together, these properties imply that for any semialgebraic set P, the premises of LZZ are definable by finite formulas. This makes them amenable to derivation in our proof calculus for dL. However, note that the rule is still highly schematic – the equivalences for $\text{In}_{f(x)}(P)$ requires P to be decomposed into semialgebraic sets, and also requires side conditions on the differential rank with respect to $x' = f(x)$ for each of the polynomials in P. A direct implementation of the rule would have to syntactically decompose P into polynomials, and correctly compute each polynomial's Lie derivatives and differential rank with respect to the specific vector field $x' = f(x)$ on which the rule is applied. We show that we can soundly derive any instance of the rule with axioms, rather than such complex schemata.

6.2 Boundary Crossing Axioms

A crucial feature of the formulas characterizing $\text{In}_{f(x)}(P)$ is that they are concerned with how solutions behave at the boundary of P. For example, we saw that the most interesting case of $\text{In}_{f(x)}(p > 0)$ occurs when $p = 0$.

Here, we introduce two new axioms that we will use for the rest of this section. These axioms are designed to allow the sound introduction of evolution domain constraints that allow us to reason about these boundary situations within dL. Note that these axioms hold for generalized terms e containing the $\max, \min$ functions.

The first axiom is a strengthened version of the intermediate value theorem. Intuitively, it asserts that if the solution starts in a state satisfying $e(x) \succeq 0$, and ends in a state satisfying $e(x) \preceq 0$, then the solution must stay within $e(x) \succeq 0$ until we first reach the boundary at $e(x) = 0$.

Lemma 14 (Intermediate value theorem with domain constraint)**.** *The following analogue of the intermediate value theorem is sound:*

$$\text{IVT}_{\&} \quad e(x) \succeq 0 \wedge \langle x' = f(x) \,\&\, Q \rangle\, e(x) \preceq 0 \to \langle x' = f(x) \,\&\, Q \wedge e(x) \geq 0 \rangle\, e(x) = 0$$

Here, we take $\succeq$ to be either $\geq$ or $>$, and $\preceq$ to be either $\leq$ or $<$.

Proof. Consider a solution $\phi : [0, T] \to \mathbb{R}$ witnessing the existential on the LHS, and let $h : [0, T] \to \mathbb{R}$ be the valuation of $e(x)$ along ϕ. Since ϕ is continuous and e is a continuous function of its inputs[4], their composition, h, is also continuous.

Let τ be the supremum of the set $U = \{t \in [0, T] : \forall 0 \leq \zeta \leq t \; h(\zeta) \geq 0\}$, which is non-empty since $h(0) \succeq 0$. We claim that $h(\tau) = 0$. Suppose $h(\tau) > 0$, then by continuity, there exists an

[4]Polynomials, viewed as functions, are continuous, and $\max, \min$ are continuous as long as their arguments are continuous.

open interval $(\tau-\epsilon, \tau+\epsilon), \epsilon > 0$ around τ where $h > 0$, and thus we have $\tau + \frac{\epsilon}{2} \in U$, contradicting τ being the supremum. Similarly, suppose $h(\tau) < 0$, then there is an open interval to the left of τ where $h < 0$ where we may choose a smaller upper bound for U. Therefore $h(\tau) = 0$, and by construction, restricting ϕ to the interval $[0, \tau]$ yields a suitable witness for the RHS. □

The proof of $\text{IVT}_{\&}$ only required the fact that the solution ϕ is continuous. In our case, we additionally have ODE systems where the right-hand sides are analytic polynomial terms[5]. For any ODE system with analytic right-hand sides, their solutions are also analytic [Chi06, Theorem 1.3].

Using this property, we may further strengthen $\text{IVT}_{\&}$. As before, if a solution starts in a state satisfying $e \geq 0$ and ends in a state satisfying $e < 0$, then we stay in $e \geq 0$ until we reach $e = 0$. Now, $\text{IVT}_{\&}$ does not place further restrictions on the behavior of the solution at the intermediate state satisfying $e = 0$. The next axiom additionally asserts that the solution reaches a state satisfying $e = 0$, and then *immediately* enters $e < 0$ afterwards [6].

Lemma 15 (Intermediate value staging theorem)**.** *The following axiom is sound:*

$$\text{IVST}\quad e \geq 0 \land \langle x' = f(x) \,\&\, Q\rangle\, e < 0 \to \langle x' = f(x) \,\&\, Q \land e \geq 0\rangle\, \langle x' = f(x) \,\&\, Q \land e \leq 0\rangle e < 0$$

Proof. Let $\phi : [0, T] \to \mathbb{R}^n$ be a witness for the LHS of the implication, and let $h : [0, T] \to \mathbb{R}$ be the valuation of the term e along ϕ, so $h(0) \geq 0 > h(T)$. As before, note that ϕ, h are both continuous functions.

We first show by induction on the structure of e that for $0 \leq t < T$, whenever $h(t) = 0$, then there exists $0 < \varepsilon \leq T - t$ such that the sign of h on the interval $(t, t + \varepsilon]$ is constant.

- **Case** $e := p$. Since $x' = f(x)$ is assumed to be a polynomial system, its solution ϕ is an analytic function. The valuation of polynomial p along ϕ is a polynomial of an analytic function, therefore, h is also analytic. By analyticity, there exists an open interval $a < t < b \leq T$ around $h(t) = 0$ where the Taylor series of h about t converges to h in that interval.

  If the series is uniformly zero, then h is uniformly zero in that interval, and so we may choose $\varepsilon \in (0, b - t)$ where the $h = 0$ is constant in $(t, t + \varepsilon)$.

  Otherwise, the Taylor series is not uniformly zero and h is locally dominated by its first non-zero term for a small enough choice of ε. Choosing such a ε yields an interval $(t, t + \varepsilon)$ where the sign of h is equal to the sign the first non-zero term in its Taylor series expansion about t.

- **Case** $e := \max(e_1, e_2)$. Let h_1, h_2 be the valuation of e_1, e_2 along ϕ respectively, then $h = \max(h_1, h_2)$. Since $h(t) = 0$, without loss of generality, assume $h_1 = 0, h_2 \leq 0$. If $h_2 < 0$, then by continuity, $h_2 < 0$ for a sufficiently small interval around t. Therefore, the local sign of $\max(h_1, h_2)$ around t is equal to the sign of h_1 around t, and the conclusion follows by the induction hypothesis. Otherwise, $h_1 = 0$ and $h_2 = 0$ so by the induction

[5] In fact, rational functions are also analytic if their denominators are non-zero in the domain of definition.

[6] Note that we have carefully chosen this axiom as it can be stated without soundness critical side conditions. An alternative is presented in Appendix B.

hypothesis, there exist $(t, t+\varepsilon_1], (t, t+\varepsilon_2]$ where the signs of h_1, h_2 are constant. Now, let $\tau = \min(\tau_1, \tau_2)$ so that both h_1, h_2 have constant signs on $(t, t+\varepsilon]$, a simple case analysis on the local signs of h_1, h_2 shows that the sign of h is also constant on $(t, t+\varepsilon]$.

- **Case** $e := \min(e_1, e_2)$. This is symmetric to the previous case.

Pick τ following the same construction as in the proof of $\text{IVT}_{\&}$. Following the same continuity argument, $h(\tau) = 0$. We showed that there is $\varepsilon > 0$ such that the sign of h is constant on the interval $(\tau, \tau+\varepsilon)$. It is easy to see that the sign must be $h < 0$, because otherwise, $h \geq 0$ for the interval, contradicting the choice of τ as the supremum.

We may now construct a witness for the RHS by first choosing ϕ restricted to the interval $[0, \tau]$ as the witness for the outer diamond modality. For the inner diamond modality, we noted that h is strictly negative on $(\tau, \tau+\varepsilon)$, therefore, we may use ϕ restricted to $[\tau, \tau+\frac{\varepsilon}{2}]$ as the witness. □

Note that $\text{IVT}_{\&}$ is implied by IVST because of the evolution domain constraints $e \geq 0, e \leq 0$, so we really only need to add the latter axiom. However, IVST requires analyticity of solutions, which restricts the type of functions that we may include as the RHS of ODEs.

A simple combination of $\text{IVT}_{\&}$ with $\text{reflect}_{\langle\cdot\rangle}$ yields the following corollary restricting backwards evolution.

Corollary 16 (Intermediate value theorem, backwards restriction)**.** *The following (reversed) version of $\text{IVT}_{\&}$ is sound:*

$$\text{IVT}_{\not\&}\ \ \exists x\,(e \succeq 0 \land \langle x' = f(x)\,\&\,Q\rangle e < 0) \to \exists x\,(e = 0 \land \langle x' = f(x)\,\&\,Q \land e \leq 0\rangle e < 0)$$

Proof.

$$\dfrac{\dfrac{\dfrac{*}{e(y) < 0, \langle y' = -f(y)\,\&\,Q \land e(y) \leq 0\rangle e(y) = 0 \vdash \exists x\,(e(x) < 0 \land \langle x' = -f(x)\,\&\,Q \land e(x) \leq 0\rangle e(x) = 0)}\exists\text{R}}{e(y) < 0, \langle y' = -f(y)\,\&\,Q\rangle e(y) \succeq 0 \vdash \exists x\,(e(x) < 0 \land \langle x' = -f(x)\,\&\,Q \land e(x) \leq 0\rangle e(x) = 0)}\text{IVT}_{\&}}{\exists x\,(e(x) < 0 \land \langle x' = -f(x)\,\&\,Q\rangle e(x) \succeq 0) \vdash \exists x\,(e(x) < 0 \land \langle x' = -f(x)\,\&\,Q \land e(x) \leq 0\rangle e(x) = 0)}\exists\text{L}}{\exists x\,(e(x) \succeq 0 \land \langle x' = f(x)\,\&\,Q\rangle e(x) < 0) \vdash \exists x\,(e(x) = 0 \land \langle x' = f(x)\,\&\,Q \land e(x) \leq 0\rangle e(x) < 0)}\text{reflect}_{\langle\cdot\rangle}$$

□

6.3 Frozen Predicates

As a first consequence of the new axioms, we show that time-frozen systems, i.e. where the time variable t is held fixed in the evolution domain constraint, cannot evolve. The significance of reasoning about frozen systems has been indicated elsewhere [Pla17b, MBT05]. The proof is generic for vectorial x, although it can be done component-wise as well.

Corollary 17 (Frozen evolution)**.** *The following is a derived axiom:*

$$\text{Frz}\ \ x = y \to [x' = f(x), t' = 1\,\&\,Q \land t = 0]x = y$$

Proof. The idea is to explicitly find a region where $(|x-y|^2)' \leq \epsilon, \epsilon > 0$. In that region, $|x-y|^2$ is bounded above by $\epsilon t = 0$, but that implies $x = y$. The rest follows since $x = y$ is the minimum point of $|x-y|^2$, i.e. $(|x-y|^2)' = 0 < \epsilon$. In detail:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(|x-y|^2 \leq \epsilon t = 0, (|x-y|^2)' = 0 < \epsilon)}{\epsilon > 0, t = 0, (|x-y|^2)' \leq \epsilon, |x-y|^2 \leq \epsilon t \vdash (|x-y|^2)' \neq \epsilon}\,\mathbb{R}}{\epsilon > 0 \vdash [x' = f(x), t' = 1 \,\&\, Q \wedge t = 0 \wedge (|x-y|^2)' \leq \epsilon \wedge |x-y|^2 \leq \epsilon t](|x-y|^2)' \neq \epsilon}\,\text{DW}}{\epsilon > 0 \vdash [x' = f(x), t' = 1 \,\&\, Q \wedge t = 0 \wedge (|x-y|^2)' \leq \epsilon](|x-y|^2)' \neq \epsilon}\,\text{DI,DC}}{\epsilon > 0, \langle x' = f(x), t' = 1 \,\&\, Q \wedge t = 0 \wedge (|x-y|^2)' \leq \epsilon\rangle(|x-y|^2)' = \epsilon \vdash \mathit{false}}\,\langle\cdot\rangle,\neg\text{L}}{\epsilon > 0, (|x-y|^2)' \leq \epsilon, \langle x' = f(x), t' = 1 \,\&\, Q \wedge t = 0\rangle(|x-y|^2)' > \epsilon \vdash \mathit{false}}\,\text{IVT}_{\&}}{\epsilon > 0, |x-y|^2 = 0, \langle x' = f(x), t' = 1 \,\&\, Q \wedge t = 0\rangle(|x-y|^2)' > \epsilon \vdash \mathit{false}}\,\text{cut},\mathbb{R}}{|x-y|^2 = 0, \langle x' = f(x), t' = 1 \,\&\, Q \wedge t = 0\rangle(|x-y|^2)' > 0 \vdash \mathit{false}}\,\mathbb{R},\text{B},\exists\text{L}}{|x-y|^2 = 0, \langle x' = f(x), t' = 1 \,\&\, Q \wedge t = 0\rangle|x-y|^2 > 0 \vdash \mathit{false}}\,\text{MVT}}{|x-y|^2 = 0 \vdash [x' = f(x), t' = 1 \,\&\, Q \wedge t = 0]|x-y|^2 = 0}\,[\cdot],\neg\text{R}}{x = y \vdash [x' = f(x), t' = 1 \,\&\, Q \wedge t = 0]x = y}\,\mathbb{R},\text{CE}$$

Note that $(|x-y|^2)' = 2(x-y)^T x'$, and this is abbreviated in the derivation above for clarity. The expanded form is used to prove $|x-y|^2 = 0 \to (|x-y|^2)' = 0$. □

By contextual equivalence and monotonicity [Pla17a], any predicate that holds before a frozen ODE continues to hold after the ODE:

Corollary 18 (Frozen predicates)**.** *The following is a derived axiom:*

$$\text{FrzP}\quad [?Q \wedge t = 0]p(x) \leftrightarrow [x' = f(x), t' = 1 \,\&\, Q \wedge t = 0]p(x)$$

Proof. "$\to$"

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{y = x, Q, t = 0, p(y) \vdash [x' = f(x), t' = 1 \,\&\, Q \wedge t = 0 \wedge y = x]p(x)}\,\text{DW}}{y = x, Q, t = 0, p(y) \vdash [x' = f(x), t' = 1 \,\&\, Q \wedge t = 0]p(x)}\,\text{Frz,DC}}{Q, t = 0, p(x) \vdash [x' = f(x), t' = 1 \,\&\, Q \wedge t = 0]p(x)}\,\mathbb{R},\exists\text{L}}{[?Q \wedge t = 0]p(x) \vdash [x' = f(x), t' = 1 \,\&\, Q \wedge t = 0]p(x)}\,\text{DW},[?],\to\text{L}$$

"$\leftarrow$"

$$\dfrac{*}{[x' = f(x), t' = 1 \,\&\, Q \wedge t = 0]p(x) \vdash [?Q \wedge t = 0]p(x)}\,\text{DW},[?]$$

□

6.4 Local Sign Conditions

Consider the following situation, where p is locally increasing because $\mathcal{L}_{f(x)}(p) > 0$, but $p \leq 0$ is in the evolution domain, preventing p from locally increasing.

$$\mathcal{L}_{f(x)}(p) > 0 \wedge p = 0 \wedge P \to [x' = f(x) \,\&\, Q \wedge p \leq 0]P$$

Intuitively, the ODE system is stuck because evolving for non-zero time would immediately violate the evolution domain constraint. Therefore, any predicate P that holds initially continues to hold after evolving the ODE.

This argument is central to our derivation of all semialgebraic invariants of ODEs, and we now prove a family of these local sign conditions.

Lemma 19 (Locally frozen predicates)**.** *The following are derived axioms:*

$$\text{frzSgn}\ \ \gamma^{=n}_{f(x)}(p) > 0 \land P \to [x' = f(x)\,\&\,Q \land p \leq 0]P$$

$$\text{frzSgn}_{\leq}\ \ \gamma^{\leq n}_{f(x)}(p) > 0 \land P \to [x' = f(x)\,\&\,Q \land p \leq 0]P$$

Proof. We can recursively apply $\lor$L to derive any instance of frzSgn$_{\leq}$ using the appropriate instance of frzSgn:

$$\lor\text{L}\frac{\text{frzSgn}\dfrac{*}{\gamma^{=0}_{f(x)}(p) > 0 \vdash [x' = f(x)\,\&\,Q \land p \leq 0]x_0 = 0} \quad \cdots \quad \text{frzSgn}\dfrac{*}{\gamma^{=n}_{f(x)}(p) > 0 \vdash [x' = f(x)\,\&\,Q \land p \leq 0]x_0 = 0}}{\gamma^{\leq n}_{f(x)}(p) > 0 \vdash [x' = f(x)\,\&\,Q \land p \leq 0]P}$$

To derive frzSgn, we assume that an appropriate clock, $x_0' = 1$, with $x_0 = 0$ initially is already present in the system. The idea is to show that x_0 is stuck at $x_0 = 0$, and apply FrzP. Note that the case with $n = 0$ is trivial because the evolution domain constraint is false initially.

$$\text{DC}\frac{x_0 = 0, \gamma^{=n}_{f(x)}(p) > 0 \vdash [x' = f(x)\,\&\,Q \land p \leq 0]x_0 = 0 \qquad \text{FrzP}\dfrac{*}{P \vdash [x' = f(x)\,\&\,Q \land p \leq 0 \land x_0 = 0]P}}{x_0 = 0, \gamma^{=n}_{f(x)}(p) > 0, P \vdash [x' = f(x)\,\&\,Q \land p \leq 0]P}$$

The next observation is that if $\mathcal{L}^{(n)}_{f(x)}(p)$ is positive, it must stay positive for a short amount of time. We may introduce this fact by reducing the left open premise down to a classical case split. We use the following modal equivalence in the cut step before case splitting with $\lor$L:

$$\langle\alpha\rangle P \lor \neg\langle\alpha\rangle P \iff \langle\alpha\rangle P \lor [\alpha]\neg P$$

$$\text{DI,DC}\frac{\dfrac{\lor\text{L}\dfrac{\text{①}\quad\text{②}}{\epsilon > 0, \cdots, \langle x' = f(x)\,\&\,\cdots\rangle \mathcal{L}^{(n)}_{f(x)}(p) \leq \epsilon \lor [x' = f(x)\,\&\,\cdots]\mathcal{L}^{(n)}_{f(x)}(p) > \epsilon \vdash [x' = f(x)\,\&\,\cdots]x_0 = 0}}{\epsilon > 0, x_0 = 0, \mathcal{L}^{(n)}_{f(x)}(p) > \epsilon, \bigwedge_{i=0}^{n-1} \mathcal{L}^{(i)}_{f(x)}(p) = 0 \vdash [x' = f(x)\,\&\,Q \land p \leq 0 \land x_0 \geq 0]x_0 = 0}\,\text{cut}}{x_0 = 0, \mathcal{L}^{(n)}_{f(x)}(p) > 0, \bigwedge_{i=0}^{n-1} \mathcal{L}^{(i)}_{f(x)}(p) = 0 \vdash [x' = f(x)\,\&\,Q \land p \leq 0 \land x_0 \geq 0]x_0 = 0}\,\mathbb{R}}{x_0 = 0, \gamma^{=n}_{f(x)}(p) > 0 \vdash [x' = f(x)\,\&\,Q \land p \leq 0 \land x_0 \geq 0]x_0 = 0}}{x_0 = 0, \gamma^{=n}_{f(x)}(p) > 0 \vdash [x' = f(x)\,\&\,Q \land p \leq 0]x_0 = 0}$$

For the right disjunct (②), we add $\mathcal{L}^{(n)}_{f(x)}(p) \geq \epsilon$ into the evolution domain constraint with DC.

$$\text{DC}\frac{\epsilon > 0, \cdots \vdash [x' = f(x)\,\&\,\cdots \land \mathcal{L}^{(n)}_{f(x)}(p) \geq \epsilon]x_0 = 0}{\epsilon > 0, \cdots, [x' = f(x)\,\&\,\cdots]\mathcal{L}^{(n)}_{f(x)}(p) > \epsilon \vdash [x' = f(x)\,\&\,\cdots]x_0 = 0}$$

For the left disjunct (①), we obtain a similar evolution domain constraint using $\text{IVT}_{\&}$ instead.

$$\text{IVT}_{\&}\,\dfrac{\langle\cdot\rangle,\neg\text{L},\text{M}[\cdot]\,\dfrac{\epsilon>0,\cdots\vdash[x'=f(x)\,\&\,\cdots\wedge\mathcal{L}^{(n)}_{f(x)}(p)\geq\epsilon]\mathcal{L}^{(n)}_{f(x)}(p)>\epsilon}{\epsilon>0,\cdots,\langle x'=f(x)\,\&\,\cdots\wedge\mathcal{L}^{(n)}_{f(x)}(p)\geq\epsilon\rangle\mathcal{L}^{(n)}_{f(x)}(p)=\epsilon\vdash \mathit{false}}}{\epsilon>0,\mathcal{L}^{(n)}_{f(x)}(p)>\epsilon,\cdots,\langle x'=f(x)\,\&\,\cdots\rangle\mathcal{L}^{(n)}_{f(x)}(p)\leq\epsilon\vdash \mathit{false}}$$

The next step for both disjuncts is to apply repeated integration using the bound that we have just introduced into the evolution domain. This eventually allows us to derive $x_0 = 0$. In the left disjunct, we need an additional FrzP step to show that $\mathcal{L}^{(k)}_{f(x)}(p) > \epsilon$ remains true in the postcondition. Since the proofs for both disjuncts are similar, we will write R here for a predicate that has to be frozen across the evolution.

$$\text{DI,DC}\,\dfrac{\text{DI,DC}\,\dfrac{\cdots}{\epsilon>0,x_0=0,\bigwedge_{i=0}^{n-1}\mathcal{L}^{(i)}_{f(x)}(p)=0,R\vdash[x'=f(x)\,\&\,Q\wedge p\leq 0\wedge x_0\geq 0\wedge\mathcal{L}^{(n)}_{f(x)}(p)\geq\epsilon,\mathcal{L}^{(n-1)}_{f(x)}(p)\geq\epsilon x_0]R}}{\epsilon>0,x_0=0,\bigwedge_{i=0}^{n-1}\mathcal{L}^{(i)}_{f(x)}(p)=0,R\vdash[x'=f(x)\,\&\,Q\wedge p\leq 0\wedge x_0\geq 0\wedge\mathcal{L}^{(n)}_{f(x)}(p)\geq\epsilon]R}$$

$$\text{DC,DW,}\mathbb{R}\,\dfrac{\text{FrzP}\,\dfrac{*}{\epsilon>0,x_0=0,\bigwedge_{i=0}^{n-1}\mathcal{L}^{(i)}_{f(x)}(p)=0,R\vdash[x'=f(x)\,\&\,Q\wedge p\leq 0\wedge x_0\geq 0\wedge\cdots\wedge p\geq\epsilon\frac{x_0^k}{k!}\wedge x_0=0]R}}{\epsilon>0,x_0=0,\bigwedge_{i=0}^{n-1}\mathcal{L}^{(i)}_{f(x)}(p)=0,R\vdash[x'=f(x)\,\&\,Q\wedge p\leq 0\wedge x_0\geq 0\wedge\cdots\wedge p\geq\epsilon\frac{x_0^k}{k!}]R}$$

□

In most cases, we shall use the following immediate corollaries of $\text{frzSgn}_{\leq}$ with diamond modalities.

Corollary 20 (Local sign conditions)**.** *The following derived rules are sound:*

$$\text{frzSgn}_{\langle\cdot\rangle}\;\dfrac{*}{\gamma^{\leq n}_{f(x)}(p)>0,P,\langle x'=f(x)\,\&\,Q\wedge p\leq 0\rangle\neg P\vdash \mathit{false}}$$

$$\text{LocSgn}\;\dfrac{*}{\gamma^{\leq n}_{f(x)}(p)>0,\langle x'=f(x)\,\&\,Q\wedge p\leq 0\rangle p<0\vdash \mathit{false}}$$

Proof. $\text{frzSgn}_{\langle\cdot\rangle}$ follows by negating the box modality in $\text{frzSgn}_{\leq}$. LocSgn follows by instantiating $P \overset{\text{def}}{=} p \geq 0$ because $\gamma^{\leq n}_{f(x)}(p) > 0$ implies $p \geq 0$. □

We will need to generalize to a situation where there are sign conditions on multiple p_i, but where the evolution domain constraint is disjunctive. For simplicity, the statement and proof here is for a simultaneous condition on two polynomials, p, q, although the technique generalizes to any p_i. Note that we have written $\preceq$ instead of $\leq$ here because the proof works even if the comparison operator was $<$ for some of the p_i.

Corollary 21 (Simultaneous locally frozen predicates)**.** *The following are derived axioms:*

$$\text{frzSgn}\;\;\gamma^{=n}_{f(x}(p)>0\wedge\gamma^{=m}_{f(x)}(q)>0\wedge P\to[x'=f(x)\,\&\,Q\wedge(p\preceq 0\vee q\preceq 0)]P$$

$$\text{frzSgn}_{\leq}\;\;\gamma^{\leq n}_{f(x}(p)>0\wedge\gamma^{\leq m}_{f(x)}(q)>0\wedge P\to[x'=f(x)\,\&\,Q\wedge(p\preceq 0\vee q\preceq 0)]P$$

Proof. As before, it is sufficient for us to show frzSgn because frzSgn$_{\leq}$ follows by taking disjunctive combinations with $\vee$L. The proof strategy is also very similar: we show that $x_0 = 0$ is frozen and apply FrzP. For convenience, we use the same ϵ here to bound both p, q.

$$\text{IVT}_{\&},\text{DC}\ \frac{\epsilon > 0, x_0 = 0, \bigwedge_{i=0}^{n-1} \mathcal{L}^{(i)}_{f(x)}(p) = 0, \bigwedge_{i=0}^{m-1} \mathcal{L}^{(i)}_{f(x)}(q) = 0, R \vdash [x' = f(x) \,\&\, \cdots \wedge \mathcal{L}^{(n)}_{f(x)}(p) \geq \epsilon \wedge \mathcal{L}^{(m)}_{f(x)}(q) \geq \epsilon]R}{\epsilon > 0, \cdots, \mathcal{L}^{(n)}_{f(x)}(p) > \epsilon, \mathcal{L}^{(m)}_{f(x)}(q) > \epsilon \vdash [x' = f(x) \,\&\, Q \wedge (p \preceq 0 \vee q \preceq 0) \wedge x_0 \geq 0]x_0 = 0}$$

$$\mathbb{R}\ \frac{\epsilon > 0, \cdots, \mathcal{L}^{(n)}_{f(x)}(p) > \epsilon, \mathcal{L}^{(m)}_{f(x)}(q) > \epsilon \vdash [x' = f(x) \,\&\, Q \wedge (p \preceq 0 \vee q \preceq 0) \wedge x_0 \geq 0]x_0 = 0}{x_0 = 0, \cdots, \mathcal{L}^{(n)}_{f(x)}(p) > 0, \mathcal{L}^{(m)}_{f(x)}(q) > 0 \vdash [x' = f(x) \,\&\, Q \wedge (p \preceq 0 \vee q \preceq 0) \wedge x_0 \geq 0]x_0 = 0}$$

$$\frac{x_0 = 0, \gamma^{=n}_{f(x)}(p) > 0, \gamma^{=m}_{f(x)}(q) > 0 \vdash [x' = f(x) \,\&\, Q \wedge (p \preceq 0 \vee q \preceq 0) \wedge x_0 \geq 0]x_0 = 0}{}$$

$$\text{DI,DC}\ \frac{x_0 = 0, \gamma^{=n}_{f(x)}(p) > 0, \gamma^{=m}_{f(x)}(q) > 0 \vdash [x' = f(x) \,\&\, Q \wedge (p \preceq 0 \vee q \preceq 0)]x_0 = 0}{}$$

$$\text{DC,FrzP}\ \frac{x_0 = 0, \gamma^{=n}_{f(x)}(p) > 0, \gamma^{=m}_{f(x)}(q) > 0, P \vdash [x' = f(x) \,\&\, Q \wedge (p \preceq 0 \vee q \preceq 0)]P}{}$$

The IVT$_{\&}$,DC step above applies the same case split technique twice to introduce both $\mathcal{L}^{(n)}_{f(x)}(p) \geq \epsilon$ and $\mathcal{L}^{(m)}_{f(x)}(q) \geq \epsilon$ into the evolution domain constraints. We again write R for an arbitrary predicate that needs to be preserved across frozen evolution of the ODE; there are 4 cases of the same shape arising from the case splits.

From here, we apply repeated integration to simultaneously bound both p, q. This allows us to add $x_0 = 0$ into the evolution domain constraints, and apply FrzP.

$$\text{FrzP}\ \frac{*}{\epsilon > 0, x_0 = 0, \cdots, R \vdash [x' = f(x) \,\&\, Q \wedge (p \preceq 0 \vee q \preceq 0) \wedge x_0 \geq 0 \wedge \cdots p \geq \epsilon \tfrac{x_0^n}{n!} \wedge q \geq \epsilon \tfrac{x_0^m}{m!} \wedge x_0 = 0]R}$$

$$\text{DC,DW,}\mathbb{R}\ \frac{\epsilon > 0, x_0 = 0, \cdots, R \vdash [x' = f(x) \,\&\, Q \wedge (p \preceq 0 \vee q \preceq 0) \wedge x_0 \geq 0 \wedge \cdots p \geq \epsilon \tfrac{x_0^n}{n!} \wedge q \geq \epsilon \tfrac{x_0^m}{m!} \wedge x_0 = 0]R}{}$$

$$\text{DI,DC}\ \frac{\epsilon > 0, x_0 = 0, \cdots, R \vdash [x' = f(x) \,\&\, \cdots \wedge (p \preceq 0 \vee q \preceq 0) \wedge x_0 \geq 0 \wedge p \geq \epsilon \tfrac{x_0^n}{n!} \wedge q \geq \epsilon \tfrac{x_0^m}{m!}]R}{}$$

$$\text{DI,DC}\ \frac{\cdots}{}$$

$$\text{DI,DC}\ \frac{\epsilon > 0, x_0 = 0, \bigwedge_{i=0}^{n-1} \mathcal{L}^{(i)}_{f(x)}(p) = 0, \cdots, R \vdash [x' = f(x) \,\&\, \cdots \wedge \mathcal{L}^{(m)}_{f(x)}(q) \geq \epsilon \wedge \mathcal{L}^{(n-1)}_{f(x)}(p) \geq \epsilon x_0]R}{}$$

$$\text{DI,DC}\ \frac{\epsilon > 0, x_0 = 0, \bigwedge_{i=0}^{n-1} \mathcal{L}^{(i)}_{f(x)}(p) = 0, \cdots, R \vdash [x' = f(x) \,\&\, \cdots \mathcal{L}^{(n)}_{f(x)}(p) \geq \epsilon \wedge \mathcal{L}^{(m)}_{f(x)}(q) \geq \epsilon]R}{}$$

□

As before, we will often refer to the diamond modality version of frzSgn$_{\leq}$ in the sequel.

Corollary 22 (Simultaneous local sign conditions)**.** *The following derivation is sound:*

$$\text{frzSgn}_{\langle\cdot\rangle}\ \frac{*}{\gamma^{\leq n}_{f(x)}(p) > 0, \gamma^{\leq m}_{f(x)}(q) > 0, P, \langle x' = f(x) \,\&\, Q \wedge (p \preceq 0 \vee q \preceq 0)\rangle \neg P \vdash \mathit{false}}$$

6.5 Invariant Inequalities

We are now ready for the instance of In with a single inequality $p \geq 0$.

Lemma 23 (In, $p \geq 0$)**.** *The In proof rule for invariants of the form $p \geq 0$ is derivable using IVT$_{\otimes}$,DRI,LocSgn, which are in turn derivable from vectorial DG with IVT$_{\&}$,$'$*.*

Proof. The first part of the deduction uses IVT$_{\otimes}$ to focus on the last zero crossing, then the right In premise is applied for a case split. The left premise after $\vee$L closes immediately by LocSgn. The remaining open premise is abbreviated by ①.

$$\text{LocSgn}\dfrac{\dfrac{*}{p=0,\gamma^{\leq N-1}_{f(x)}(p)>0,\langle x'=f(x)\,\&\,p\leq 0\rangle p<0\vdash \mathit{false}}\ ①}{\vee\text{L}\dfrac{p=0,\gamma^{\leq N-1}_{f(x)}(p)>0\vee\bigwedge_{i=0}^{N-1}\mathcal{L}^{(i)}_{f(x)}(p)=0,\langle x'=f(x)\,\&\,p\leq 0\rangle p<0\vdash \mathit{false}}{\text{assum}\dfrac{p=0,\langle x'=f(x)\,\&\,p\leq 0\rangle p<0\vdash \mathit{false}}{\text{IVT}_{\gg},\exists\text{L}\dfrac{p\geq 0,\langle x'=f(x)\rangle p<0\vdash \mathit{false}}{[\cdot],\neg\text{R}\dfrac{}{p\geq 0\vdash[x'=f(x)]p\geq 0}}}}}$$

The remaining premise (①) closes by DRI:

$$\text{DRI}\dfrac{(\mathcal{L}^{(N)}_{f(x)}(p)=g_{N-1}\mathcal{L}^{(N-1)}_{f(x)}(p)+\cdots+g_1\mathcal{L}_{f(x)}(p)+g_0p)}{\text{M}[\cdot]\dfrac{\bigwedge_{i=0}^{N-1}\mathcal{L}^{(i)}_{f(x)}(p)=0\vdash[x'=f(x)\,\&\,p\leq 0]\bigwedge_{i=0}^{N-1}\mathcal{L}^{(i)}_{f(x)}(p)=0}{\langle\cdot\rangle,\neg\text{L}\dfrac{p=0,\bigwedge_{i=1}^{N-1}\mathcal{L}^{(i)}_{f(x)}(p)=0\vdash[x'=f(x)\,\&\,p\leq 0]p\geq 0}{p=0,\bigwedge_{i=1}^{N-1}\mathcal{L}^{(i)}_{f(x)}(p)=0,\langle x'=f(x)\,\&\,p\leq 0\rangle p<0\vdash \mathit{false}}}}$$

□

The last proof step with DRI is of special interest, because it could be done at the start of the derivation *before* any subsequent proof steps. This observation will help to streamline all of our subsequent proofs. The following is a simple consequence of VDbx$_{\neq}$:

Corollary 24 (Disequilibria)**.** *The following is sound:*

$$\text{Diseq}\quad \bigvee_{i=0}^{N_p-1}\mathcal{L}^{(i)}_{f(x)}(p)\neq 0\rightarrow[x'=f(x)\,\&\,Q]\bigvee_{i=0}^{N_p-1}\mathcal{L}^{(i)}_{f(x)}(p)\neq 0$$

where $\mathcal{L}^{(N)}_{f(x)}(p)=g_{N-1}\mathcal{L}^{(N-1)}_{f(x)}(p)+\cdots+g_1\mathcal{L}_{f(x)}(p)+g_0p$.

Proof. We make the same choice of cofactor matrix $G\overset{\text{def}}{=}\begin{pmatrix} g_{N-1} & \cdots & g_1 & g_0\\ 1 & \ldots & 0 & 0\\ 0 & \ddots & 0 & 0\\ 0 & \ldots & 1 & 0\end{pmatrix}$ as in the derivation of DRI from VDbx. Let $\vec{l}\overset{\text{def}}{=}\begin{pmatrix}\mathcal{L}^{(N-1)}_{f(x)}(p)\\ \vdots\\ \mathcal{L}_{f(x)}(p)\\ p\end{pmatrix}$ be the vector of Lie derivatives.

$$\text{cut},\mathbb{R}\dfrac{\text{M}[\cdot]\dfrac{\text{VDbx}_{\neq}\dfrac{\dfrac{*}{Q\vdash[x':=f(x)](\vec{l}(x))'=G(x)\vec{l}(x)}}{\vec{l}(x)\cdot\vec{l}(x)>0\vdash[x'=f(x)\,\&\,Q]\vec{l}(x)\cdot\vec{l}(x)>0}}{\vec{l}(x)\cdot\vec{l}(x)>0\vdash[x'=f(x)\,\&\,Q]\bigvee_{i=0}^{N_p-1}\mathcal{L}^{(i)}_{f(x)}(p)\neq 0}}{\bigvee_{i=0}^{N_p-1}\mathcal{L}^{(i)}_{f(x)}(p)\neq 0\vdash[x'=f(x)\,\&\,Q]\bigvee_{i=0}^{N_p-1}\mathcal{L}^{(i)}_{f(x)}(p)\neq 0}$$

□

Intuitively, Diseq shows that any polynomial that does not already start at equilibrium can never reach equilibrium. This leads us to the following remark on our derivations.

Remark 25 (Removing equilibria)**.** *To show the invariance of a semialgebraic formula P, i.e.*

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

where some of the polynomials in P are (possibly) at equilibrium, it is sufficient to consider a set of open premises P_i, each of the form:

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

where we may additionally assume that none of the polynomials appearing in each P_i are at equilibrium. Furthermore, if the LZZ premises hold for P, then they continue to hold for P_i.

Proof. Consider a semialgebraic formula $P \equiv \bigvee_{i=0}^{M} \big(p \geq 0 \wedge \bigwedge_{j=0}^{m(i)} p_{ij} \geq 0 \wedge \bigwedge_{j=0}^{n(i)} q_{ij} > 0\big)$. Here, p is a polynomial that might be at equilibrium – note that none of q_{ij} can be at equilibrium because they must start at $q_{ij} > 0$ in order to satisfy the invariant.

Let $P_{p=0} \overset{\text{def}}{=} \bigvee_{i=0}^{M} \big(\bigwedge_{j=0}^{m(i)} p_{ij} \geq 0 \wedge \bigwedge_{j=0}^{n(i)} q_{ij} > 0\big)$. We classically case split on whether p starts at equilibrium, ① abbreviates the left premise after applying $\vee$L:

$$\vee\text{L}\,\dfrac{\dfrac{\textcircled{1}}{P, \bigwedge_{j=0}^{N-1} p^{(j)} = 0 \vdash [x' = f(x) \,\&\, Q]P} \quad \text{DC,Diseq}\,\dfrac{P \vdash [x' = f(x) \,\&\, Q \wedge \bigvee_{i=0}^{N_p - 1} \mathcal{L}_{f(x)}^{(i)}(p) \neq 0]P}{P, \neg\bigwedge_{j=0}^{N-1} p^{(j)} = 0 \vdash [x' = f(x) \,\&\, Q]P}}{P, \bigwedge_{j=0}^{N-1} p^{(j)} = 0 \vee \neg\bigwedge_{j=0}^{N-1} p^{(j)} = 0 \vdash [x' = f(x) \,\&\, Q]P}}{P \vdash [x' = f(x) \,\&\, Q]P}$$

The open right disjunct has been reduced to an invariant where p does not start at equilibrium, and additionally, Diseq allows us to add this fact to the evolution domain constraint. We may continue on the right, e.g. with LZZ, using this additional assumption.

The left disjunct (①) removes p from consideration entirely using DRI:

$$\text{DRI}\,\dfrac{\text{DW,M}[\cdot]\,\dfrac{P_{p=0} \vdash [x' = f(x) \,\&\, Q \wedge p = 0]P_{p=0}}{P, \bigwedge_{j=0}^{N-1} p^{(j)} = 0 \vdash [x' = f(x) \,\&\, Q \wedge p = 0]P}}{P, \bigwedge_{j=0}^{N-1} p^{(j)} = 0 \vdash [x' = f(x) \,\&\, Q]P}$$

In this case, $P_{p=0}$ has one fewer polynomial (possibly) at equilibrium. We may also check that if the LZZ premises hold for P initially, then the premises of LZZ continue to hold for $P_{p=0}$. By recursively applying this derivation for all polynomials p that appear in P on the open premises, we eventually reduce to open premises where all of the polynomials involved are not at equilibrium. □

An important consequence of removing equilibria is that we may, without loss of generality, assume that $\bigvee_{i=0}^{N_p - 1} \mathcal{L}_{f(x)}^{(i)}(p) \neq 0$ is in the evolution domain for all polynomials p in the invariant

under consideration. Under this assumption, we have:

$$\begin{aligned}\mathrm{In}_{f(x)}(p \geq 0) &\iff \gamma^{\leq N-1}_{f(x)}(p) > 0 \vee \bigwedge_{i=0}^{N_p-1} \mathcal{L}^{(i)}_{f(x)}(p) = 0\\ &\iff \gamma^{\leq N-1}_{f(x)}(p) > 0\\ &\iff \mathrm{In}_{f(x)}(p > 0)\end{aligned}$$

Formally, we use DI,DW together with the evolution domain constraint in order to apply the above equivalence wherever $\mathrm{In}_{f(x)}(p \geq 0)$ occurs. We omit these steps and directly use the equivalence in the sequel.

6.6 Closed or Open Semialgebraic Invariants

Any closed semialgebraic formula may be written as $P \equiv \bigvee_{i=0}^{M} \bigwedge_{j=0}^{m(i)} p_{ij} \geq 0$.

$$\begin{aligned}\mathrm{In}_{f(x)}(\bigvee_{i=0}^{M}\bigwedge_{j=0}^{m(i)} p_{ij} \geq 0) &\iff \bigvee_{i=0}^{M}\bigwedge_{j=0}^{m(i)} \mathrm{In}_{f(x)}(p_{ij} \geq 0)\\ &\iff \bigvee_{i=0}^{M}\bigwedge_{j=0}^{m(i)} \gamma^{\leq N_{ij}-1}_{f(x)}(p_{ij}) > 0\end{aligned}$$

Lemma 26 (In, $\bigvee_{i=0}^{M} \bigwedge_{j=0}^{m(i)} p_{ij} \geq 0$)**.** *The In proof rule for closed semialgebraic invariants is derivable using IVT$_{\otimes}$,DRI,frzSgn$_{\langle\cdot\rangle}$, which are in turn derivable from vectorial DG with IVT$_{\&}$,$'^*$.*

Proof. We rely on the equivalence $\bigvee_{i=0}^{M} \bigwedge_{j=0}^{m(i)} p_{ij} \geq 0 \iff \max_{i=0}^{M} \min_{j=0}^{m(i)} p_{ij} \geq 0$. Introducing the generalized term involving $\max, \min$ allows us to apply IVT$_{\otimes}$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\bigvee_{i=0}^{M} \bigwedge_{j=0}^{m(i)} \gamma^{\leq N_{ij}-1}_{f(x)}(p_{ij}) > 0, \langle x' = f(x) \,\&\, \bigwedge_{i=0}^{M} \bigvee_{j=0}^{m(i)} p_{ij} \leq 0\rangle \bigwedge_{i=0}^{M} \bigvee_{j=0}^{m(i)} p_{ij} < 0 \vdash \mathit{false}}{\max_{i=0}^{M} \min_{j=0}^{m(i)} p_{ij} = 0, \langle x' = f(x) \,\&\, \max_{i=0}^{M} \min_{j=0}^{m(i)} p_{ij} \leq 0\rangle \max_{i=0}^{M} \min_{j=0}^{m(i)} p_{ij} < 0 \vdash \mathit{false}}\,\mathbb{R}\text{,assum,CE}}{\max_{i=0}^{M} \min_{j=0}^{m(i)} p_{ij} \geq 0, \langle x' = f(x)\rangle \max_{i=0}^{M} \min_{j=0}^{m(i)} p_{ij} < 0 \vdash \mathit{false}}\,\mathrm{IVT}_{\otimes},\exists\mathrm{L}}{\max_{i=0}^{M} \min_{j=0}^{m(i)} p_{ij} \geq 0 \vdash [x' = f(x)] \max_{i=0}^{M} \min_{j=0}^{m(i)} p_{ij} \geq 0}\,[\cdot],\neg\mathrm{R}}{\bigvee_{i=0}^{M} \bigwedge_{j=0}^{m(i)} p_{ij} \geq 0 \vdash [x' = f(x)] \bigvee_{i=0}^{M} \bigwedge_{j=0}^{m(i)} p_{ij} \geq 0}\,\mathbb{R}\text{,CE}$$

We case split on the disjunction using $\vee$L, and for the case resulting from index i, we finish with the following derivation:

$$\dfrac{\dfrac{*}{\bigwedge_{j=0}^{m(i)} \gamma^{\leq N_{ij}-1}_{f(x)}(p_{ij}) > 0, \langle x' = f(x) \,\&\, \bigwedge_{i=0}^{M} \bigvee_{j=0}^{m(i)} p_{ij} \leq 0\rangle \bigvee_{j=0}^{m(i)} p_{ij} < 0 \vdash \mathit{false}}\,\mathrm{frzSgn}_{\langle\cdot\rangle}}{\bigwedge_{j=0}^{m(i)} \gamma^{\leq N_{ij}-1}_{f(x)}(p_{ij}) > 0, \langle x' = f(x) \,\&\, \bigwedge_{i=0}^{M} \bigvee_{j=0}^{m(i)} p_{ij} \leq 0\rangle \bigwedge_{i=0}^{M} \bigvee_{j=0}^{m(i)} p_{ij} < 0 \vdash \mathit{false}}\,\langle\rangle\wedge$$

Note that frzSgn$_{\langle\cdot\rangle}$ applies here because $\bigvee_{j=0}^{m(i)} p_{ij} \leq 0$ is implied by the evolution domain constraint, and because $\bigwedge_{j=0}^{m(i)} \gamma^{\leq N_{ij}-1}_{f(x)}(p_{ij}) > 0$ implies $\bigwedge_{j=0}^{m(i)} p_{ij} \geq 0$, which, when negated, yields $\bigvee_{j=0}^{m(i)} p_{ij} < 0$. □

If instead the invariant P under consideration was an open semialgebraic set, then its complement, $\neg P$ is closed and semialgebraic. Therefore, we may apply the derivation above after using reflect to change the invariant under consideration to $\neg P$.

6.7 Semialgebraic Invariants

Let $P \equiv \bigvee_{i=0}^{M} \big(\bigwedge_{j=0}^{m(i)} p_{ij} \geq 0 \wedge \bigwedge_{j=0}^{n(i)} q_{ij} > 0 \big)$ be semialgebraic, notice that we are unable to encode P directly using $\max, \min$, unlike in the previous section. However, by careful case splits, we may derive the proof rule with the help of the IVST axiom.

Lemma 27 (In)**.** *The In proof rule for semialgebraic invariants is derivable using IVST, along with DRI,frzSgn$_{\langle\cdot\rangle}$, which are in turn derivable from vectorial DG with '*.*

Proof. By propositional rearrangement, we have

$$\begin{aligned}
\neg P &\iff \neg \bigvee_{i=0}^{M} \big(\bigwedge_{j=0}^{m(i)} p_{ij} \geq 0 \wedge \bigwedge_{j=0}^{n(i)} q_{ij} > 0 \big) \\
&\iff \bigwedge_{i=0}^{M} \big(\bigvee_{j=0}^{m(i)} p_{ij} < 0 \vee \bigvee_{j=0}^{n(i)} q_{ij} \leq 0 \big) \\
&\iff \bigvee_{i=0}^{N} \big(\bigwedge_{j=0}^{a(i)} r_{ij} < 0 \wedge \bigwedge_{j=0}^{b(i)} s_{ij} \leq 0 \big)
\end{aligned}$$

In the last step, we distribute conjunctions over disjunctions and rename the resulting polynomials accordingly. Note that r_{ij}, s_{ij} are from the same set of polynomials as p_{ij}, q_{ij} respectively. Following the same rearrangement, we also have:

$$\begin{aligned}
\text{In}_{-f(x)}(\neg P) &\iff \neg \text{In}_{-f(x)}(P) \\
&\iff \bigvee_{i=0}^{N} \big(\bigwedge_{j=0}^{a(i)} \text{In}_{-f(x)}(r_{ij} < 0) \wedge \bigwedge_{j=0}^{b(i)} \text{In}_{-f(x)}(s_{ij} \leq 0) \big) \\
&\iff \bigvee_{i=0}^{N} \big(\bigwedge_{j=0}^{a(i)} \text{In}_{-f(x)}(r_{ij} < 0) \wedge \bigwedge_{j=0}^{b(i)} \text{In}_{-f(x)}(s_{ij} < 0) \big) \\
&\iff \bigvee_{i=0}^{N} \big(\bigwedge_{j=0}^{c(i)} \text{In}_{-f(x)}(t_{ij} > 0) \big)
\end{aligned}$$

Since we assumed that none of polynomials in P are at equilibrium, we also have that none of r_{ij}, s_{ij} are at equilibrium. The second-to-last equivalence uses this to replace $\text{In}_{-f(x)}(s_{ij} \leq 0)$ with $\text{In}_{-f(x)}(s_{ij} < 0)$. The last equivalence further combines r_{ij}, s_{ij} for brevity in our derivation below.

An approximation of the interior of $\neg P$ is given by:

$$\text{int}(\neg P) \stackrel{\text{def}}{=} \bigvee_{i=0}^{N} \big(\bigwedge_{j=0}^{a(i)} r_{ij} < 0 \wedge \bigwedge_{j=0}^{b(i)} s_{ij} < 0 \big)$$

Following the re-indexing above, we may equivalently write:

$$\text{int}(\neg P) \iff \bigvee_{i=0}^{N} \big(\bigwedge_{j=0}^{c(i)} t_{ij} < 0 \big)$$

The first proof step is to case split classically on whether we enter $\text{int}(\neg P)$.

$$\dfrac{\dfrac{P, \langle x' = f(x)\rangle \neg P, \langle x' = f(x)\rangle \text{int}(\neg P) \vdash \mathit{false} \quad P, \langle x' = f(x)\rangle \neg P, [x' = f(x)] \neg \text{int}(\neg P) \vdash \mathit{false}}{P, \langle x' = f(x)\rangle \neg P, \langle x' = f(x)\rangle \text{int}(\neg P) \vee [x' = f(x)] \neg \text{int}(\neg P) \vdash \mathit{false}}\,\vee\text{L}}{P, \langle x' = f(x)\rangle \neg P \vdash \mathit{false}}\,\text{cut}}{P \vdash [x' = f(x)] P}\,[\cdot],\neg\text{L}$$

For the right branch, we immediately DC $\neg\text{int}(\neg P)$ into the evolution domain constraint. In the re-indexed form, the last line closes by the same derivation we showed previously.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{\neg P, \bigvee_{i=0}^{N} \bigwedge_{j=0}^{c(i)} \gamma^{\leq N^t_{ij}}_{-f(x)}(t_{ij}) > 0, \langle x' = -f(x) \,\&\, \bigwedge_{i=0}^{N} \bigvee_{j=0}^{c(i)} t_{ij} \leq 0\rangle P \vdash \mathit{false}}\,\text{frzSgn}_{\langle\cdot\rangle},\vee\text{L}}{\neg P, \bigvee_{i=0}^{N} \bigwedge_{j=0}^{c(i)} \text{In}_{-f(x)}(t_{ij} > 0), \langle x' = -f(x) \,\&\, \bigwedge_{i=0}^{N} \bigvee_{j=0}^{c(i)} t_{ij} \leq 0\rangle P \vdash \mathit{false}}}{\neg P, \text{In}_{-f(x)}(\neg P), \langle x' = -f(x) \,\&\, \neg\text{int}(\neg P)\rangle P \vdash \mathit{false}}\,\text{assum}}{\neg P, \langle x' = -f(x) \,\&\, \neg\text{int}(\neg P)\rangle P \vdash \mathit{false}}\,\text{reflect}_{\langle\cdot\rangle}}{P, \langle x' = f(x) \,\&\, \neg\text{int}(\neg P)\rangle \neg P \vdash \mathit{false}}\,\text{DC}}{P, \langle x' = f(x)\rangle \neg P, [x' = f(x)] \neg\text{int}(\neg P) \vdash \mathit{false}}$$

It is useful to note here that $P \iff \bigwedge_{i=0}^{N} \big(\bigvee_{j=0}^{a(i)} r_{ij} < 0 \vee \bigvee_{j=0}^{b(i)} s_{ij} \leq 0 \big)$, and so the evolution domain we introduced plays the role of an approximation for the topological closure $\overline{P}$.

For the left branch, we note that $\text{int}(\neg P)$ is expressible using $\max, \min$ as:

$$\text{int}(\neg P) \iff \min_{i=0}^{N} \max \big(\max_{j=0}^{a(i)} r_{ij}, \max_{j=0}^{b(i)} s_{ij} \big) < 0$$

For brevity in the derivations, we write $T := \min_{i=0}^{N} \max \big(\max_{j=0}^{a(i)} r_{ij}, \max_{j=0}^{b(i)} s_{ij} \big)$. Furthermore, we have:

$$\begin{aligned}
P &\iff \neg\neg P \\
&\iff \bigwedge_{i=0}^{N} \big(\bigvee_{j=0}^{a(i)} r_{ij} \geq 0 \vee \bigwedge_{j=0}^{b(i)} s_{ij} > 0 \big) \\
&\implies \bigwedge_{i=0}^{N} \big(\bigvee_{j=0}^{a(i)} r_{ij} \geq 0 \vee \bigwedge_{j=0}^{b(i)} s_{ij} \geq 0 \big) \\
&\iff \neg\text{int}(\neg P) \iff T \geq 0
\end{aligned}$$

We may thus cut $T \geq 0$ immediately on the left of the sequent, allowing us to setup an application of IVST.

$$\text{cut}\;\dfrac{\text{CE}\;\dfrac{\text{IVST}\;\dfrac{P, \langle x' = f(x)\,\&\,T \geq 0\rangle\langle x' = f(x)\,\&\,T \leq 0\rangle T < 0 \vdash \mathit{false}}{P, T \geq 0, \langle x' = f(x)\rangle T < 0 \vdash \mathit{false}}}{P, T \geq 0, \langle x' = f(x)\rangle \text{int}(\neg P) \vdash \mathit{false}}}{P, \langle x' = f(x)\rangle \text{int}(\neg P) \vdash \mathit{false}}$$

Next, we use CE to classically case split in the middle of the diamond modalities. By expanding out the abbreviation T, we have already shown that the left branch closes earlier in this section. We write ① for the remaining open premise.

$$\text{CE}\;\dfrac{\langle\rangle\vee,\vee\text{L}\;\dfrac{\langle\rangle\wedge\;\dfrac{\dfrac{}{P, \langle x' = f(x)\,\&\,T \geq 0\rangle \neg P \vdash \mathit{false}}\,*}{P, \langle x' = f(x)\,\&\,T \geq 0\rangle\big(\neg P \wedge \langle x' = f(x)\,\&\,T \leq 0\rangle T < 0\big) \vdash \mathit{false}}\quad ①}{P, \langle x' = f(x)\,\&\,T \geq 0\rangle\big((P \vee \neg P) \wedge \langle x' = f(x)\,\&\,T \leq 0\rangle T < 0\big) \vdash \mathit{false}}}{P, \langle x' = f(x)\,\&\,T \geq 0\rangle\langle x' = f(x)\,\&\,T \leq 0\rangle T < 0 \vdash \mathit{false}}$$

The remaining open premise in ① is:

$$P, \langle x' = f(x)\,\&\,T \geq 0\rangle\big(P \wedge \langle x' = f(x)\,\&\,T \leq 0\rangle T < 0\big) \vdash \mathit{false}$$

We first note a simple propositional re-arrangement:

$$\begin{aligned}
T \leq 0 &\iff \min_{i=0}^{N} \max\big(\max_{j=0}^{a(i)} r_{ij}, \max_{j=0}^{b(i)} s_{ij}\big) \leq 0 \\
&\iff \bigvee_{i=0}^{N}\big(\bigwedge_{j=0}^{a(i)} r_{ij} \leq 0 \wedge \bigwedge_{j=0}^{b(i)} s_{ij} \leq 0\big) \\
&\iff \bigwedge_{i=0}^{M}\big(\bigvee_{j=0}^{m(i)} p_{ij} \leq 0 \vee \bigvee_{j=0}^{n(i)} q_{ij} \leq 0\big)
\end{aligned}$$

where the last step follows by reversing the re-arrangement that we used to get $\neg P$ from P.

Similarly,

$$\begin{aligned}
T < 0 &\iff \bigwedge_{i=0}^{M}\big(\bigvee_{j=0}^{m(i)} p_{ij} < 0 \vee \bigvee_{j=0}^{n(i)} q_{ij} < 0\big) \\
&\implies \bigwedge_{i=0}^{M}\big(\bigvee_{j=0}^{m(i)} p_{ij} < 0 \vee \bigvee_{j=0}^{n(i)} q_{ij} \leq 0\big) \\
&\iff \neg P
\end{aligned}$$

Therefore, we have:

$$\text{frzSgn}_{\langle\cdot\rangle},\vee\text{L}\ \frac{*}{P, \text{In}_{f(x)}(P), \langle x' = f(x)\,\&\,\bigwedge_{i=0}^{M}\big(\bigvee_{j=0}^{m(i)} p_{ij} \leq 0 \vee \bigvee_{j=0}^{n(i)} q_{ij} \leq 0\big)\rangle\neg P \vdash \mathit{false}}$$
$$\text{assum}\ \frac{}{P, \langle x' = f(x)\,\&\,\bigwedge_{i=0}^{M}\big(\bigvee_{j=0}^{m(i)} p_{ij} \leq 0 \vee \bigvee_{j=0}^{n(i)} q_{ij} \leq 0\big)\rangle\neg P \vdash \mathit{false}}$$
$$\text{CE}\ \frac{}{P, \langle x' = f(x)\,\&\,T \leq 0\rangle\neg P \vdash \mathit{false}}$$
$$\text{CM}\ \frac{}{P, \langle x' = f(x)\,\&\,T \leq 0\rangle T < 0 \vdash \mathit{false}}$$
$$\text{V}\ \frac{}{P, \langle x' = f(x)\,\&\,T \geq 0\rangle\big(P \wedge \langle x' = f(x)\,\&\,T \leq 0\rangle T < 0\big) \vdash \mathit{false}}$$

Again, note that the evolution domain introduced here corresponds to an approximation for the closure $\overline{\neg P}$. □

6.8 Semialgebraic Invariants with Semialgebraic Evolution Domains

We now show that the full LZZ rule for a semialgebraic evolution domain constraint Q is a mild extension of the derivations we made for In.

Firstly, note that in all of our derivations of In above, we may additionally assume that the evolution domain Q holds initially whenever we use the premises of In. In particular, we may derive the following sound proof rule:

$$\text{In}_{\&}\ \frac{Q \wedge \neg P \to \text{In}_{-f(x)}(\neg P) \quad Q \wedge P \to \text{In}_{f(x)}(P)}{P \to [x' = f(x)\,\&\,Q]P}$$

From a continuity point of view, if Q represents an open set, then we must locally stay in Q under any evolution of the ODE. Therefore, $Q \to \text{In}_{f(x)}(Q)$ and $Q \to \text{In}_{-f(x)}(Q)$, which simplifies the premises of LZZ. This implies that $\text{In}_{\&}$ is complete for open Q, and that In is complete for $Q \equiv \mathit{true}$.

However, $\text{In}_{\&}$ is not complete when Q is not open. For example, $x \geq 0 \wedge t = 0$ is trivially invariant in the following system because t is stuck.

$$x \geq 0 \wedge t = 0 \to [x' = -1, t' = 1\,\&\,t = 0](x \geq 0 \wedge t = 0)$$

However, the right premise of $\text{In}_{\&}$ is not valid, and so the rule does not apply:

$$t = 0 \wedge x \geq 0 \to \underbrace{(t = 0 \wedge 1 = 0)}_{\text{In}_{x'=-1,t'=1}(t=0)} \wedge \underbrace{(x > 0 \vee x = 0 \wedge -1 > 0)}_{\text{In}_{x'=-1,t'=1}(x\geq 0)}$$

The issue here is that, even though we start in the evolution domain, evolving for non-zero time would immediately leave the evolution domain. The full LZZ proof rule remedies this situation by allowing the evolution domain constraint to be immediately violated. We use the fact that $\text{In}_{f(x)}(t \neq 0) \iff \neg\text{In}_{f(x)}(t = 0)$. The right premise is now trivially valid since the newly introduced disjunct is always true:

$$t = 0 \wedge x \geq 0 \to \underbrace{(t = 0 \wedge 1 = 0)}_{\text{In}_{x'=-1,t'=1}(t=0)} \wedge \underbrace{(x > 0 \vee x = 0 \wedge -1 > 0)}_{\text{In}_{x'=-1,t'=1}(x\geq 0)} \vee \underbrace{\neg(t = 0 \wedge 1 = 0)}_{\neg\text{In}_{x'=-1,t'=1}(t=0)}$$

Following this intuition, we may re-examine our derivations for In.

Lemma 28 (LZZ)**.** *The LZZ proof rule for semialgebraic invariants is derivable using IVST, along with DRI,frzSgn$_{\langle\cdot\rangle}$, which are in turn derivable from vectorial DG with $'^*$.*

Proof. Following the derivation for In, we only need to show that whenever its premises are used, we may instead use the premises of LZZ. We assume that Q is semialgebraic, and that $\neg Q \equiv \bigvee_{i=0}^{N} \big(\bigwedge_{j=0}^{m(i)} p_{ij} \geq 0 \wedge \bigwedge_{j=0}^{n(i)} q_{ij} > 0 \big)$. We therefore have that $Q \iff \neg\neg Q \iff \bigwedge_{i=0}^{M} \big(\bigvee_{j=0}^{m(i)} p_{ij} < 0 \vee \bigvee_{j=0}^{n(i)} q_{ij} \leq 0 \big)$. As usual, we assume that none of p_{ij}, q_{ij} are at equilibrium.

The key steps where the premises of LZZ are used have the shape:

$$P, \langle x' = f(x) \,\&\, Q \wedge \overline{\neg P} \rangle \neg P \vdash \mathit{false}$$

where $\overline{\neg P}$ is an approximation of the topological closure of $\neg P$.

Having the approximate closure in the evolution domain forces the system to be locally stuck if $\mathrm{In}_{f(x)}(P)$ is true initially, assuming that none of the polynomials in P are at equilibrium. Therefore, it is not possible for $\neg P$ to hold after the evolution while P is true initially, leading to a contradiction.

In the following derivation, the left branch closes as before because $\overline{\neg P}$ is in the evolution domain constraint. The remaining (new) open branch is abbreviated by ①.

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{P, \mathrm{In}_{f(x)}(P), \langle x' = f(x) \,\&\, Q \wedge \overline{\neg P} \rangle \neg P \vdash \mathit{false}}\ ①}{P, \mathrm{In}_{f(x)}(P) \vee \mathrm{In}_{f(x)}(\neg Q), \langle x' = f(x) \,\&\, Q \wedge \overline{\neg P} \rangle \neg P \vdash \mathit{false}}\,\vee\mathrm{L}}{Q, P, \langle x' = f(x) \,\&\, Q \wedge \overline{\neg P} \rangle \neg P \vdash \mathit{false}}\,\mathrm{assum}}{P, \langle x' = f(x) \,\&\, Q \wedge \overline{\neg P} \rangle \neg P \vdash \mathit{false}}\,\mathrm{DI,DW}$$

Now, we observe that:

$$\begin{aligned} Q &\iff \bigwedge_{i=0}^{M} \big(\bigvee_{j=0}^{m(i)} p_{ij} < 0 \vee \bigvee_{j=0}^{n(i)} q_{ij} \leq 0 \big) \\ &\implies \bigwedge_{i=0}^{M} \big(\bigvee_{j=0}^{m(i)} p_{ij} \leq 0 \vee \bigvee_{j=0}^{n(i)} q_{ij} \leq 0 \big) \end{aligned}$$

where the last line acts as an approximation of the closure, $\overline{\neg\neg Q}$. Therefore, the rest of ① derives similarly because the system is stuck and so cannot transition from satisfying P initially to $\neg P$ after an evolution:

$$\dfrac{\dfrac{\dfrac{*}{P, \mathrm{In}_{f(x)}(\neg Q), \langle x' = f(x) \,\&\, \overline{\neg\neg Q} \wedge \overline{\neg P} \rangle \neg P \vdash \mathit{false}}\,\mathrm{frzSgn}_{\langle\cdot\rangle},\vee\mathrm{L}}{P, \mathrm{In}_{f(x)}(\neg Q), \langle x' = f(x) \,\&\, Q \wedge \overline{\neg P} \rangle \neg P \vdash \mathit{false}}\,\mathrm{CM}$$

□

7 Conclusion

We have shown that our extended axiomatization of dL is sound and complete for all semialgebraic invariants of polynomial ODE systems. While this shows that we can always construct a proof for true semialgebraic invariants, an end user of dL would certainly not want to build all of our lemmas from scratch. Thus, an immediate application of our work would be to add the new axioms to KeYmaera X, and to implement the necessary tactical automation [FMBP17] around our derivations. As mentioned in Section 2, it may also be the case that cleaner proofs are possible using proof rules for restricted classes of invariants. Indeed, our proof relies heavily on formula manipulation in real arithmetic, which we assume is decided by quantifier elimination ($\mathbb{R}$). In practice, some additional care would have to be taken to ensure that the quantifier elimination algorithms are actually handed goals that they can decide in a reasonable amount of time. Other directions include adding automation for generating these invariants, and extending recent formalizations of dL in Isabelle/HOL and Coq [BRV+17] with our new axioms.

Acknowledgment

We thank Andrew Sogokon for his detailed comments on an earlier draft of this report.

A Barrier Certificates

The barrier certificates proof rule [PJ04, PJP07] is given by:

$$\text{BC}\ \frac{p = 0 \to \mathcal{L}_{f(x)}(p) > 0}{p \succeq 0 \to [x' = f(x)]p \succeq 0}$$

This rule is interesting because it comes with associated methods for *finding* such invariants for an ODE system. It is also easy to see that the premises are a special case of the In proof rule that we have already derived. Here, we give a direct derivation of the rule:

Lemma 29 (Barrier certificates)**.** *The barrier certificates proof rule for invariants of the form $p \succeq 0$ is derivable using IVT$_{\&}$.*

Proof. We prove the cases $p \geq 0$ and $p > 0$ separately. Firstly, the $p \geq 0$ case uses an application of IVT$_{\otimes}$ and a basic instance of LocSgn at $n = 1$.

$$\dfrac{\dfrac{\dfrac{\dfrac{*}{p = 0, \mathcal{L}_{f(x)}(p) > 0, \langle x' = f(x)\,\&\,p \leq 0\rangle p < 0 \vdash \mathit{false}}\,\text{LocSgn}}{p = 0, \langle x' = f(x)\,\&\,p \leq 0\rangle p < 0 \vdash \mathit{false}}\,\text{assum}}{p \geq 0, \langle x' = f(x)\rangle p < 0 \vdash \mathit{false}}\,\text{IVT}_{\otimes},\exists\text{L}}{p \geq 0 \vdash [x' = f(x)]p \geq 0}\,[\cdot],\neg\text{R}$$

From this, we can directly derive the proof rule for $p > 0$ invariants by reflect.

$$\text{reflect}\ \frac{\text{BC}\ \dfrac{*}{-p \geq 0 \vdash [x' = -f(x)] - p \geq 0}}{p > 0 \vdash [x' = f(x)]p > 0}$$

Note that BC for $-p \geq 0$ applies here because the premise guarantees $p = 0 \to \mathcal{L}_{f(x)}(p) > 0$, but $\mathcal{L}_{-f(x)}(-p) = \mathcal{L}_{f(x)}(p)$. □

B Alternative Boundary Crossing Axiom

We introduced the use of extended, non-smooth terms $\max, \min$ into the term language to aid in our derivation of LZZ. Here, we consider an alternative proof rule that does not require these extended terms. By closer observation of the proof, we see that these terms are used solely to apply the IVST axiom. Moreover, the purpose of IVST was to introduce an approximation of the closure into the evolution domain constraint. We shall consider the following, alternative axiom which achieves this directly:

$$S \wedge \langle x' = f(x) \,\&\, Q\rangle \neg S \to \langle x' = f(x) \,\&\, Q \wedge \overline{S}\rangle\langle x' = f(x) \,\&\, Q \wedge \overline{\neg S}\rangle \neg S$$

Here, the (true) topological closure operator is definable in first-order real arithmetic by:

$$\overline{S}(x) \overset{\text{def}}{\equiv} \forall \varepsilon{>}0\, \exists y \in S\, \|x - y\|^2 < \varepsilon^2$$

Informally, this axiom asserts that if we start in a state satisfying S, then we can travel within $\overline{S}$ to its boundary, ∂S, at which point we cross over into $\neg S$. Unfortunately, this latter assertion is not true for arbitrary S. Consider the following counter-example, let

$$g(x) = \begin{cases} 0 & x = 0 \\ x \sin(\frac{1}{x}) & x \neq 0 \end{cases}$$

and consider the instance of the axiom with $S(x) \overset{\text{def}}{=} g(x) \leq 0$, $x' = 1$, and with $x = 0$ initially. Now, the LHS of the axiom is clearly true, since we may always evolve the ODE to a state where $g(x) > 0$. However, $g(x)$ crosses 0 infinitely often near $x = 0$, which means that by choosing x small enough, we may always find $g(x) \leq 0$ for x arbitrarily close to zero. This contradicts the RHS, because there is no run satisfying the inner diamond modality.

Moreover, the set S is definable in dL (for $x \geq 0$) by:

$$x = 0 \vee [i := *; ?ix = 1; t := 0; s := 0; c := 1; s' = c, c' = -s, t' = 1](t = i \to xs \leq 0)$$

Here, i is the value of $\frac{1}{x}$, while c, s track the values of $\cos(t), \sin(t)$ respectively. After the first box modality, we force s to be $\sin(\frac{1}{x})$. We can make the axiom sound by requiring that S is semialgebraic – the proof of soundness is essentially similar to our proof of soundness for IVST. However, this results in a syntactic check that no modal operators occur in S.

References

[Bla99] Franco Blanchini. Set invariance in control. *Automatica*, 35(11):1747–1767, 1999.

[Bor17] Michele Boreale. *Algebra, Coalgebra, and Minimization in Polynomial Differential Equations*, pages 71–87. Springer Berlin Heidelberg, Berlin, Heidelberg, 2017. URL: https://doi.org/10.1007/978-3-662-54458-7_5, doi:10.1007/978-3-662-54458-7_5.

[BRV+17] Brandon Bohrer, Vincent Rahli, Ivana Vukotic, Marcus Völp, and André Platzer. Formally verified differential dynamic logic. In Yves Bertot and Viktor Vafeiadis, editors, *Certified Programs and Proofs - 6th ACM SIGPLAN Conference, CPP 2017, Paris, France, January 16-17, 2017*, pages 208–221. ACM, 2017. doi:10.1145/3018610.3018616.

[Chi06] Carmen Chicone. *Ordinary Differential Equations with Applications, Second Edition*. Texts in Applied Mathematics. Springer-Verlag New York, 2006. doi:10.1007/0-387-35794-7.

[Dar78] Gaston Darboux. Mémoire sur les équations différentielles algébriques du premier ordre et du premier degré. *Bulletin des Sciences Mathématiques et Astronomiques*, 2(1):151–200, 1878.

[FMBP17] Nathan Fulton, Stefan Mitsch, Brandon Bohrer, and André Platzer. Bellerophon: Tactical theorem proving for hybrid systems. In Mauricio Ayala-Rincón and César Mu noz, editors, *ITP*, LNCS. Springer, 2017.

[FMQ+15] Nathan Fulton, Stefan Mitsch, Jan-David Quesel, Marcus Völp, and André Platzer. KeYmaera X: An axiomatic tactical theorem prover for hybrid systems. In Amy P. Felty and Aart Middeldorp, editors, *CADE*, volume 9195 of *LNCS*, pages 527–538. Springer, 2015. doi:10.1007/978-3-319-21401-6_36.

[GP14] Khalil Ghorbal and André Platzer. Characterizing algebraic invariants by differential radical invariants. In Erika Ábrahám and Klaus Havelund, editors, *TACAS*, volume 8413, pages 279–294. Springer, 2014.

[GSP17] Khalil Ghorbal, Andrew Sogokon, and André Platzer. A hierarchy of proof rules for checking positive invariance of algebraic and semi-algebraic sets. *Computer Languages, Systems and Structures*, 47(1):19–43, 2017. doi:10.1016/j.cl.2015.11.003.

[LZZ11] Jiang Liu, Naijun Zhan, and Hengjun Zhao. Computing semi-algebraic invariants for polynomial dynamical systems. In *Proceedings of the Ninth ACM International Conference on Embedded Software*, EMSOFT '11, pages 97–106, New York, NY, USA, 2011. ACM. URL: http://doi.acm.org/10.1145/2038642.2038659, doi:10.1145/2038642.2038659.

[MBT05] Ian M Mitchell, Alexandre M Bayen, and Claire J Tomlin. A time-dependent hamilton-jacobi formulation of reachable sets for continuous dynamic games. *IEEE Transactions on automatic control*, 50(7):947–957, 2005.

[NY99] Dmitri Novikov and Sergei Yakovenko. Trajectories of polynomial vector fields and ascending chains of polynomial ideals. In *ANNALES-INSTITUT FOURIER*, volume 49, pages 563–609. Association des annales de l'institut Fourier, 1999.

[PC08] André Platzer and Edmund M. Clarke. Computing differential invariants of hybrid systems as fixedpoints. In Aarti Gupta and Sharad Malik, editors, *CAV*, volume 5123 of *LNCS*, pages 176–189. Springer, 2008. doi:10.1007/978-3-540-70545-1_17.

[PJ04] Stephen Prajna and Ali Jadbabaie. Safety verification of hybrid systems using barrier certificates. In *HSCC*, volume 2993, pages 477–492. Springer, 2004.

[PJP07] Stephen Prajna, Ali Jadbabaie, and George J Pappas. A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Transactions on Automatic Control*, 52(8):1415–1428, 2007.

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

[Pla10] André Platzer. Differential-algebraic dynamic logic for differential-algebraic programs. *J. Log. Comput.*, 20(1):309–352, 2010. Advance Access published on November 18, 2008. doi:10.1093/logcom/exn070.

[Pla12a] André Platzer. The complete proof theory of hybrid systems. In *LICS*, pages 541–550. IEEE, 2012. doi:10.1109/LICS.2012.64.

[Pla12b] André Platzer. Logics of dynamical systems. In *LICS*, pages 13–24. IEEE, 2012. doi:10.1109/LICS.2012.13.

[Pla12c] André Platzer. The structure of differential invariants and differential cut elimination. *Logical Methods in Computer Science*, 8(4):1–38, 2012. doi:10.2168/LMCS-8(4:16)2012.

[Pla15] André Platzer. Differential game logic. *ACM Trans. Comput. Log.*, 17(1):1:1–1:51, 2015. doi:10.1145/2817824.

[Pla17a] André Platzer. A complete uniform substitution calculus for differential dynamic logic. *J. Autom. Reas.*, 59(2):219–265, 2017. doi:10.1007/s10817-016-9385-1.

[Pla17b] André Platzer. Differential hybrid games. *ACM Trans. Comput. Log.*, 18(3):19:1–19:44, 2017. doi:10.1145/3091123.

[Ric69] Daniel Richardson. Some undecidable problems involving elementary functions of a real variable. *The Journal of Symbolic Logic*, 33(4):514–520, 1969.

[SSM08] Sriram Sankaranarayanan, Henny B Sipma, and Zohar Manna. Constructing invariants for hybrid systems. *Formal Methods in System Design*, 32(1):25–55, 2008.

[Tiw08] Ashish Tiwari. Abstractions for hybrid systems. *Formal Methods in System Design*, 32(1):57–83, 2008.

[TT09] Ankur Taly and Ashish Tiwari. Deductive verification of continuous dynamical systems. In *LIPIcs-Leibniz International Proceedings in Informatics*, volume 4. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2009.