A Hierarchy of Proof Rules for Checking Positive Invariance of Algebraic and Semi-Algebraic Sets[☆]

Khalil Ghorbal[a,*], Andrew Sogokon[b], André Platzer[a]

[a] *Carnegie Mellon University, Computer Science Department, Pittsburgh, PA, USA*
[b] *University of Edinburgh, LFCS, School of Informatics, Edinburgh, Scotland, UK*

Abstract

This paper studies sound proof rules for checking positive invariance of algebraic and semi-algebraic sets, that is, sets satisfying polynomial equalities and those satisfying finite boolean combinations of polynomial equalities and inequalities, under the flow of polynomial ordinary differential equations. Problems of this nature arise in formal verification of continuous and hybrid dynamical systems, where there is an increasing need for methods to expedite formal proofs. We study the trade-off between proof rule generality and practical performance and evaluate our theoretical observations on a set of benchmarks. The relationship between increased deductive power and running time performance of the proof rules is far from obvious; we discuss and illustrate certain classes of problems where this relationship is interesting.

Keywords: Formal Verification, Polynomial Differential Equations, Positive Invariance, Deductive Power, Dynamical Systems

[☆]This material is based upon work supported by the National Science Foundation (NSF) under NSF CAREER Award CNS-1054246, NSF EXPEDITION CNS-0926181, NSF CNS-0931985, by DARPA under agreement number FA8750-12-2-029, as well as the Engineering and Physical Sciences Research Council (UK) under grant EP/I010335/1.

[*]Corresponding author
Email addresses: kghorbal@cs.cmu.edu (Khalil Ghorbal), a.sogokon@sms.ed.ac.uk (Andrew Sogokon), aplatzer@cs.cmu.edu (André Platzer)

http://dx.doi.org/10.1016/j.cl.2015.11.003

1. Introduction

In safety verification of dynamical systems, one is typically concerned with ensuring that by initializing a system in some set of states $X_0 \subseteq X$ (where X is the state space), the system will never evolve into an unsafe state (belonging to some $X_u \subseteq X$). When the system is given by ordinary differential equations, one may attempt to solve the safety verification problem by showing that the solution to the initial value problem for any initial value $\boldsymbol{x}_0 \in X_0$ cannot enter the unsafe region, that is $\boldsymbol{x}(\boldsymbol{x}_0, t) \notin X_u$ for all $t \geq 0$, where $\boldsymbol{x}(\boldsymbol{x}_0, t)$ is the state of the system at time t w.r.t. the initial value $\boldsymbol{x}_0$. The safety verification problem is in this case equivalent to showing that the intersection of the reachable set $\{\boldsymbol{x}(\boldsymbol{x}_0, t) \in X \mid t \geq 0\}$ with the set of unsafe states is empty. However, solutions to ordinary differential equations will rarely be available in closed form[1]; even when they are, their description will often be much more involved than that of the differential equations themselves. Instead, it is possible to work with the differential equations *directly* [28, 22, 23, 31].

A fundamental notion in safety verification is that of a *(positively) invariant set*. In fact, exact reachable sets of any given state $\boldsymbol{x}_0$ of the system are the *smallest* positively invariant sets one can hope to find that include $\boldsymbol{x}_0$. However, obtaining and working with exact descriptions of reachable sets is not always practical or even possible. This does not mean that system safety cannot be established by other means - if one finds a *larger* positively invariant set, $I \subseteq X$, with a simpler (preferably algebraic, or semi-algebraic) description and which (i) contains the set of initial states (i.e. $X_0 \subseteq I$) and (ii) does not intersect the set of unsafe states (i.e. $I \cap X_u = \emptyset$), then one can soundly conclude that the system is safe.

We focus on methods for *checking* whether a given set defines a positively invariant region, i.e. one from which no system trajectory can escape in positive time ($t \geq 0$). In particular, we consider the important case of algebraic and semi-algebraic sets, i.e. sets that can be defined by polynomial equations and finite boolean combinations of polynomial equations and inequalities, respectively. We review previously reported methods and introduce extensions to automatically check positive invariance of semi-algebraic sets. Our work aims at identifying sweetspots in the various methods in order to suggest efficient strategies for invariant checking inside a deductive prover.

Contributions. We extend our earlier analysis presented in [12] to include proof rules that are concerned with checking positive invariance of semi-algebraic

[1] That is explicitly given in terms of elementary functions and usual operators.

sets. In addition to recalling proof rules reported previously, we introduce in Section 5.2 a new sufficient condition that we term NSSBC for Non-smooth Strict Barrier Certificate. NSSBC is able to prove positive invariance in a special class of closed semi-algebraic sets and can be seen as a generalization of strict barrier certificates introduced by Prajna [26]. We also investigate in Section 7.4 the effect of *square-free decomposition*—which generalizes the square-free reduction—on the deductive power of proof rules. Finally, we complement our theoretical results with a practical assessment of the proof rule performance on a set of benchmarks and explore interesting connections between the deductive power and the practical running time performance (Section 8.2).

2. Preliminaries

We consider autonomous[2] polynomial vector fields (see Def. 1 below).

Let $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$, and $\boldsymbol{x}(t) = (x_1(t), \ldots, x_n(t))$, where $x_i : \mathbb{R} \to \mathbb{R}$, $t \mapsto x_i(t)$. The ring of polynomials over the reals will be denoted by $\mathbb{R}[x_1, \ldots, x_n]$.

Definition 1 (Polynomial Vector Field)**.** *Let p_i, $1 \leq i \leq n$, be multivariate polynomials of the polynomial ring $\mathbb{R}[x_1, \ldots, x_n]$. A* polynomial vector field*, $\boldsymbol{p}$, is an explicit system of ordinary differential equations with polynomial right-hand side:*

$$\frac{dx_i}{dt} = \dot{x}_i = p_i(\boldsymbol{x}), \quad 1 \leq i \leq n \ . \tag{1}$$

Since polynomial functions are smooth (C^∞, i.e. they have derivatives up to any order), they are locally Lipschitz-continuous. By the Cauchy-Lipschitz theorem (a.k.a. Picard-Lindelöf) [15], there exists a unique maximal solution to the initial value problem ($\dot{\boldsymbol{x}} = \boldsymbol{p}$, $\boldsymbol{x}(0) = \boldsymbol{x}_0$) defined for t in some non-empty open interval; it is often denoted by $\boldsymbol{x}(t)$, or more explicitly as $\varphi_t(\boldsymbol{x}_0)$.

For $S \subseteq \mathbb{R}^n$, if $\varphi_t(\boldsymbol{x}_0) \in S$ for all $t \geq 0$ and $\boldsymbol{x}_0 \in S$, we say that the set S is a *(positive) invariant* under the flow of $\boldsymbol{p}$. If S is described by a quantifier-free formula of real arithmetic (i.e. is a semi-algebraic set satisfying a finite boolean combination of polynomial equalities and inequalities), positive invariance of S

[2]That is, the rate of change of the system over time explicitly depends only on the system's *state*, not on time. Non-autonomous polynomial systems with time-dependence can be made autonomous by extending the state of the system with an extra *clock variable* that reflects the progress of time and replacing every instance of the time variable with the new clock variable.

is semantically equivalent to the validity of the following formula in differential dynamic logic [21]:

$$S \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\, S. \tag{2}$$

A result about positive invariance of *closed* sets under the flow of locally Lipschitz-continuous ODEs, known as the Nagumo theorem [19, 32, Chapter 10, XV–XVI, pp. 117-119], gives a powerful (but generally intractable) geometric characterization of positively invariant closed sets. Nagumo's theorem requires the geometric notion of *sub-tangential vectors* to a set.

Definition 2 (Sub-tangent vector)**.** *A vector $\boldsymbol{v} \in \mathbb{R}^n$ is sub-tangential to a set $S \subseteq \mathbb{R}^n$ at $\boldsymbol{x} \in S$ if*

$$\liminf_{\lambda \to 0^+} \frac{\operatorname{dist}(S, \boldsymbol{x} + \lambda \boldsymbol{v})}{\lambda} = 0,$$

where dist *denotes the Euclidean set distance, i.e.* $\operatorname{dist}(S, \boldsymbol{x}) \equiv \inf_{\boldsymbol{y} \in S} \|\boldsymbol{x} - \boldsymbol{y}\|$. *The set of all sub-tangent vectors to a set S at $\boldsymbol{x} \in S$ is known as the* contingent cone *to S at $\boldsymbol{x}$ and is denoted $K_{\boldsymbol{x}}(S)$.*

Theorem 3 (Nagumo's Theorem)**.** *Given a continuous system $\dot{\boldsymbol{x}} = \boldsymbol{p}(\boldsymbol{x})$ and assuming that solutions exist and are unique inside some open set $O \subseteq \mathbb{R}^n$, let $S \subset O$ be a closed set. Then, S is* positively invariant *under the flow of the system if and only if $\boldsymbol{p}(\boldsymbol{x})$ is sub-tangential to S (or equivalently, $\boldsymbol{p}(\boldsymbol{x}) \in K_{\boldsymbol{x}}(S)$, where $K_{\boldsymbol{x}}(S)$ is the set of all sub-tangential vectors to S at $\boldsymbol{x}$, known as the* contingent cone*) for all $\boldsymbol{x} \in \operatorname{bdr}(S)$, where $\operatorname{bdr}(S)$ is the boundary of S.*[3]

Using Nagumo's Theorem, the following proof rule is sound and complete when S is a *closed* semi-algebraic set:

$$(\text{Nagumo}) \frac{\forall\, \boldsymbol{x} \in \operatorname{bdr}(S).\, \boldsymbol{p}(\boldsymbol{x}) \in K_{\boldsymbol{x}}(S)}{S \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\, S}\,.$$

More recently, a different characterization of positively invariant sets (described in detail in subsequent sections) was reported in [16].

In the important special case where a closed set S is described by the equation $h = 0$, with $h \in \mathbb{R}[x_1 \ldots, x_n]$, positive invariance of $h = 0$ is semantically equivalent to the validity of the formula:

$$(h = 0) \to [\dot{\boldsymbol{x}} = \boldsymbol{p}](h = 0). \tag{3}$$

[3]The border of a set S is often denoted by ∂S. We will use $\operatorname{bdr}(S)$ instead to avoid confusion with partial derivatives.

Geometrically, the equation $h = 0$ represents the set of real roots of the polynomial h. Such a set is known as *real algebraic set* or a *real variety* and will be henceforth denoted by $V_{\mathbb{R}}(h)$. Algebraic sets are intimately related to sets of polynomials with special algebraic properties called *ideals*. Ideals are closed under addition and external multiplication; that is, if I is an ideal, then for all $h_1, h_2 \in I$, the sum $h_1 + h_2 \in I$; and if $h \in I$, then, $qh \in I$, for all $q \in \mathbb{R}[x_1 \ldots, x_n]$. To say that the real variety $V_{\mathbb{R}}(h)$ of the ideal *generated by* h is invariant under the flow of the vector field $\boldsymbol{p}$ is equivalent to the statement that the equation $h = 0$ is invariant.

We will use ∇h to denote the gradient of $h : \mathbb{R}^n \to \mathbb{R}$, that is the vector of its partial derivatives $\left(\frac{\partial h}{\partial x_1}, \ldots, \frac{\partial h}{\partial x_n}\right)$. The *Lie derivative* of h along the vector field $\boldsymbol{p}$ gives the rate of change of h along the flow of $\dot{\boldsymbol{x}} = \boldsymbol{p}(\boldsymbol{x})$ and is formally defined as the scalar product of ∇h and $\boldsymbol{p}$.

$$\mathfrak{L}_{\boldsymbol{p}}(h) \stackrel{\text{def}}{=} \nabla h \cdot \boldsymbol{p} \ . \tag{4}$$

Higher-order Lie derivatives are defined recursively as $\mathfrak{L}_{\boldsymbol{p}}^{(k+1)}(h) = \mathfrak{L}_{\boldsymbol{p}}(\mathfrak{L}_{\boldsymbol{p}}^{(k)}(h))$, with $\mathfrak{L}_{\boldsymbol{p}}^{(0)}(h) = h$.

3. Proof Rules for Algebraic Sets

We recall five important proof rules for checking invariance of polynomial equalities, or equivalently the validity of Equation 3. In Figure 1, FI refers to invariant polynomial functions.[4] The premise of the Polynomial-scale consecution proof rule [28], P-c in Figure 1, requires $\mathfrak{L}_{\boldsymbol{p}}(h)$ to be in the ideal generated by h. The condition given in the premise is only sufficient (but is eminently suitable for *generating* invariant varieties [17]). We also consider the constant-scale consecution proof rule [28, 31], denoted by C-c. The premise of proof rule C-c requires that $\mathfrak{L}_{\boldsymbol{p}}(h) = \lambda h$, where λ is a scalar, not a polynomial as in P-c. It is therefore a simple special case of P-c. When $\lambda = 0$, one obtains the premise of the proof rule FI. It is worth noting that the condition in the premise of P-c, including its special case C-c, was mentioned as early as 1878 [6] and used extensively in the study of integrability of dynamical systems (e.g. see *second integrals* in [13, Chapter 2]). It serves as a natural extension to invariant functions, also known as *first integrals*, which are covered by the proof rule FI. The proof rule Lie gives Lie's criterion [14, 20] for invariance of $h = 0$; this proof rule will be discussed in more depth

[4] We used the notation $\text{DI}_=$ for the same proof rule in [12].

$$(\text{FI})\frac{\mathfrak{L}_{\boldsymbol{p}}(h)=0}{(h=0)\to[\dot{\boldsymbol{x}}=\boldsymbol{p}](h=0)} \qquad (\text{C-c})\frac{\exists\lambda\in\mathbb{R},\ \mathfrak{L}_{\boldsymbol{p}}(h)=\lambda h}{(h=0)\to[\dot{\boldsymbol{x}}=\boldsymbol{p}](h=0)}$$

$$(\text{Lie})\frac{h=0\to(\mathfrak{L}_{\boldsymbol{p}}(h)=0\wedge\nabla h\neq\mathbf{0})}{(h=0)\to[\dot{\boldsymbol{x}}=\boldsymbol{p}](h=0)} \qquad (\text{P-c})\frac{\mathfrak{L}_{\boldsymbol{p}}(h)\in\langle h\rangle}{(h=0)\to[\dot{\boldsymbol{x}}=\boldsymbol{p}](h=0)}$$

$$(\text{DRI})\frac{h=0\to\bigwedge_{i=0}^{N-1}\mathfrak{L}_{\boldsymbol{p}}^{(i)}(h)=0}{(h=0)\to[\dot{\boldsymbol{x}}=\boldsymbol{p}](h=0)}$$

Figure 1: Proof rules for checking the invariance of $h=0$ w.r.t. $\boldsymbol{p}$: FI, C-c and P-c [28, Lemma 2], Lie [20, Theorem 2.8], DRI [10, Theorem 2]

and extended to handle tricky cases in Section 4. The last rule, DRI in Fig. 1, was recently introduced and characterizes (i.e. gives necessary and sufficient conditions for) invariant real varieties under the flow of polynomial vector fields [10]. The number N in the premise of DRI is the maximum length of the ascending chain of polynomial ideals $\langle h\rangle\subset\langle h,\mathfrak{L}_{\boldsymbol{p}}(h)\rangle\subset\langle h,\mathfrak{L}_{\boldsymbol{p}}(h),\mathfrak{L}_{\boldsymbol{p}}^{(2)}(h)\rangle\subset\cdots$, which is finite and computable [10].

4. Extending Lie's Criterion

One immediate deficiency of the proof rule Lie (Fig. 1) is its inability to prove invariance properties for isolated points (e.g. system equilibria) for the simple reason that a description of such a point $\boldsymbol{a}=(a_1,\ldots,a_n)\in\mathbb{R}^n$, e.g. given by the sum-of-squares equation $h(\boldsymbol{x})=(x_1-a_1)^2+\cdots+(x_n-a_n)^2=0$, will have an extremum at $\boldsymbol{a}$, i.e. $h(\boldsymbol{a})=0$ and

$h(\boldsymbol{x})>0$ for all $\boldsymbol{x}\in\mathbb{R}^n\setminus\{\boldsymbol{a}\}$. Functions whose real roots characterize isolated points have vanishing gradient at these roots, in this case $\boldsymbol{a}$, and thus the formula $h=0\to\nabla h=\mathbf{0}$ holds. This violates the regularity condition in the premise of the proof rule Lie, namely:

$$h=0\longrightarrow\nabla h\neq\mathbf{0}\ . \tag{5}$$

In fact, $h=0\to\mathfrak{L}_{\boldsymbol{p}}(h)=0$ is a necessary condition when $h=0$ is an invariant equation. Note that simply removing Eq. (5) from the premise of the proof rule Lie is unsound (see e.g. [23]); that is, the condition $h=0\to\mathfrak{L}_{\boldsymbol{p}}(h)=0$ alone is insufficient to prove the invariance property for $h=0$. Unsoundness in the above

naïve attempt at a generalization is a consequence of *singularities* that may be present in the variety $V_{\mathbb{R}}(h)$. Singularities of $V_{\mathbb{R}}(h)$ are points $\boldsymbol{x} \in V_{\mathbb{R}}(h)$ where the gradient of h vanishes, i.e. $\nabla h(\boldsymbol{x}) = \mathbf{0}$.

Definition 4 (Singular Locus)**.** *Let $h \in \mathbb{R}[x_1, \ldots, x_n]$, the* singular locus *of $h = 0$, henceforth denoted $\mathrm{SL}(h)$, is the set of singular points, that is, points $\boldsymbol{x}$ satisfying*

$$h = 0 \wedge \frac{\partial h}{\partial x_1} = 0 \wedge \cdots \wedge \frac{\partial h}{\partial x_n} = 0 \ .$$

Points that are not singular are called regular. At singular points, the Lie derivative of h along any vector field is $\mathbf{0} \cdot \boldsymbol{p} = 0$. To avoid these degenerate cases, the regularity condition (Eq. (5)) rules out singularities altogether. In the next section we present two extensions of Lie's criterion that, in a similar vein to [29], partially overcome the strong regularity condition by treating the points on the singular locus separately.

4.1. Handling Singularities

Equilibria are points in the state space where the vector field vanishes ($\boldsymbol{p} = \mathbf{0}$) so that there is no motion. However, as seen above, Lie's criterion cannot generally be applied to prove invariance properties of isolated equilibria because their description involves singularities. One simple way to resolve this issue is to drop the non-vanishing gradient condition and replace it with the proviso that there be no flow (that is $\boldsymbol{p} = \mathbf{0}$) in the variables of the invariant candidate on the singular locus; this will allow singularities in the invariant candidate and will provide a *sound* proof method in which there is no need to check for non-vanishing gradient. Below we present two extensions to the proof rule Lie and justify their soundness after recalling some basic geometric notions.

Definition 5 (Lie°: Lie + Equilibria)**.**

$$(\mathrm{Lie}^\circ)\frac{h = 0 \to \big(\mathfrak{L}_{\boldsymbol{p}}(h) = 0 \wedge \big(\mathrm{SL}(h) \to \bigwedge_{x_i \in \mathrm{vars}(h)} p_i = 0\big)\big)}{(h = 0) \to [\dot{\boldsymbol{x}} = \boldsymbol{p}](h = 0)},$$

where $\mathrm{vars}(h)$ denotes the set of state variables x_i occurring in the polynomial h.

The Lie° proof rule can be generalized further at the expense of adding an extra variable by replacing the "no flow" condition ($p_i = 0$) for points on the singular locus with $\forall \lambda.\ h(\boldsymbol{x} + \lambda \boldsymbol{p}(\boldsymbol{x})) = 0$, where λ is a fresh symbol.

Definition 6 (Lie^*: Lie + Vanishing Sub-tangent)**.**

$$(\mathrm{Lie}^*)\frac{h=0 \to \big(\mathfrak{L}_{\boldsymbol{p}}(h)=0 \wedge (\mathrm{SL}(h) \to h(\boldsymbol{x}+\lambda\boldsymbol{p})=0)\big)}{(h=0)\to[\dot{\boldsymbol{x}}=\boldsymbol{p}](h=0)} \ .$$

To prove soundness of Lie° and Lie^*, we appeal to the Nagumo theorem. Let us observe that given $\boldsymbol{x} \in \mathrm{bdr}(S)$, if $\boldsymbol{x}+\lambda\boldsymbol{p}(\boldsymbol{x}) \in S$ for all $\lambda \in \mathbb{R}$, then $\mathrm{dist}\,(S, \boldsymbol{x}+\lambda\boldsymbol{p}(x)) = 0$ and so $\boldsymbol{p}(\boldsymbol{x})$ is sub-tangential to S at $\boldsymbol{x}$. This observation is important for algebraic sets, for which $\mathrm{bdr}(S) = S$, and the condition $\boldsymbol{x}+\lambda\boldsymbol{p}(\boldsymbol{x}) \in S$ translates to $h(\boldsymbol{x}+\lambda\boldsymbol{p}(\boldsymbol{x}))=0$. This is the main idea behind the soundness of the proof rule Lie^*.

Proposition 7. *The proof rule* Lie^* *is sound.*

Proof. A point on the variety is either regular or singular. For regular points (these form an *open subset* of the variety), since $\mathfrak{L}_{\boldsymbol{p}}(h)(\boldsymbol{x})=0$, the vector $\boldsymbol{p}(\boldsymbol{x})$ is sub-tangent to the variety at $\boldsymbol{x}$ (in fact, it is even *tangent*, so the condition we check is exactly that which is used in Lie). At singular points $\boldsymbol{x} \in V_{\mathbb{R}}(h)$ if $h(\boldsymbol{x}+\lambda\boldsymbol{p}(\boldsymbol{x}))=0$ holds for all λ then $\mathrm{dist}(V_{\mathbb{R}}(h), \boldsymbol{x}+\lambda\boldsymbol{p}(\boldsymbol{x}))=0$ for all λ, from which it follows that $\liminf_{\lambda\to 0^+} \frac{\mathrm{dist}(V_{\mathbb{R}}(h),\boldsymbol{x}+\lambda\boldsymbol{p}(\boldsymbol{x}))}{\lambda} = 0$ and thus $\boldsymbol{p}(\boldsymbol{x})$ is sub-tangential to $V_{\mathbb{R}}(h)$ at $\boldsymbol{x}$. Assuming solutions exist and are unique, the variety $V_{\mathbb{R}}(h)$ is positively invariant under the vector field $\boldsymbol{p}$ by Nagumo's theorem. □

The case $\boldsymbol{p}(\boldsymbol{x})=0$ for all $\boldsymbol{x}$ in the singular locus is a special case of the proof rule Lie^*. Therefore, the soundness of Lie° is an immediate corollary of Prop. 7.

Corollary 8. *The proof rule* Lie° *is sound.*

Remark 9. *It is worth remarking that the proof rules presented in this section, as well as* Lie *and* FI*, also work for non-polynomial vector fields and invariant candidates which themselves are not polynomial but sufficiently smooth. However, in such cases the resulting arithmetic may no longer be decidable [27].*

5. Proof rules for semi-algebraic sets

In this section we will discuss three different methods for proving positive invariance of semi-algebraic sets, that is sets described by boolean combinations of polynomial equalities and inequalities.

5.1. Differential Invariants

Differential induction with differential invariants (henceforth DI) was introduced in [22, Theorem 1].

Theorem 10 (Differential Invariants (DI))**.** *Given a polynomial system $\dot{\boldsymbol{x}} = \boldsymbol{p}$ and a quantifier-free formula of real arithmetic S in the state variables (describing some semi-algebraic set), the following rule of inference is sound:*

$$(\mathrm{DI})\frac{D(S)^{\boldsymbol{p}}_{\dot{\boldsymbol{x}}}}{S \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\, S} \quad .$$

In DI, S is a quantifier-free first-order formula in the theory of real arithmetic and D is the *derivation operator* [23, Definition 3.2], which is defined as follows:

$$\begin{aligned}
D(r) &= 0 \quad \text{for numbers,}\\
D(x) &= \dot{x} \quad \text{for variables,}\\
D(a+b) &= D(a) + D(b),\\
D(a \cdot b) &= D(a) \cdot b + a \cdot D(b),\\
D\left(\frac{a}{b}\right) &= \frac{D(a) \cdot b - a \cdot D(b)}{b^2},\\
D(S_1 \wedge S_2) &\equiv D(S_1) \wedge D(S_2),\\
D(S_1 \vee S_2) &\equiv D(S_1) \wedge D(S_2), \ (\wedge \text{ here is important for soundness})\\
D(a \leq b) &\equiv D(a) \leq D(b), \quad \text{accordingly for } \geq, >, < .
\end{aligned} \tag{6}$$

The formula $D(S)^{\boldsymbol{p}}_{\dot{\boldsymbol{x}}}$ is obtained by replacing each $\dot{x}_i$ in $D(S)$ with the corresponding right hand side in the system of differential equations, i.e. by $p_i(\boldsymbol{x})$.

Remark 11. *Note that if S has the form $h \leq 0$ for a polynomial h, then the requirements in the premise of* DI *are exactly the conditions that a barrier certificate [25] has to satisfy. Thus, for this case, differential invariants include barrier certificates as a special case [22]. Barrier certificates are, however, also accompanied with interesting techniques for generating such invariant regions.*

Remark 12. *When $S \equiv h = 0$, the premise of* DI *is equivalent to the premise of* FI*. Thus,* DI *lifts* FI *to formulas following the arithmetic of the D operator in Eq.* (6)*.*

In practice, although differential invariants allow one to work with sets that are expressed using formulas with boolean operators, the conditions are very conservative (because they are required to hold everywhere in the state space, rather

than only on the boundary of the set defined by S) and may fail to hold even for seemingly simple positively invariant sets. That is why differential invariants are used in conjunction with differential cuts [22, 24], a process of successively augmenting the system dynamics with provable invariants, which we do not consider here.

5.2. Non-Smooth Strict Barrier Certificate

Another criterion, which we term *non-smooth strict barrier certificate*, may be seen as a generalization of the strict barrier certificates criterion [25, 26] (limited to closed sets of the form $h \leq 0$) to generic closed semi-algebraic sets. Notice that our generalization only concerns the sufficient conditions for checking the invariance of supplied candidates. In particular, we do not extend nor adapt the computation techniques (convex optimization) underlying the barrier certificates generation to the new criterion we present in the sequel.

Given a closed semi-algebraic set $S \equiv \bigvee_{i=1}^{k} \bigwedge_{j=1}^{m(i)} h_{ij} \leq 0$ with polynomials $h_{ij} \in \mathbb{R}[x_1, \ldots, x_n]$, we can equivalently rewrite S by a sub-level set of a continuous function, namely

$$S \equiv \bigvee_{i=1}^{k} \bigwedge_{j=1}^{m(i)} h_{ij} \leq 0 \equiv \min_{i=1,\ldots,k} \max_{j=1,\ldots,m(i)} h_{ij} \leq 0 \ .$$

Before stating the proof rule, we first define the Lie derivation for $\min \max$ functions as follows. The set $\mathfrak{L}_{\boldsymbol{p}}(\max(h_1, h_2, \ldots, h_m)) < 0$ is defined inductively by $\mathfrak{L}_{\boldsymbol{p}}(h_1) < 0$ if $m = 1$, and for $m \geq 2$ by

$$\begin{array}{ll} & (h_1 > \max(h_2, \ldots, h_m) \rightarrow \mathfrak{L}_{\boldsymbol{p}}(h_1) < 0) \\ \wedge & (h_1 < \max(h_2, \ldots, h_m) \rightarrow \mathfrak{L}_{\boldsymbol{p}}(\max(h_2, \ldots, h_m)) < 0) \\ \wedge & (h_1 = \max(h_2, \ldots, h_m) \rightarrow \mathfrak{L}_{\boldsymbol{p}}(h_1) < 0 \wedge \mathfrak{L}_{\boldsymbol{p}}(\max(h_2, \ldots, h_m)) < 0) \end{array} \tag{7}$$

For instance, for $m = 2$, one gets:

$$\begin{array}{rcll} \mathfrak{L}_{\boldsymbol{p}}(\max(h_1, h_2)) < 0 & \stackrel{\text{def}}{=} & (h_1 > h_2 \rightarrow \mathfrak{L}_{\boldsymbol{p}}(h_1) < 0) \\ & \wedge & (h_1 < h_2 \rightarrow \mathfrak{L}_{\boldsymbol{p}}(h_2) < 0) \\ & \wedge & (h_1 = h_2 \rightarrow \mathfrak{L}_{\boldsymbol{p}}(h_1) < 0 \wedge \mathfrak{L}_{\boldsymbol{p}}(h_2) < 0) \end{array}$$

We similarly define the set $\mathfrak{L}_{\boldsymbol{p}}(\min(g_1, \ldots, g_m)) < 0$ by $\mathfrak{L}_{\boldsymbol{p}}(g_1) < 0$ if $m = 1$, and for $m \geq 2$,

$$\begin{array}{ll} & (g_1 < \min(g_2, \ldots, g_m) \rightarrow \mathfrak{L}_{\boldsymbol{p}}(g_1) < 0) \\ \wedge & (g_1 > \min(g_2, \ldots, g_m) \rightarrow \mathfrak{L}_{\boldsymbol{p}}(\min(g_2, \ldots, g_m)) < 0) \\ \wedge & (g_1 = \min(g_2, \ldots, g_m) \rightarrow \mathfrak{L}_{\boldsymbol{p}}(g_1) < 0 \vee \mathfrak{L}_{\boldsymbol{p}}(\min(g_2, \ldots, g_m)) < 0) \end{array} \ . \tag{8}$$

where g_i is of the form $\max(h_{i,1}, \ldots, h_{i,m})$. For instance,

$$\begin{aligned}\mathfrak{L}_{\boldsymbol{p}}(\min(\max(h_1,h_2),h_3)) < 0 \equiv \\ (\max(h_1,h_2) < h_3 \rightarrow \mathfrak{L}_{\boldsymbol{p}}(\max(h_1,h_2)) < 0) \\ \wedge \quad (\max(h_1,h_2) > h_3 \rightarrow \mathfrak{L}_{\boldsymbol{p}}(h_3) < 0) \\ \wedge \quad (\max(h_1,h_2) = h_3 \rightarrow \mathfrak{L}_{\boldsymbol{p}}(\max(h_1,h_2)) < 0 \vee \mathfrak{L}_{\boldsymbol{p}}(h_3) < 0)\end{aligned} \tag{9}$$

We are now ready to state the non-smooth strict barrier certificate proof rule.

Proposition 13 (Non-smooth strict barrier certificates (NSSBC))**.** *Given a continuous system $\dot{\boldsymbol{x}} = \boldsymbol{p}$ and a* closed *semi-algebraic set $S \equiv \bigvee_{i=1}^{k} \bigwedge_{j=1}^{m(i)} h_{ij} \leq 0$, where $h_{ij} \in \mathbb{R}[x_1, \ldots, x_n]$, then, the following proof rule is sound:*

$$\text{(NSSBC)}\ \frac{\left(\min\limits_{i=1,\ldots,k}\ \max\limits_{j=1,\ldots,m(i)} h_{ij} = 0\right) \rightarrow \mathfrak{L}_{\boldsymbol{p}}\left(\min\limits_{i=1,\ldots,k}\ \max\limits_{j=1,\ldots,m(i)} h_{ij}\right) < 0}{\left(\bigvee_{i=1}^{k} \bigwedge_{j=1}^{m(i)} h_{ij} \leq 0\right) \rightarrow [\dot{\boldsymbol{x}} = \boldsymbol{p}] \left(\bigvee_{i=1}^{k} \bigwedge_{j=1}^{m(i)} h_{ij} \leq 0\right)}.$$

Proof. Consider an arbitrary point $\boldsymbol{x}_0 \in \mathbb{R}^n$ such that

$$\min_{i=1,\ldots,k}\ \max_{j=1,\ldots,m(i)} h_{ij}\Big|_{\boldsymbol{x}_0} = 0,$$

then it is necessarily the case that for those *active* $\max$ arguments with indices i_* in $I_* \subseteq \{1, \ldots, k\}$ such that

$$\max_{j=1,\ldots,m(i_*)} h_{i_* j}\Big|_{\boldsymbol{x}_0} = 0$$

for all $i_* \in I_*$, the condition

$$\mathfrak{L}_{\boldsymbol{p}}\left(\max_{j=1,\ldots,m(i_*)} h_{i_* j}\right)\Big|_{\boldsymbol{x}_0} < 0$$

needs to hold for at least some $i_* \in I_*$ (otherwise the premise of the proof rule is not satisfied). Without loss of generality, assume that at $\boldsymbol{x}_0$ there is one such i_*. The condition guarantees that for all polynomial arguments of the $\max$ function, their Lie derivative is strictly negative at $\boldsymbol{x}_0$. Since Lie derivatives of polynomials under polynomial vector fields are also polynomial functions (and thus continuous), there exists an open neighbourhood around $\boldsymbol{x}_0$ inside which $\mathfrak{L}_{\boldsymbol{p}}(h_{i_* j}) < 0$

is true for all $j \in \{1, \ldots, m(i_*)\}$. Thus, if the system is initialized at $\boldsymbol{x}_0$, it is guaranteed to enter the region where

$$\max_{j=1,\ldots,m(i_*)} h_{i_* j} < 0$$

and remain there for some non-empty time interval $(0, \epsilon)$, where $\epsilon > 0$, by following the solution $\varphi_t(\cdot)$, which implies that

$$\min_{i=1,\ldots,k} \max_{j=1,\ldots,m(i)} h_{ij}(\varphi_t(\boldsymbol{x}_0)) \leq 0$$

for all $t \in [0, \frac{\epsilon}{2}]$. The closed set S is thus locally positively invariant and therefore positively invariant. □

5.3. Nagumo-like Conditions for Closed Semi-algebraic Sets

Nagumo's theorem gives a necessary and sufficient condition for positive invariance of arbitrary *closed* sets (cf. Theorem 3); however, one needs to be careful when applying this result to sets defined by formulas with logical connectives. It is often tempting to apply the sub-tangency condition *element-wise* to sets defined by atomic formulas, but in certain degenerate cases this leads to incorrect conclusions. To appreciate this problem, we first require some basic facts about the closure properties of the contingent cone (i.e. the set of all sub-tangent vectors to a set at a given point).

Proposition 14. *Let $S_1, S_2 \subseteq \mathbb{R}^n$, then for all $\boldsymbol{x} \in S$ we have*

$$K_{\boldsymbol{x}}(S_1) \cup K_{\boldsymbol{x}}(S_2) \subseteq K_{\boldsymbol{x}}(S_1 \cup S_2).$$

Proof. Since $\operatorname{dist}(S, \cdot) \geq 0$ and $S_1 \subseteq S_1 \cup S_2$, we have

$$\begin{aligned} 0 \leq \quad & \inf_{\boldsymbol{x} \in S_1 \cup S_2} \|\boldsymbol{x} - \boldsymbol{x}_0\| \leq \quad \inf_{\boldsymbol{x} \in S_1} \|\boldsymbol{x} - \boldsymbol{x}_0\| \quad \text{for any } \boldsymbol{x}_0, \text{ and} \\ 0 \leq \quad & \operatorname{dist}(S_1 \cup S_2, \boldsymbol{x}_0) \leq \quad \operatorname{dist}(S_1, \boldsymbol{x}_0) \quad \text{by definition.} \end{aligned}$$

Substituting $\boldsymbol{x}_0 + t\boldsymbol{v}$ for $\boldsymbol{x}_0$ and dividing by $t > 0$ we get

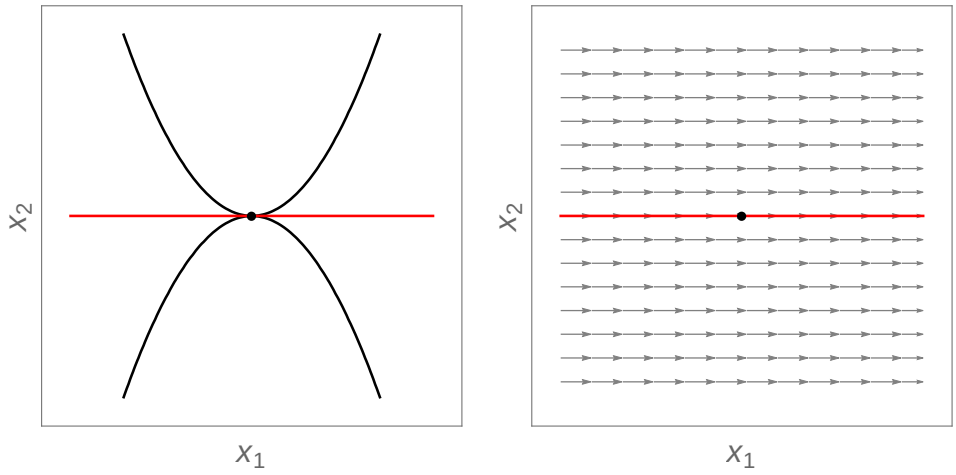
$$\begin{aligned} 0 \leq \quad & \frac{\operatorname{dist}(S_1 \cup S_2, \boldsymbol{x}_0 + t\boldsymbol{v})}{t} \leq \quad \frac{\operatorname{dist}(S_1, \boldsymbol{x}_0 + t\boldsymbol{v})}{t} \quad \text{and by assumption} \\ 0 \leq \quad & \liminf_{t \to 0^+} \frac{\operatorname{dist}(S_1 \cup S_2, \boldsymbol{x}_0 + t\boldsymbol{v})}{t} \leq \quad \liminf_{t \to 0^+} \frac{\operatorname{dist}(S_1, \boldsymbol{x}_0 + t\boldsymbol{v})}{t} = 0. \end{aligned}$$

from which it follows that if $\boldsymbol{v}$ is sub-tangential to S_1 at $\boldsymbol{x}_0$, then it is also sub-tangential to $S_1 \cup S_2$. Thus, $K_{\boldsymbol{x}}(S_1) \subseteq K_{\boldsymbol{x}}(S_1 \cup S_2)$ for all $\boldsymbol{x} \in S_1$; by the same argument one shows $K_{\boldsymbol{x}}(S_2) \subseteq K_{\boldsymbol{x}}(S_1 \cup S_2)$ for all $\boldsymbol{x} \in S_2$, from which one concludes that the inclusion $K_{\boldsymbol{x}}(S_1) \cup K_{\boldsymbol{x}}(S_2) \subseteq K_{\boldsymbol{x}}(S_1 \cup S_2)$ holds for all $\boldsymbol{x} \in S_1 \cup S_2$. □

Proposition 15. *Let $S_1, S_2 \subseteq \mathbb{R}^n$, then in general*

$$K_{\boldsymbol{x}}(S_1) \cap K_{\boldsymbol{x}}(S_2) \nsubseteq K_{\boldsymbol{x}}(S_1 \cap S_2).$$

Proof. Consider $S_1 \equiv \{\boldsymbol{x} \mid x_2 + x_1^2 = 0\}$ and $S_2 \equiv \{\boldsymbol{x} \mid x_2 - x_1^2 = 0\}$. The two sets intersect at $\mathbf{0} \in \mathbb{R}^2$. At the origin, the intersection of the contingent cones is given by the real line, i.e. $K_{\mathbf{0}}(S_1) \cap K_{\mathbf{0}}(S_2) = \{\boldsymbol{x} \mid x_2 = 0\}$, whereas the contingent cone to the intersection of the two sets is given by the zero vector, $K_{\mathbf{0}}(S_1 \cap S_2) = \{\mathbf{0}\}$. See Figure 2 for an illustration and [33] for an overview this problem. □



(a) $x_2 + x_1^2 = 0 \wedge x_2 - x_1^2 = 0$ (b) $\dot{x}_1 = 1, \dot{x}_2 = 0$

Figure 2: Closure properties of the contingent cone at an intersection of two closed sets. The intersection of the contingent cones to the two sets is shown in red. The contingent cone to the intersection itself is $\{\mathbf{0}\}$.

In general, given a closed set S which is presented as a finite union of intersections of closed sets S_{ij}, i.e.

$$\bigcup_{i=1}^{k} \bigcap_{j=1}^{m(i)} S_{ij},$$

one would like to determine if $\boldsymbol{p}(\boldsymbol{x}) \in K_{\boldsymbol{x}}(S)$ by only checking $\boldsymbol{p}(\boldsymbol{x}) \in K_{\boldsymbol{x}}(S_{ij})$. If one has

$$\bigcup_{i=1}^{k} \bigcap_{j=1}^{m(i)} K_{\boldsymbol{x}}(S_{ij}) \subseteq K_{\boldsymbol{x}}(\bigcup_{i=1}^{k} \bigcap_{j=1}^{m(i)} S_{ij}). \tag{10}$$

for all $\boldsymbol{x}$ on the boundary of S, then Nagumo's criterion for vector field membership in the contingent cone for the whole set can be applied component-wise, i.e. the condition becomes

$$\forall \boldsymbol{x} \in \mathrm{bdr} \left(\bigcup_{i=1}^{k} \bigcap_{j=1}^{m(i)} S_{ij} \right) . \quad \boldsymbol{p}(\boldsymbol{x}) \in \bigcup_{i=1}^{k} \bigcap_{j=1}^{m(i)} K_{\boldsymbol{x}}(S_{ij}).$$

It is possible to formulate inference rules based on Nagumo's theorem which allow one to prove positive invariance of a large class of closed semi-algebraic sets. This has previously been investigated in [29], where a number of inference rules are presented for checking positive invariance of closed sets of the form $h \geq 0$. For instance, it is shown that the following is a sound inference (similar to Lie):

$$\frac{h = 0 \rightarrow \mathfrak{L}_{\boldsymbol{p}}(h) \geq 0 \wedge \nabla h \neq \mathbf{0}}{h \geq 0 \rightarrow [\dot{\boldsymbol{x}} = \boldsymbol{p}]\, h \geq 0},$$

along with other rules with more general premises, all of which seek to check membership of $\boldsymbol{p}(\boldsymbol{x})$ in the contingent cone $K_{\boldsymbol{x}}(h \geq 0)$. The lifting of the conditions to formulas with boolean connectives (leading to a potential proof rule for closed semi-algebraic sets) described in [29, p. 393] essentially requires each S_{ij} to be of the form $h_{ij} \geq 0$ and assumes the soundness-critical property (10). Soundness issues may arise when this assumption fails to hold (as in Fig. 2). This deficiency can be fixed by e.g. requiring the matrix of partial derivatives of active components on the boundary to be full rank, i.e. $rk(\nabla h_1, \nabla h_2, \ldots, \nabla h_k) = k$ whenever the polynomials $h_1, h_2, \ldots, h_k$ evaluate to 0 on the boundary (this need only apply to conjunctive components). A number of other possible *sufficient conditions* for removing this source of unsoundness has been studied in non-smooth analysis [33] (see also *practical sets* in [2]). However, in practice, even ensuring the full-rank property for a matrix with polynomial entries is computationally expensive. Furthermore, even with conditions for soundness in place, the result may not be applied to reason about positive invariance of semi-algebraic sets that are neither closed nor open.

5.4. Liu, Zhan & Zhao Decision Procedure

In [16], it was shown that checking whether a given semi-algebraic set is positively invariant under the flow of a polynomial vector field is *decidable*. The conditions one is required to check are phrased in terms of set inclusion of semi-algebraic sets, which can be determined using a decision procedure for real arithmetic. The result builds on ideas described earlier in [29] and crucially depends on the property of solutions to differential equations with analytic right-hand sides being themselves analytic. In the remainder of this section, we rephrase and provide a detailed illustration of the main components of the result presented in [16].

Theorem 16. *Let $h : \mathbb{R}^n \to \mathbb{R}$ be an analytic function and $\dot{\boldsymbol{x}} = \boldsymbol{p}$ be an analytic system of ODEs. If $\boldsymbol{x}_0 \in \mathbb{R}^n$ is such that $h(\boldsymbol{x}_0) = 0$, then one has three possibilities at $\boldsymbol{x}_0$:*

1. $\exists\, N > 0.\ \mathfrak{L}_{\boldsymbol{p}}^{(N)}(h) < 0\ \bigwedge_{i=1}^{N-1} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h) = 0$,
2. $\exists\, N > 0.\ \mathfrak{L}_{\boldsymbol{p}}^{(N)}(h) > 0\ \bigwedge_{i=1}^{N-1} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h) = 0$,
3. $\forall\, N > 0.\ \bigwedge_{i=1}^{N} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h) = 0$.

If $\boldsymbol{x}(0) = \boldsymbol{x}_0$, then in case 1 one has $h(\boldsymbol{x}(t)) < 0$ for all $t \in (0, \epsilon)$ for some $\epsilon > 0$; case 2 is analogous, but with $h(\boldsymbol{x}(t)) > 0$ for all $t \in (0, \epsilon)$. In case 3, one is guaranteed that $h(\boldsymbol{x}(t)) = 0$ for all $t \in (0, \epsilon)$.

Proof. Since both h and the solution to the analytic ODE are analytic functions, the Taylor series expansion of $h(\varphi_t(\boldsymbol{x}_0))$ around $t = 0$ is given by

$$h(\boldsymbol{x}_0) + \sum_{i=1}^{\infty} \left(\frac{t^i}{i!} \cdot \frac{d^i h}{dt^i}\bigg|_{\boldsymbol{x}_0} \right) = \sum_{i=1}^{\infty} \left(\frac{t^i}{i!} \cdot \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h)\big|_{\boldsymbol{x}_0} \right)$$

and *converges* on some non-empty open interval of t containing zero. Thus, the most significant term to become sign-definite will determine the sign of the entire sum on some sufficiently small interval. See [16, Proof of Proposition 9]. See also [29, Proof of Theorem 7], which employed very much the same ideas as [16]. □

The following theorem is a simple corollary to [16, Theorem 19].

Theorem 17 (Liu, Zhan & Zhao [16])**.** *Given a polynomial system $\dot{\boldsymbol{x}} = \boldsymbol{p}(\boldsymbol{x})$, and a semi-algebraic set $S \subseteq \mathbb{R}^n$, define*

$$\mathrm{In}_{\boldsymbol{p}}(S) \equiv \{\boldsymbol{x} \in \mathbb{R}^n \mid \exists\, \epsilon > 0.\, \forall\, t \in (0, \epsilon).\, \boldsymbol{x}(t) \in S\},$$
$$\mathrm{In}_{(-\boldsymbol{p})}(S) \equiv \{\boldsymbol{x} \in \mathbb{R}^n \mid \exists\, \epsilon > 0.\, \forall\, t \in (0, \epsilon).\, \boldsymbol{x}(-t) \in S\},$$

where $\boldsymbol{x}(t)$ is the solution to the initial value problem $(\dot{\boldsymbol{x}} = \boldsymbol{p}(\boldsymbol{x}), \boldsymbol{x}(0) = \boldsymbol{x}_0)$ at time t. The set S is positively invariant under the flow of the system if and only if the inclusions $\mathrm{In}_{(-\boldsymbol{p})}(S) \subseteq S \subseteq \mathrm{In}_{\boldsymbol{p}}(S)$ hold, which implies soundness (and relative completeness) of the following rule of inference:

$$(\mathrm{LZZ})\frac{\big(\mathrm{In}_{(-\boldsymbol{p})}(S) \to S\big) \wedge (S \to \mathrm{In}_{\boldsymbol{p}}(S))}{S \to [\dot{\boldsymbol{x}} = \boldsymbol{p}]\, S}.$$

To develop some intuition for the construction of $\mathrm{In}_{\boldsymbol{p}}(S)$, let us first consider the case where S is characterized by a single non-strict inequality $h \leq 0$. Whenever h is an analytic function, one may use Theorem 16 to give a characterization of $\mathrm{In}_{\boldsymbol{p}}(h \leq 0)$ as the set of states in $\mathbb{R}^n$ that satisfy the following *infinite* set of conditions (cf. [29, Theorem 7, Theorem 8]):

$$\begin{aligned}
h < 0 \quad &\vee \\
(h = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}(h) < 0) \quad &\vee \\
(h = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}(h) = 0 \wedge \mathfrak{L}^{(2)}_{\boldsymbol{p}}(h) < 0) \quad &\vee \\
(h = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}(h) = 0 \wedge \mathfrak{L}^{(2)}_{\boldsymbol{p}}(h) = 0 \wedge \mathfrak{L}^{(3)}_{\boldsymbol{p}}(h) < 0) \quad &\vee \\
&\vdots
\end{aligned}$$

The *decidability* of checking the conditions in Proposition 17 (i.e. the premise of LZZ) hinges on the ability to construct *semi-algebraic sets* $\mathrm{In}_{\boldsymbol{p}}(S)$ whenever S is semi-algebraic. In [16] the authors make the crucial observation that whenever h is a polynomial and $\dot{\boldsymbol{x}} = \boldsymbol{p}(\boldsymbol{x})$ is a system of polynomial ODEs, then the Lie derivatives $\mathfrak{L}^{(i)}_{\boldsymbol{p}}(h)$ up to any order i are also polynomials. Using the fact that the ring of multivariate polynomials with coefficients in some Noetherian ring is also Noetherian (by Hilbert's basis theorem), the set $\mathrm{In}_{\boldsymbol{p}}(h \leq 0)$ can be characterized by a *finite* disjunction [16]:

$$\begin{aligned}
h < 0 \quad &\vee \\
(h = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}(h) < 0) \quad &\vee \\
(h = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}(h) = 0 \wedge \mathfrak{L}^{(2)}_{\boldsymbol{p}}(h) < 0) \quad &\vee \\
&\vdots \\
(h = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}(h) = 0 \wedge \mathfrak{L}^{(2)}_{\boldsymbol{p}}(h) = 0 \wedge \cdots \wedge \mathfrak{L}^{(N-1)}_{\boldsymbol{p}}(h) < 0) \quad &\vee \\
(h = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}(h) = 0 \wedge \mathfrak{L}^{(2)}_{\boldsymbol{p}}(h) = 0 \wedge \cdots \wedge \mathfrak{L}^{(N-1)}_{\boldsymbol{p}}(h) = 0 \wedge \mathfrak{L}^{(N)}_{\boldsymbol{p}}(h) \leq 0).&
\end{aligned}$$

The ascending chain property of Noetherian rings guarantees that there is a finite positive integer N such that for all $N' > N$ we have the following ideal membership:

$$\mathfrak{L}_{\boldsymbol{p}}^{(N')}(h) \in \langle h, \mathfrak{L}_{\boldsymbol{p}}(h), \ldots, \mathfrak{L}_{\boldsymbol{p}}^{(N)}(h) \rangle.$$

The integer N may be found using Gröbner bases to successively check for ideal membership of $\mathfrak{L}_{\boldsymbol{p}}^{(N)}(h)$ in the ideal generated by the Lie derivatives of orders lower than N for $N = 1, 2, 3, \ldots$ until the ideal saturates (as with DRI). Once N is found, if the formula

$$(h = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}(h) = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}^{(2)}(h) = 0 \wedge \cdots \wedge \mathfrak{L}_{\boldsymbol{p}}^{(N-1)}(h) = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}^{(N)}(h) = 0)$$

holds, then for any $N' \geq N$ we have

$$(h = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}(h) = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}^{(2)}(h) = 0 \wedge \cdots \wedge \mathfrak{L}_{\boldsymbol{p}}^{(N-1)}(h) = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}^{(N)}(h) = 0 \wedge \cdots \wedge \mathfrak{L}_{\boldsymbol{p}}^{(N')}(h) = 0),$$

which removes the need to consider disjuncts with Lie derivatives of orders higher than N, as all the (infinitely many) formulas

$$(h = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}(h) = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}^{(2)}(h) = 0 \wedge \cdots \wedge \mathfrak{L}_{\boldsymbol{p}}^{(N-1)}(h) = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}^{(N)}(h) = 0 \wedge \cdots \wedge \mathfrak{L}_{\boldsymbol{p}}^{(N')}(h) < 0),$$

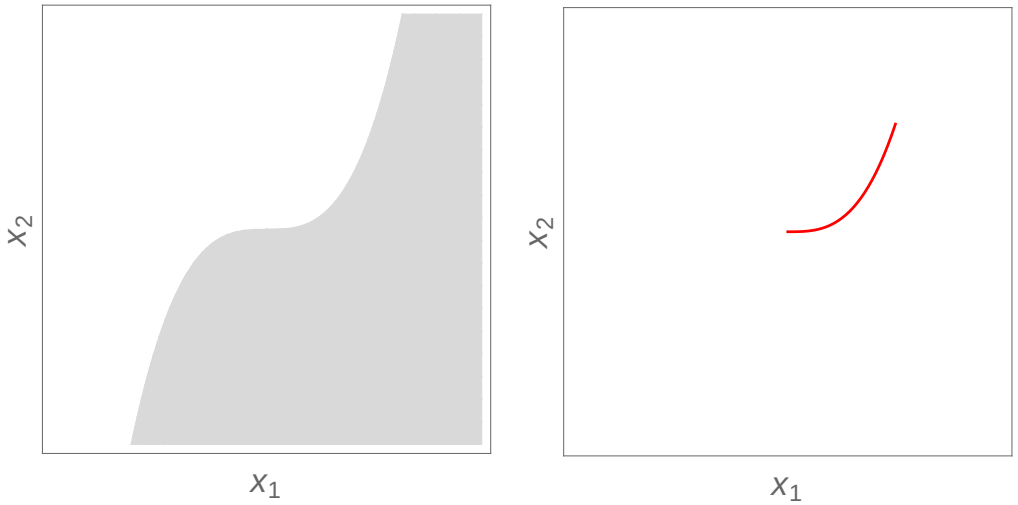
with $N' > N$ are guaranteed to be false.

Remark 18. *The ascending chain property is crucial in making it possible to reason about sign conditions of* infinitely many *higher-order Lie derivatives by only considering a* finite *number of sign conditions. The same idea was independently pursued in [10] to give a necessary and sufficient criterion for invariance of real algebraic sets under the flow of polynomial ODEs (summarized in the proof rule* DRI*; discussed earlier).*

Thus, by computing N for a given polynomial h and a system $\dot{\boldsymbol{x}} = \boldsymbol{p}(\boldsymbol{x})$, one may construct a *semi-algebraic* set $\mathrm{In}_{\boldsymbol{p}}(h \leq 0)$. In Fig. 3d we detail the computation for $N = 3$ and depict the different "pieces" involved to form $\mathrm{In}_{\boldsymbol{p}}(h \leq 0)$, which is, in this particular case, the same as $h \leq 0$ as shown in Fig. 4b.

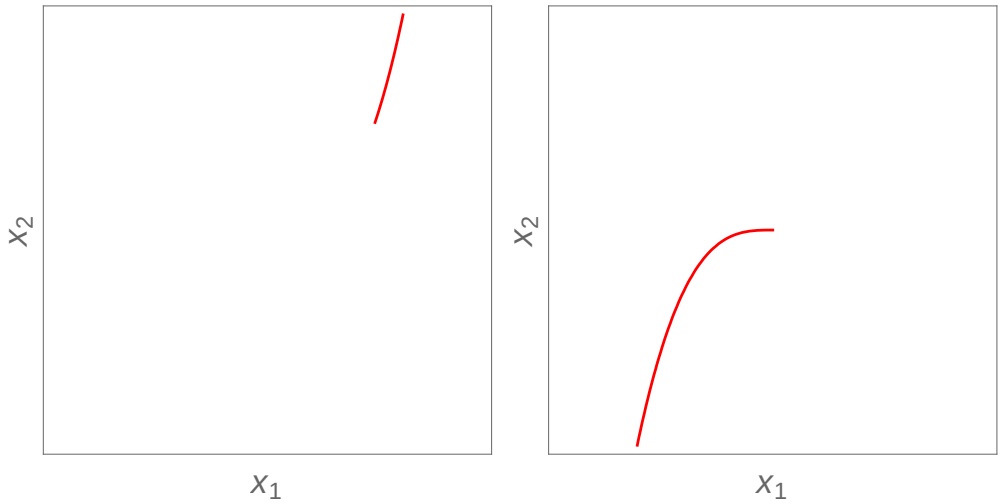
Likewise in the case of strict polynomial inequalities $h < 0$, the set $\mathrm{In}_{\boldsymbol{p}}(h < 0)$ is semi-algebraic and is characterized by the following formula:

$$
\begin{aligned}
h < 0 \quad &\vee \\
(h = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}(h) < 0) \quad &\vee \\
(h = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}(h) = 0 \wedge \mathfrak{L}^{(2)}_{\boldsymbol{p}}(h) < 0) \quad &\vee \\
&\vdots \\
(h = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}(h) = 0 \wedge \mathfrak{L}^{(2)}_{\boldsymbol{p}}(h) = 0 \wedge \cdots \wedge \mathfrak{L}^{(N-1)}_{\boldsymbol{p}}(h) < 0) \quad &\vee \\
(h = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}(h) = 0 \wedge \mathfrak{L}^{(2)}_{\boldsymbol{p}}(h) = 0 \wedge \cdots \wedge \mathfrak{L}^{(N-1)}_{\boldsymbol{p}}(h) = 0 \wedge \mathfrak{L}^{(N)}_{\boldsymbol{p}}(h) < 0).
\end{aligned}
$$



(a) $\mathfrak{L}_{\boldsymbol{p}}^{(0)}(h) < 0$ (i.e. $h < 0$)

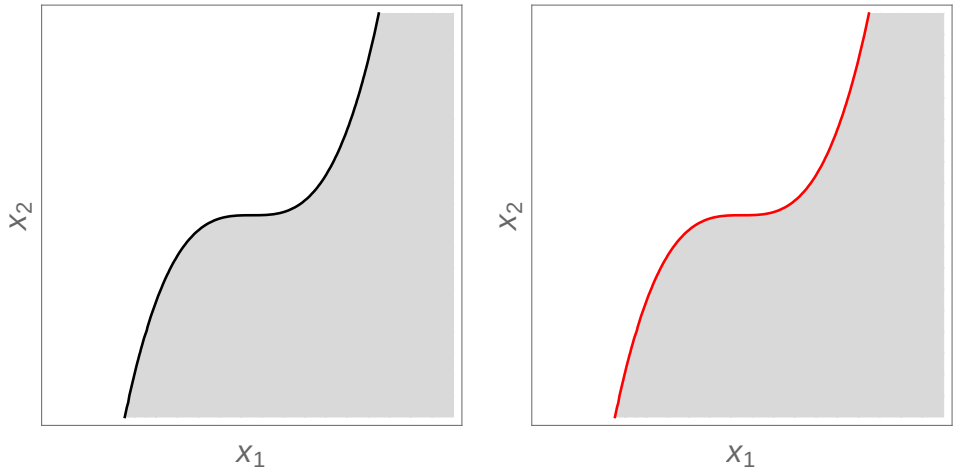
(b) $h = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}(h) < 0$



(c) $h = \mathfrak{L}_{\boldsymbol{p}}(h) = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}^{(2)}(h) < 0$

(d) $h = \mathfrak{L}_{\boldsymbol{p}}(h) = \mathfrak{L}_{\boldsymbol{p}}^{(2)}(h) = 0 \wedge \mathfrak{L}_{\boldsymbol{p}}^{(3)}(h) \leq 0$

Figure 3: Sign conditions on Lie derivatives in the construction of $\mathrm{In}_{\boldsymbol{p}}(h \leq 0)$ with $N = 3$.



(a) $h \leq 0$ (b) $\mathrm{In}_{\boldsymbol{p}}(h \leq 0)$

Figure 4: Constructing $\mathrm{In}_{\boldsymbol{p}}(h \leq 0)$ using higher-order Lie derivatives.

In order to construct $\mathrm{In}_{\boldsymbol{p}}(\cdot)$ for semi-algebraic sets with boolean structure, an important distribution property, proved in [16, Theorem 20], is required. For convenience, the property is stated below.

Theorem 19 ([16])**.** *Given a polynomial system $\dot{\boldsymbol{x}} = \boldsymbol{p}(\boldsymbol{x})$ and a semi-algebraic set $S \equiv \bigvee_{i=1}^{k} \bigwedge_{j=1}^{m(i)} h_{ij} \sim 0$ where $\sim \in \{<, \leq\}$, we have*

$$\mathrm{In}_{\boldsymbol{p}}(S) \equiv \bigvee_{i=1}^{k} \bigwedge_{j=1}^{m(i)} \mathrm{In}_{\boldsymbol{p}}(h_{ij} \sim 0).$$

Finally, $\mathrm{In}_{(-\boldsymbol{p})}(S)$ is constructed in exactly the same way as $\mathrm{In}_{\boldsymbol{p}}(S)$, except the Lie derivatives are computed with respect to the vector field induced by the system in which time is reversed, i.e. $\dot{\boldsymbol{x}} = -\boldsymbol{p}(\boldsymbol{x})$. This is possible because

$$\frac{d}{dt}\boldsymbol{x}(-t) = -\boldsymbol{p}(\boldsymbol{x}(-t)),$$

and the solution to $\dot{\boldsymbol{x}} = -\boldsymbol{p}(\boldsymbol{x})$ is given by $\boldsymbol{x}(-t)$, where $\boldsymbol{x}(t)$ is the solution to $\dot{\boldsymbol{x}} = \boldsymbol{p}(\boldsymbol{x})$. Once all the semi-algebraic sets in the premise of LZZ are constructed, the validity of the premise can be decided using a decision procedure for real arithmetic [30].

6. Hierarchy

In this section, we compare the deductive power of the existing (Fig. 1) as well as the newly-introduced proof rules (Lie° and Lie^* in Section 4, and NSSBC in Section 5.2) for checking the invariance of algebraic and semi-algebraic sets. This study should be complemented by another comparison that considers the interaction between the different proof rules in the context of a formal proof system in a similar vein to [24]. We leave this for future work.

Given two proof rules R_1 and R_2 of the form

$$(\mathrm{R}_1)\frac{P_1}{(S_1 : T_1) \longrightarrow [\dot{\boldsymbol{x}} = \boldsymbol{p}](S_1 : T_1)} \quad (\mathrm{R}_2)\frac{P_2}{(S_2 : T_2) \longrightarrow [\dot{\boldsymbol{x}} = \boldsymbol{p}](S_2 : T_2)} \tag{11}$$

where P_i refers to the premise of the proof rule R_i, and the conclusion has the form $(S_1 : T_1) \longrightarrow [\dot{\boldsymbol{x}} = \boldsymbol{p}](S_1 : T_1)$, where $S_i : T_i$ denotes that the set S_i is of type T_i (the typical types we are considering in this work are algebraic and semi-algebraic sets).

Definition 20 (Partial order over proof rules)**.** *Let* R_1 *and* R_2 *be two proof rules of the form of Eq.* (11)*. We say that* R_2 *generalizes* R_1 *and write* $\mathrm{R}_2 \succcurlyeq \mathrm{R}_1$ *(or* $\mathrm{R}_1 \preccurlyeq \mathrm{R}_2$*), if the premise of* R_1 *implies the premise of* R_2 *(*$P_1 \to P_2$*), and* T_1 *is a subtype of* T_2 *(for instance, the type algebraic set is a subtype of the type semi-algebraic set).*

Intuitively, if the proof rule R_1 proves that $S_1 : T_1$ is an invariant for the vector field $\boldsymbol{p}$, then R_2 can be also applied to discharge the invariance of S_1. If $\mathrm{R}_1 \preccurlyeq \mathrm{R}_2$ and $\mathrm{R}_1 \succcurlyeq \mathrm{R}_2$, we say that R_1 and R_2 are equivalent, and denote this by $\mathrm{R}_1 \sim \mathrm{R}_2$. Observe that two equivalent proof rules operate necessarily on equivalents type of sets so T_1 and T_2 are equivalent. In a similar vein, $\mathrm{R}_1 \not\preccurlyeq \mathrm{R}_2$ (or $\mathrm{R}_2 \not\succcurlyeq \mathrm{R}_1$) denotes that R_1 is not generalized by R_2. So in the absence of other rules, a proof rule that operates on algebraic sets cannot generalize a proof rule for semi-algebraic sets. Finally, we also write $\mathrm{R}_1 \prec \mathrm{R}_2$ when $\mathrm{R}_1 \preccurlyeq \mathrm{R}_2$ and $\mathrm{R}_1 \not\succcurlyeq \mathrm{R}_2$. That is, the rule R_2 *increases* the deductive power of R_1.

It is easy to see that the order $\preccurlyeq$ is a partial order (with $\sim$ acting as equality): it is reflexive, $\mathrm{R} \preccurlyeq \mathrm{R}$ (the premise of R implies itself); it is anti-symmetric (by definition), and transitive: if $\mathrm{R}_1 \preccurlyeq \mathrm{R}_2$ and $\mathrm{R}_2 \preccurlyeq \mathrm{R}_3$, then the premise of R_1 implies the premise of R_3 by transitivity of the implication, so $\mathrm{R}_1 \preccurlyeq \mathrm{R}_3$. Finally, if $\mathrm{R}_1 \not\preccurlyeq \mathrm{R}_2$ and $\mathrm{R}_1 \not\succcurlyeq \mathrm{R}_2$, we will write $\mathrm{R}_1 \prec\succ \mathrm{R}_2$ and say that the proof rules R_1 and R_2 are *incomparable*. This means that for both R_1 and R_2 there are problems

that one rule can prove and the other cannot. Notice that a proof rule for invariance of a certain class of semi-algebraic sets does not automatically generalize a proof rule for invariance of algebraic sets, even though the subtype condition is satisfied. Such proof rules are likely to be incomparable.

In what follows we use the partial order ($\preccurlyeq$) to illustrate the lattice structure of the proof rules under consideration. We use $\preccurlyeq$ to compare the deductive power of the proof rules. On one hand, the proof rules for algebraic sets:

$$\{\mathrm{FI}, \mathrm{C\text{-}c}, \mathrm{P\text{-}c}, \mathrm{Lie}, \mathrm{Lie}^{\circ}, \mathrm{Lie}^{*}, \mathrm{DRI}\},$$

and, on the other hand, the proof rules for semi-algebraic sets:

$$\{\mathrm{NSSBC}, \mathrm{Nagumo}, \mathrm{DI}, \mathrm{LZZ}\} \ .$$

For convenience, the propositions of this section are summarized in the comparison matrices in Fig. 6 and Fig. 8. For instance, Prop. 25 proves that $\mathrm{FI} \prec\succ \mathrm{Lie}$. Cells without numbers are proved by transitivity of the partial order. For instance, $\mathrm{FI} \prec \mathrm{DRI}$ can be proved using $\mathrm{FI} \prec \mathrm{C\text{-}c}$ (Prop. 21) and $\mathrm{C\text{-}c} \prec \mathrm{P\text{-}c}$ (Prop. 22) and $\mathrm{P\text{-}c} \prec \mathrm{DRI}$ (Prop. 24). The Hasse diagram (Fig. 5) gives the lattice structure where arrows represent strictly increasing deductive power; every missing edge in the graph represents $\prec\succ$, as shown in the comparison matrix.

6.1. Proof Rules for Algebraic Sets

We begin by comparing Darboux-based proof rules, i.e. $\{\mathrm{FI}, \mathrm{C\text{-}c}, \mathrm{P\text{-}c}\}$ and then proceed to the Lie-based proof rule family, i.e. $\{\mathrm{Lie}, \mathrm{Lie}^{\circ}, \mathrm{Lie}^{*}\}$. Next, we demonstrate the deductive superiority of the necessary and sufficient conditions in the premise of the proof rule DRI. Finally, we show that Darboux-based proof rules and Lie-based proof rules form two *distinct* proof rule families; that is, any proof rule from one family is deductively incomparable to any proof rule from the other family.

Proposition 21. $\mathrm{FI} \prec \mathrm{C\text{-}c}$.

Proof. The premise of the rule $\mathrm{C\text{-}c}$ requires the existence of some $\lambda \in \mathbb{R}$, such that $\mathfrak{L}_{\boldsymbol{p}}(h) = \lambda h$. In particular, $\lambda = 0$ gives the premise of FI. Thus, $\mathrm{FI} \preccurlyeq \mathrm{C\text{-}c}$. To see that $\mathrm{FI} \not\succcurlyeq \mathrm{C\text{-}c}$, consider the one-dimensional vector field $\boldsymbol{p} = (x)$, we have $\mathfrak{L}_{\boldsymbol{p}}(x) = 1x$, and hence $\mathrm{C\text{-}c}$ ($\lambda = 1$) concludes that $x = 0$ is an invariant. However, FI cannot prove the invariance of $x = 0$ because x is not a conserved quantity in the system. □

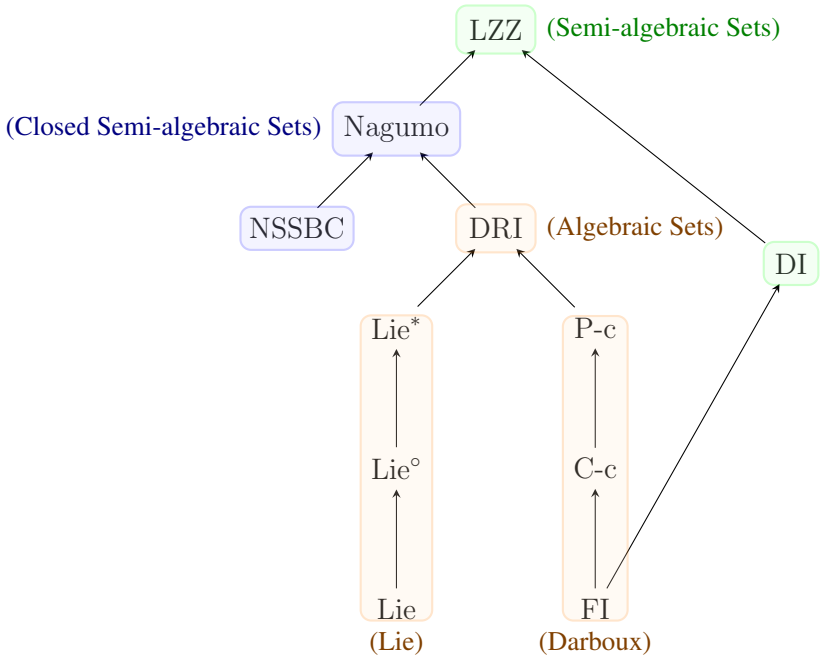


Figure 5: Hasse diagram. An arrow $\mathrm{R}_1 \to \mathrm{R}_2$ means $\mathrm{R}_1 \prec \mathrm{R}_2$; absence of connecting arrow(s) means $(\prec\succ)$.

Proposition 22. C-c $\prec$ P-c.

Proof. The premise of the rule P-c requires the existence of some $\alpha \in \mathbb{R}[\boldsymbol{x}]$, such that $\mathfrak{L}_{\boldsymbol{p}}(h) = \alpha h$ (equivalently, $\mathfrak{L}_{\boldsymbol{p}}(h) \in \langle h \rangle$). In particular, the constant polynomial gives the premise of C-c. Thus, C-c $\preccurlyeq$ P-c. To prove that C-c $\not\succcurlyeq$ P-c, consider the two-dimensional vector field $\boldsymbol{p} = (xy, x)$, we have $\mathfrak{L}_{\boldsymbol{p}}(x) = xy$ (or equivalently $\mathfrak{L}_{\boldsymbol{p}}(x) \in \langle x \rangle \subset \mathbb{R}[x, y]$) and hence conclude, using P-c, that $x = 0$ is an invariant. However, C-c fails to prove this invariant as the required cofactor is not a scalar. □

Proposition 23. Lie $\prec$ Lie° *and* Lie° $\prec$ Lie*.

Proof. We already established that Lie $\preccurlyeq$ Lie° (Prop. 8) and Lie° $\preccurlyeq$ Lie* (Prop. 7); we give two counterexamples to establish the strict inclusion. (**I**) Lie $\not\preccurlyeq$ Lie°. Whenever the variety has a singularity, the proof rule Lie will fail. Lie° is tailored to prove invariance of equilibrium points in addition to regular points of the variety. For instance, for $\boldsymbol{p} = ((-1 + x_1)x_2, x_2(1 + x_2))$, Lie fails to prove that $h = (-1+x_1)^2+(1+x_2)^2 = 0$ is invariant as the gradient ∇h vanishes at $(1, -1)$

	FI	C-c	P-c	Lie	Lie$^\circ$	Lie*	DRI
FI	$\sim$	$\prec$ 21	$\prec$	$\prec\!\succ$ 25	$\prec\!\succ$ 28	$\prec\!\succ$ 27	$\prec$
C-c	$\succ$ 21	$\sim$	$\prec$ 22	$\prec\!\succ$ 29	$\prec\!\succ$ 30	$\prec\!\succ$ 30	$\prec$
P-c	$\succ$	$\succ$ 22	$\sim$	$\prec\!\succ$ 29	$\prec\!\succ$ 30	$\prec\!\succ$ 30	$\prec$ 24
Lie	$\prec\!\succ$ 25	$\prec\!\succ$ 29	$\prec\!\succ$ 29	$\sim$	$\prec$ 23	$\prec$	$\prec$
Lie$^\circ$	$\prec\!\succ$ 28	$\prec\!\succ$ 30	$\prec\!\succ$ 30	$\succ$ 23	$\sim$	$\prec$ 23	$\prec$
Lie*	$\prec\!\succ$ 27	$\prec\!\succ$ 30	$\prec\!\succ$ 30	$\succ$	$\succ$ 23	$\sim$	$\prec$ 24
DRI	$\succ$	$\succ$	$\succ$	$\succ$	$\succ$	$\succ$	$\sim$

Figure 6: Comparison matrix for proof rules for algebraic sets (the numbers refer to the respective propositions).

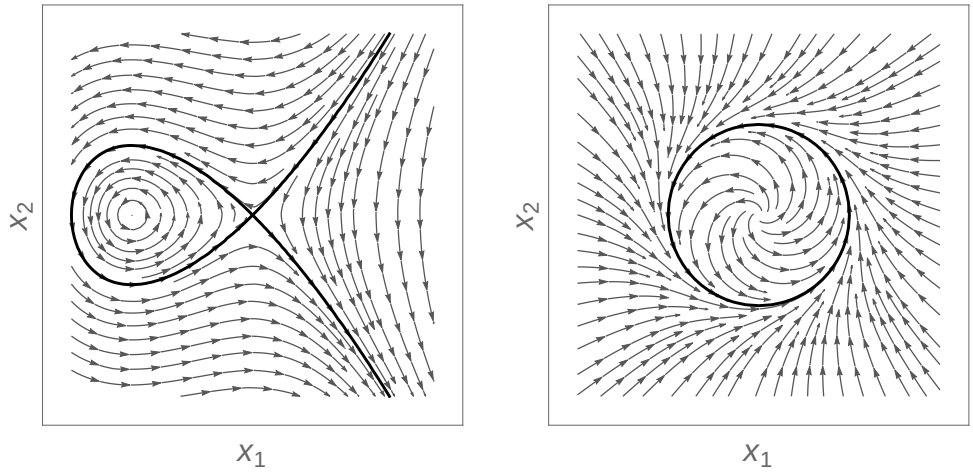
and $h((1,-1)) = 0$. However, at $(1,-1)$ we also have $p_1 = p_2 = 0$, and hence the premise of Lie$^\circ$ is satisfied, and $h = 0$ is proved to be an invariant under the flow of $\boldsymbol{p}$. (**II**) Lie$^\circ \not\preccurlyeq$ Lie*. In addition to equilibria, Lie* goes one step further and handles all singular points, $\boldsymbol{x}$, where the vector $\boldsymbol{x} + \lambda\boldsymbol{p}$ is in the variety $V_{\mathbb{R}}(h)$ for all $\lambda \in \mathbb{R}$ (that is $h(\boldsymbol{x} + \lambda\boldsymbol{p}) = 0$, for all λ). For instance, consider the polynomial $h = x_1x_2x_3$, its singular locus is given by the three axes $x_1 = x_2 = 0$, $x_1 = x_3 = 0$ and $x_2 = x_3 = 0$. For the vector field $\boldsymbol{p} = (x_1, x_2, x_3)$, the equilibrium point is at the origin $(0,0,0)$, which obviously does not contain the entire singular locus of h. Thus, Lie$^\circ$ fails but Lie* succeeds because $h(\boldsymbol{x} + \lambda\boldsymbol{p}) = 0$ when $\boldsymbol{x}$ is a point of one of the axes. □

Proposition 24. P-c $\prec$ DRI *and* Lie* $\prec$ DRI.

Proof. DRI is both necessary and sufficient [10], so we know that P-c $\preccurlyeq$ DRI and Lie* $\preccurlyeq$ DRI. To prove the claim it is left to show that (**I**) P-c $\not\succcurlyeq$ DRI. Consider the following two-dimensional vector field: $\boldsymbol{p} = ((-1+x_1)(1+x_1), (-1+x_2)(1+x_2))$. The candidate invariant (given by the roots of the Motzkin polynomial) $h = 1 - 3x_1^2x_2^2 + x_1^4x_2^2 + x_1^2x_2^4 = 0$ cannot be proved using P-c, as $\mathfrak{L}_{\boldsymbol{p}}(h) \notin \langle h \rangle$. However, the invariance property may be proved using DRI. For this, we need to consider the second-order Lie derivative of h and we prove that $\mathfrak{L}^{(2)}_{\boldsymbol{p}}(h) \in \langle h, \mathfrak{L}_{\boldsymbol{p}}(h) \rangle$. Thus, the premise of DRI holds for $N = 2$. (**II**) Lie$^* \not\succcurlyeq$ DRI. Consider the following three-dimensional vector field $\boldsymbol{p} = (-x_2 + x_1(1 - x_1^2 -$

$x_2^2), x_1 + x_2(1 - x_1^2 - x_2^2), x_3)$. We want to prove that $h = (-1 + x_1^2 + x_2^2)^2 + x_3^2 = 0$ is an invariant. In this case, the variety $V_{\mathbb{R}}(h)$ is exactly equal to the singular locus of h which is the two-dimensional unit circle $-1 + x_1^2 + x_2^2 = 0$. However, at all points of this unit circle, the vector field $\boldsymbol{p}$ is equal to $(-x_2, x_1, 0) \neq 0$, which prevents us from using Lie^* (because $h((x_1, x_2, 0) + \lambda(-x_2, x_1, 0)) \neq 0$ for some $\lambda \in \mathbb{R}$). The rule DRI proves the invariance of $h = 0$ with $N = 2$. □

To appreciate the difference between FI and Lie, let us note that while the condition in the premise of FI may seem strong (i.e. too conservative), singularities in the invariant candidate do not present a problem for FI, whereas the premise of Lie rules out such candidates altogether (see Fig. 7). Indeed, the proof rule Lie cannot prove that $0 = 0$ (the whole space is invariant), whereas this is the most trivial case for FI.



(a) Positive invariance of the variety $V_{\mathbb{R}}(x_1^2 + x_1^3 - x_2^2)$ provable using FI (but not Lie since $(0, 0)$ is a singular point).

(b) Smooth invariant limit cycle $V_{\mathbb{R}}(x_1^2 + x_2^2 - 1)$ provable using Lie (but not FI since $x_1^2 + x_2^2 - 1$ is not an invariant function).

Figure 7: Invariant functions and invariant equations.

Proposition 25 (FI and Lie are incomparable.)**.** FI $\prec\succ$ Lie.

Proof. (**I**) FI $\not\preccurlyeq$ Lie. For the vector field $\boldsymbol{p} = (-2x_2, -2x_1 - 3x_1^2)$, the equation $x_1^2 + x_1^3 - x_2^2 = 0$ is provable with FI but not Lie, see Fig. 7 (left). (**II**) FI $\not\preccurlyeq$ Lie. For the vector field $\boldsymbol{p} = (x_1 - x_1^3 - x_2 - x_1x_2^2, x_1 + x_2 - x_1^2x_2 - x_2^3)$, the invariance

of the limiting cycle $x_1^2 + x_2^2 - 1 = 0$ is provable with Lie but not FI, see Fig. 7 (right). □

We now prove that Lie-based proof rules $\{\text{Lie}, \text{Lie}^\circ, \text{Lie}^*\}$, and Darboux-based proof rules $\{\text{FI}, \text{C-c}, \text{P-c}\}$ are two distinct families of proof rules; that is, any Lie-based proof is deductively incomparable to any Darboux-based proof rule. The following lemma follows from the transitivity of the partial order.

Lemma 26. *If* $R_1 \preccurlyeq R_2$ *and* $R_3 \prec\succ R_1$*, then* $R_2 \not\preccurlyeq R_3$.

Proof. Consider three proof rules R_1, R_2 and R_3. If $R_2 \preccurlyeq R_3$, using $R_1 \preccurlyeq R_2$, one gets by transitivity $R_1 \preccurlyeq R_3$, which contradicts the assumption $R_3 \prec\succ R_1$. □

Proposition 27. $\text{FI} \prec\succ \text{Lie}^*$.

Proof. Since $\text{Lie} \preccurlyeq \text{Lie}^\circ$ (Prop. 8) and $\text{Lie}^\circ \preccurlyeq \text{Lie}^*$ (Prop. 7), $\text{Lie} \preccurlyeq \text{Lie}^*$. By Lem. 26, from $\text{Lie} \preccurlyeq \text{Lie}^*$ and $\text{FI} \prec\succ \text{Lie}$ (Prop. 25), we obtain $\text{Lie}^* \not\preccurlyeq \text{FI}$. The following example proves that $\text{FI} \not\preccurlyeq \text{Lie}^*$: Consider the three-dimensional vector field $\boldsymbol{p} = (x_2, -x_1, 0)$. The invariance of the equation $x_3^2 + (-1 + x_1^2 + x_2^2 + x_3^2)^2 = 0$ cannot be established using Lie^* (the singular locus is a circle in $\mathbb{R}^3$), but is easily provable using FI as $\mathfrak{L}_{\boldsymbol{p}}(h)$ vanishes. □

Proposition 28. $\text{FI} \prec\succ \text{Lie}^\circ$.

Proof. By Lem. 26, from $\text{Lie} \preccurlyeq \text{Lie}^\circ$ (Prop. 8) and $\text{FI} \prec\succ \text{Lie}$ (Prop. 25), we get $\text{Lie}^\circ \not\preccurlyeq \text{FI}$. On the other hand, if $\text{FI} \preccurlyeq \text{Lie}^\circ$ then, by transitivity $\text{FI} \preccurlyeq \text{Lie}^*$ (since $\text{Lie}^\circ \preccurlyeq \text{Lie}^*$ by Prop. 7), which contradicts $\text{FI} \prec\succ \text{Lie}^*$ (Prop. 27). Thus, $\text{FI} \not\preccurlyeq \text{Lie}^\circ$, and the proposition follows. □

Similarly, by substituting FI by Lie, Lie^* by P-c, and Lie° by C-c in Prop. 27 and Prop. 28 as well as their respective proofs, we show that:

Proposition 29. $\text{Lie} \prec\succ \text{P-c}$ *and* $\text{Lie} \prec\succ \text{C-c}$.

Proof. To complete the proof, we still need an example showing that $\text{Lie} \not\preccurlyeq \text{P-c}$. Consider the vector field $\boldsymbol{p} = (3(-4 + x^2), 3 + xy - y^2)$, the proof rule Lie fails to prove that the equation $h = -3 + x^2 + 2xy + 6y^2 + 2xy^3 + y^4 = 0$ is invariant as the singular locus of h contains $(-2, 1)$ and $(2, -1)$. However, $\mathfrak{L}_{\boldsymbol{p}}(h) = (6x - 4y)h$ and therefore P-c proves that $h = 0$ is an invariant equation. □

The remaining cases follow from the results established above.

	NSSBC	Nagumo	DI	LZZ
NSSBC	$\sim$	$\prec$ 32	$\prec\!\succ$ 34	$\prec$
Nagumo	$\succ$ 32	$\sim$	$\prec\!\succ$ 35	$\prec$ 33
DI	$\prec\!\succ$ 34	$\prec\!\succ$ 35	$\sim$	$\prec$ 33
LZZ	$\succ$	$\succ$ 33	$\succ$ 33	$\sim$

Figure 8: Comparison matrix for proof rules for semi-algebraic sets (the numbers refer to the propositions).

Proposition 30. *For* $d \in \{\text{C-c}, \text{P-c}\}$, $\ell \in \{\text{Lie}^\circ, \text{Lie}^*\}$, $d \prec\!\succ \ell$.

Proof. Since FI $\prec d$, if $d \preccurlyeq \ell$, then FI $\preccurlyeq \ell$. However, FI $\prec\!\succ \ell$ (Prop. 27 and Prop. 28). Thus $d \not\preccurlyeq \ell$. Similarly, since $l \succ \text{Lie}$, if $d \succcurlyeq \ell$, then $d \succcurlyeq \text{Lie}$ which contradicts $d \prec\!\succ \text{Lie}$ (Prop. 29). Hence $d \not\succcurlyeq \ell$ and the proposition follows. □

Remark 31. *Provided that the invariant candidate has no singular points, Lie's criterion is known to be both necessary and sufficient to prove invariance properties of level sets [20, Theorem 2.8]. Also,* FI *characterizes invariant functions [23] but not all invariant equations. On the other hand, for algebraic differential equations, the differential radical criterion in* DRI *fully characterizes all invariant algebraic sets [10]. Thus, as established in Prop. 24,* DRI *increases the deductive power of both Darboux-based rules* $\{\text{FI}, \text{C-c}, \text{P-c}\}$ *and Lie-based rules* $\{\text{Lie}, \text{Lie}^\circ, \text{Lie}^*\}$*, which form different families.*

6.2. Proof Rules for Semi-Algebraic Sets

In this section, we compare the deductive power of the proof rules

$$\{\text{NSSBC}, \text{Nagumo}, \text{DI}, \text{LZZ}\},$$

as well as their relationships to the proof rules for checking the invariance of algebraic sets.

Proposition 32. NSSBC $\prec$ Nagumo.

Proof. The Nagumo theorem characterizes closed positively invariant sets under the flow of locally Lipschitz ODEs. In particular, this covers closed semi-algebraic

sets and polynomial ODE. Hence $\mathrm{NSSBC} \preccurlyeq \mathrm{Nagumo}$. To see why the inequality is strict, consider any vector field with an invariant algebraic set (recall that algebraic sets are special closed semi-algebraic sets with empty interior). The proof rule NSSBC cannot work for such invariant sets precisely because it requires $\mathfrak{L}_{\boldsymbol{p}}(h) < 0$ whenever $h = 0$. In fact, $h = 0 \rightarrow \mathfrak{L}_{\boldsymbol{p}}(h) = 0$ is a necessary condition for any invariant algebraic set. □

Proposition 33. $\mathrm{Nagumo} \prec \mathrm{LZZ}$ *and* $\mathrm{DI} \prec \mathrm{LZZ}$.

Proof. For semi-algebraic sets, the proof rule LZZ characterizes (arbitrary) invariant semi-algebraic sets for polynomial ODE. The Nagumo theorem only characterizes closed semi-algebraic sets. Hence the strict inequality. Similarly, DI gives only a sufficient condition and is therefore strictly less powerful than LZZ. □

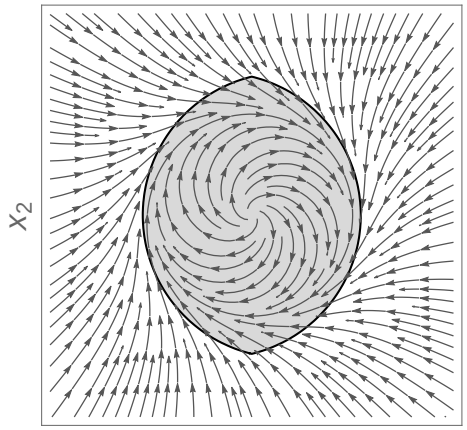
Proposition 34. $\mathrm{NSSBC} \prec\succ \mathrm{DI}$.

Proof. $\mathrm{DI} \not\succcurlyeq \mathrm{NSSBC}$. Consider the system

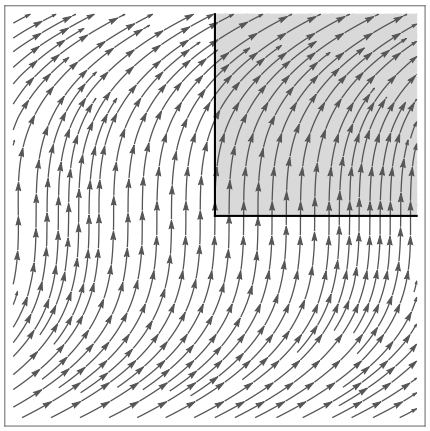
$$\boldsymbol{p}(\boldsymbol{x}) = \left(-\left(x_1^3 + x_2^2 x_1 - x_1 - x_2\right), -\left(x_2^3 + x_1^2 x_2 - x_2 + x_1\right)\right)$$

and let $S_1 \equiv \left(x_1 - \frac{1}{3}\right)^2 + x_2^2 - 2 \leq 0 \wedge \left(x_1 + \frac{1}{3}\right)^2 + x_2^2 - 2 \leq 0$, which is a positively invariant set under the flow of the system (see Fig. 9a). The invariance property cannot be proved using the rule DI, but is easily proved using NSSBC (and LZZ).

$\mathrm{NSSBC} \not\succcurlyeq \mathrm{DI}$. Consider the system $\boldsymbol{p}(\boldsymbol{x}) = (x_2^2, 2)$ and let $S_2 \equiv x_2 \geq 0 \wedge x_1 \geq 0$. Positive invariance of S_2 is proved easily using either DI (and LZZ), but cannot be proved using NSSBC. Intuitively, this can be seen because at the origin the vector $\boldsymbol{p}(\mathbf{0})$ does not point strictly into the interior of $S_2 \equiv \max(-x_2, -x_1) \leq 0$, since $\mathfrak{L}_{\boldsymbol{p}}(-x_1) = -x_2^2|_{\mathbf{0}} = 0$ (see Fig. 9b). □



(a) $S_1 \equiv \left(x_1 - \frac{1}{3}\right)^2 + x_2^2 - 2 \leq 0 \wedge \left(x_1 + \frac{1}{3}\right)^2 + x_2^2 - 2 \leq 0$



(b) $S_2 \equiv x_2 \geq 0 \wedge x_1 \geq 0$

Figure 9: Positive invariance of the semi-algebraic set S_1 (**left**) provable using NSSBC (but not DI) and a positive invariant S_2 (**right**) provable using DI (but not NSSBC).

Proposition 35. Nagumo $\prec\succ$ DI.

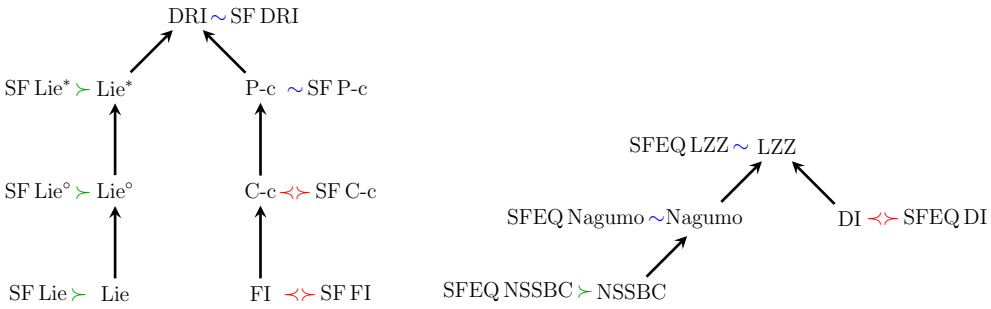
Proof. By Prop. 34 and Lem. 26, Nagumo $\not\preccurlyeq$ DI. In addition, the proof rule DI cannot be generalized by Nagumo since it can be applied to sets that are not necessarily closed or open, which is not the case with Nagumo. □

In Fig. 5, one can see that the proof rules for algebraic sets are incomparable with NSSBC. This is precisely because invariant algebraic sets are ruled out all together by the premise of NSSBC which requires the vector field to point inward on the boundaries. Furthermore, because only algebraic sets are allowed in the conclusion of those proof rules, they cannot generalize NSSBC nor DI which can be apply more generally. Thus:

Proposition 36. *Let* $\ell \in \{\text{FI}, \text{C-c}, \text{P-c}, \text{Lie}, \text{Lie}^\circ, \text{Lie}^*, \text{DRI}\}$*, then* $\ell \prec\succ$ NSSBC *and* $\ell \not\succcurlyeq$ DI.

The proof rule DI cannot generalize C-c, P-c, Lie ,Lie$^\circ$, Lie*, and DRI. For the same reason FI cannot generalize those proof rules (cf. Section 6.1). Thus:

Proposition 37. *Let* $\ell \in \{\text{C-c}, \text{P-c}, \text{Lie}, \text{Lie}^\circ, \text{Lie}^*, \text{DRI}\}$*, then* $\ell \prec\succ$ DI.



(a) Algebraic Sets (b) Semi-algebraic Sets

Figure 10: Square-free Reduction (Summary)

The generalization FI $\prec$ DI is a straightforward consequence of DI: in fact, by definition, the proof rule DI lifts, in a conservative way, the simplest condition for a differentiable function to be positive or negative—namely by checking if its derivative is positive or negative respectively—to a finite boolean formula of such functions. Said differently, the premise of FI is identical to the premise of DI when used for an atomic formula of the form $h = 0$.

Remark 38. *The premises of the proof rules for algebraic sets could be used to work with a larger class of invariant sets, namely those of the form $h \geq 0$ in addition to algebraic sets. For instance, if $\mathfrak{L}_{\boldsymbol{p}}(h) \in \langle h \rangle$, then necessarily $h \geq 0$ is an invariant of the system. In fact, the invariance of $h = 0$ implies the invariance of $h \bowtie 0$ for $\bowtie \in \{\leq, <, \geq, >\}$. Such extra proof rules do not bring any additional insight to the realm of proof rules depicted in Fig. 5 and are therefore not represented.*

7. Square-free Reduction

In this section we assess the utility of performing square-free reduction of invariant candidates as a means of (i) increasing the deductive power of certain proof rules to be identified and (ii) simplifying problems passed to decision procedures for real arithmetic. Our results are summarized in Fig. 10 for convenience.

7.1. Square-free Reduction with Lie-based Proof Rules

While Lie uses a powerful criterion that captures a large class of practically relevant invariant sets, it will fail for some seemingly simple invariant candidates. For instance, the condition in the premise of Lie will not hold when the goal is

to prove that $h = x^2 - 6x + 9 = 0$ is invariant, no matter what vector field one considers. The reason for this is simple: $x^2 - 6x + 9$ factorizes into $(x-3)^2$. The problem here lies in the polynomial h itself, rather than the real variety $V_{\mathbb{R}}(h)$. In fact, $V_{\mathbb{R}}(h)$ is exactly the singular locus of h and the proof rule Lie fails because *all* points inside $V_{\mathbb{R}}(h)$ are singular points. More generally, the chain rule implies $\nabla h^k \cdot \boldsymbol{p} = k h^{k-1} \nabla h \cdot \boldsymbol{p}$, which has the consequence that any polynomial h which is not square-free will have vanishing gradient at the real roots of factors with multiplicity greater than 1.

One can eliminate such annoying instances by reducing h to square-free form, which is a basic pre-processing step used in computer algebra systems. The square-free reduction of a polynomial h may be computed as follows:

$$\mathrm{SF}(h) = \frac{h}{\gcd\left(h, \frac{\partial h}{\partial x_1}, \ldots, \frac{\partial h}{\partial x_n}\right)}. \tag{12}$$

Intuitively, in performing square-free reduction we hope to shrink the singular locus of the original polynomial. If $\mathrm{SL}(\mathrm{SF}(h))$ is the empty set (which is the case for $h = x^2 - 6x + 9$ in the example given above), the proof rule Lie applies to $\mathrm{SF}(h)$ but not to h. In general, $\mathrm{SF}(h)$ may satisfy the assumptions of the proof rules Lie° or Lie^*, where h fails to do so. It is always sound to conclude that $h = 0$ is invariant from the knowledge that $\mathrm{SF}(h) = 0$ is invariant, since real varieties remain unaltered under square-free reduction of their defining polynomials [5], i.e. $V_{\mathbb{R}}(h) \equiv V_{\mathbb{R}}(\mathrm{SF}(h))$. Thus, replacing h with $\mathrm{SF}(h)$ in the premise of Lie, Lie° and Lie^* does not compromise soundness (it us a use of the generalization proof rule [21]) and enlarges the class of polynomials that these proof rules can work with.

Proposition 39. *For all* $\ell \in \{\mathrm{Lie}, \mathrm{Lie}^\circ, \mathrm{Lie}^*\}$, $\ell \prec \mathrm{SF}\,\ell$.

This result is unsurprising when one understands that Lie-based proof rules use geometric concepts to prove invariance properties of sets. In fact, the square-free reduction removes some purely algebraic oddities that prevent the geometric condition from holding true when checked syntactically by a machine.

In addition to increasing the deductive power, the square-free reduction reduces the total degree of the polynomial in the invariant candidate and hence serves to reduce the complexity of deciding the conditions in the premise (cf. discussion in Section 8). In our implementation, we adopt the convention that invariant candidates supplied to Lie and its generalizations are square-free reduced in a pre-processing step.

7.2. Square-free Reduction with Darboux-based proof rules

Unlike Lie-based proof rules, it is perhaps surprising that using square-free reduction as a pre-processing step for the proof rules FI and C-c, denoted SFFI and SFC-c respectively, does *not*, in general, increase the deductive power and may even lead to properties that are no longer provable.

Proposition 40. FI $\prec\succ$ SFFI.

Proof. (**I**) FI $\not\prec$ SFFI. The polynomial $h = x^2y$ is an invariant function for the vector field $\boldsymbol{p} = (\frac{\partial h}{\partial y}, -\frac{\partial h}{\partial x}) = (x^2, -2xy)$, thus FI proves the invariance of $h = 0$. However, $\mathrm{SF}(h)$ is not an invariant function for the same vector field, since $\mathfrak{L}_{\boldsymbol{p}}(\mathrm{SF}(h)) = \mathfrak{L}_{\boldsymbol{p}}(xy) = -x^2y \neq 0$, thus SFFI fails to prove the invariance of $h = 0$. (**II**) SFFI $\not\prec$ FI. Similarly, the polynomial $h = xy$ is an invariant function for the vector field $\boldsymbol{p} = (\frac{\partial h}{\partial y}, -\frac{\partial h}{\partial x}) = (x, -y)$, thus SFFI proves the invariance of $x^2y = 0$, since $\mathrm{SF}(x^2y) = h$. However, FI fails to prove the invariance of $x^2y = 0$, because $\mathfrak{L}_{\boldsymbol{p}}(x^2y) = x^2y \neq 0$. □

Prop. 40 may at first seem counter-intuitive. However, the criterion in the premise of FI is different as it proves that the candidate h is an *invariant function*. In performing square-free reduction on h, one in general obtains a different function, $\mathrm{SF}(h)$, which need not be conserved in the system if h is conserved or, conversely, may be conserved even if h is not.

The same observation holds for C-c as the SF reduction does not preserve the constant rate exponential decrease (or increase).

Proposition 41. C-c $\prec\succ$ SFC-c.

Proof. (**I**) C-c $\not\prec$ SFC-c. The proof rule C-c proves the invariance of $h = x^2y = 0$ for the vector field $\boldsymbol{p} = (x^2, y(1-2x))$ as $\mathfrak{L}_{\boldsymbol{p}}(h) = 1h$. However, C-c cannot prove $\mathrm{SF}(h) = 0$, since $\mathfrak{L}_{\boldsymbol{p}}(\mathrm{SF}(h)) = \mathfrak{L}_{\boldsymbol{p}}(xy) = (1-x)\,\mathrm{SF}(h)$. (**II**) SFC-c $\not\prec$ C-c. For the same h, C-c proves the invariance of $\mathrm{SF}(h) = 0$ for the vector field $\boldsymbol{p} = (x^2, y(1-x))$ as $\mathfrak{L}_{\boldsymbol{p}}(\mathrm{SF}(h)) = \mathfrak{L}_{\boldsymbol{p}}(xy) = 1\,\mathrm{SF}(h)$. However, without the SF reduction C-c alone fails to prove the invariance of $h = 0$ for the considered $\boldsymbol{p}$, as $\mathfrak{L}_{\boldsymbol{p}}(h) = (x+1)h$. □

After Prop. 40 and 41, one expects P-c to be incomparable with its square-free counterpart. Surprisingly, the proof rules P-c and SFP-c (which applies P-c after the square-free reduction) are in fact equivalent. This follows from the fact that a polynomial is Darboux for a vector field $\boldsymbol{p}$ if and only if all its factors are

also Darboux for the same vector field. Our findings are stated in Prop. 42 and its corollary Prop. 43.[5]

Proposition 42. *Let $h = q_1^{m_1} \cdots q_r^{m_r}$ denote the decomposition of the polynomial h into irreducible (over the reals) factors, q_i. Then, h is Darboux for $\boldsymbol{p}$ if and only if, for all i, q_i is Darboux for $\boldsymbol{p}$.*

Proof. If, for all i, the polynomial q_i is Darboux for $\boldsymbol{p}$, then q_i divides $\mathfrak{L}_{\boldsymbol{p}}(q_i)$, i.e. $\frac{\mathfrak{L}_{\boldsymbol{p}}(q_i)}{q_i} \in \mathbb{R}[x_1, \ldots, x_n]$. Therefore, using the chain rule,

$$\begin{aligned}
\mathfrak{L}_{\boldsymbol{p}}(h) &= \mathfrak{L}_{\boldsymbol{p}}(q_1^{m_1} \cdots q_r^{m_r}) && (13)\\
&= \sum_{i=1}^{r} \Big(m_i \mathfrak{L}_{\boldsymbol{p}}(q_i) q_i^{m_i - 1} \prod_{j \neq i} q_j^{m_j} \Big) && (14)\\
&= \sum_{i=1}^{r} m_i \mathfrak{L}_{\boldsymbol{p}}(q_i) q_i^{m_i - 1} \frac{h}{q_i^{m_i}} && (15)\\
&= h \sum_{i=1}^{r} m_i \frac{\mathfrak{L}_{\boldsymbol{p}}(q_i)}{q_i} && (16)\\
&\in \langle h \rangle, && (17)
\end{aligned}$$

and h is also Darboux for $\boldsymbol{p}$.

If h is Darboux for $\boldsymbol{p}$, then h divides $\mathfrak{L}_{\boldsymbol{p}}(h)$ and $\frac{\mathfrak{L}_{\boldsymbol{p}}(h)}{h}$ is a polynomial. Recall that $\mathrm{SF}(h) = q_1 \cdots q_r$. Using Eq. (16), one gets

$$\frac{\mathfrak{L}_{\boldsymbol{p}}(h)}{h} \mathrm{SF}(h) = \sum_{i=1}^{r} m_i \frac{\mathfrak{L}_{\boldsymbol{p}}(q_i)}{q_i} \mathrm{SF}(h) \quad . \tag{18}$$

For a fixed i, q_i divides $\mathrm{SF}(h)$, it thus divides the left hand side of Eq. (18). Moreover, q_i divides $\frac{\mathrm{SF}(h)}{q_j}$, for all $j \neq i$. It thus necessarily divides $m_i \frac{\mathrm{SF}(h)}{q_i} \mathfrak{L}_{\boldsymbol{p}}(q_i)$. If q_i divides $\frac{\mathrm{SF}(h)}{q_i}$, then there exists $j \neq i$ such that q_i divides q_j, which contradicts the fact that all factors $q_1, \ldots, q_r$ are irreducible. Thus, q_i divides $\mathfrak{L}_{\boldsymbol{p}}(q_i)$ and $\mathfrak{L}_{\boldsymbol{p}}(q_i) \in \langle q_i \rangle$. □

Proposition 43. P-c $\sim$ SFP-c.

[5] See [8, Proposition 8.4] for a similar proposition over the complex numbers.

Proof. The proof rule P-c proves the invariance of $h = 0$ for $\boldsymbol{p}$ if and only if the polynomial h is Darboux. However, by Prop. 42, h is Darboux if and only if $\mathrm{SF}(h)$ is also Darboux. Therefore, SFP-c could be used equivalently to prove the invariance of $h = 0$. □

Remark 44. *The condition $\mathfrak{L}_{\boldsymbol{p}}(h) \in \langle \mathrm{SF}(h) \rangle$—which is weaker than $\mathfrak{L}_{\boldsymbol{p}}(h) \in \langle h \rangle$—is not sufficient to prove the invariance of $h = 0$. It is therefore an unsound proof rule. Consider the polynomial $h = (-1 + x^2)^2$ and the 1-dimensional vector field $\dot{x} = x$. Although $\mathfrak{L}_{\boldsymbol{p}}(h) = 4(-1 + x^2)x^2 \in \langle -1 + x^2 \rangle = \langle \mathrm{SF}(h) \rangle$, the equation $h = 0$ is not invariant, however, because $x(t) = \pm e^t$. Notice that the proof rule* P-c *(with or without the square-free reduction) is unable to prove or disprove the invariance of $h = 0$.*

*7.3. Square-free Reduction On Differential Radical Invariants (*DRI*)*

Square-free reduction cannot increase the deductive power of the proof rule DRI because its premise is necessary and sufficient to prove invariance of real algebraic sets, which is unaffected by applying SF reduction. However, the computational impact of using square-free reduction with DRI remains an interesting question. Empirically, we observed a better performance of DRI when the SF reduction is applied first. In addition to lowering the degrees of the involved polynomials (as it did for Lie-based proof rules), we observed that the order N_{SF} for $\mathrm{SF}(h)$ is always lower than the order N for h. We, therefore, conjecture $N_{\mathrm{SF}} \leq N$. However, we identified an example (cf. Ex. 45 below) for which square-free reduction resulted in a significant ($\times 100$) computational overhead due to the ideal membership checking (which we perform using Gröbner bases with reverse lexicographic monomial ordering). In our implementation of DRI, called DRI_{opt} in the sequel, we use the square-free reduction only as a pre-processing step for the quantifier elimination problems in the premise of DRI.

Example 45. *Consider the following vector field $\mathbf{p}$:*

$$
\begin{aligned}
\dot{x_1} &= -24\,(x_1+x_3)\left(x_3^6-3x_1^2x_2^2x_3^2+x_1^2x_2^4+x_1^4x_2^2\right)x_4x_5\left(x_7^2+x_2-12341\right)^{16}\left(x_4x_5^2-12x_6x_8\right)^{11},\\
\dot{x_2} &= 144\,(x_1+x_3)\left(x_3^6-3x_1^2x_2^2x_3^2+x_1^2x_2^4+x_1^4x_2^2\right)\left(x_7^2+x_2-12341\right)^{16}x_8\left(x_4x_5^2-12x_6x_8\right)^{11},\\
\dot{x_3} &= -32\,(x_1+x_3)\left(x_3^6-3x_1^2x_2^2x_3^2+x_1^2x_2^4+x_1^4x_2^2\right)x_7\left(x_7^2+x_2-12341\right)^{15}\left(x_4x_5^2-12x_6x_8\right)^{12},\\
\dot{x_4} &= 144\,(x_1+x_3)\left(x_3^6-3x_1^2x_2^2x_3^2+x_1^2x_2^4+x_1^4x_2^2\right)x_6\left(x_7^2+x_2-12341\right)^{16}\left(x_4x_5^2-12x_6x_8\right)^{11},\\
\dot{x_5} &= (x_1+x_3)\left(2x_1x_2^4+4x_1^3x_2^2-6x_1x_3^2x_2^2\right)\left(x_4x_5^2-12x_6x_8\right)^{12}\left(x_7^2+x_2-12341\right)^{16}\\
&\quad+\left(x_3^6-3x_1^2x_2^2x_3^2+x_1^2x_2^4+x_1^4x_2^2\right)\left(x_4x_5^2-12x_6x_8\right)^{12}\left(x_7^2+x_2-12341\right)^{16},\\
\dot{x_6} &= (x_1+x_3)\left(2x_2x_1^4+4x_2^3x_1^2-6x_2x_3^2x_1^2\right)\left(x_4x_5^2-12x_6x_8\right)^{12}\left(x_7^2+x_2-12341\right)^{16}\\
&\quad+16\,(x_1+x_3)\left(x_3^6-3x_1^2x_2^2x_3^2+x_1^2x_2^4+x_1^4x_2^2\right)\left(x_4x_5^2-12x_6x_8\right)^{12}\left(x_7^2+x_2-12341\right)^{15},\\
\dot{x_7} &= (x_1+x_3)\left(6x_3^5-6x_1^2x_2^2x_3\right)\left(x_4x_5^2-12x_6x_8\right)^{12}\left(x_7^2+x_2-12341\right)^{16}\\
&\quad+\left(x_3^6-3x_1^2x_2^2x_3^2+x_1^2x_2^4+x_1^4x_2^2\right)\left(x_4x_5^2-12x_6x_8\right)^{12}\left(x_7^2+x_2-12341\right)^{16},\\
\dot{x_8} &= 12\,(x_1+x_3)\left(x_3^6-3x_1^2x_2^2x_3^2+x_1^2x_2^4+x_1^4x_2^2\right)x_5^2\left(x_7^2+x_2-12341\right)^{16}\left(x_4x_5^2-12x_6x_8\right)^{11},
\end{aligned}
$$

and let

$$
\begin{aligned}
h_1 &= \left(x_4x_5^2-12x_6x_8\right)^{12}\\
h &= (x_1+x_3)\left(x_3^6-3x_1^2x_2^2x_3^2+x_1^2x_2^4+x_1^4x_2^2\right)\left(x_7^2+x_2-12341\right)^{16}h_1.
\end{aligned}
$$

Attempting to prove that $h=0$ is invariant under the flow of this system using DRI *we observe running time of under 2 seconds. Reducing h to be square-free results in* DRI *running for over 8 minutes before it is able to prove the result. In this case, square-free reduction introduces a performance penalty when checking for polynomial ideal membership (which is performed using Gröbner bases with reverse lexicographic monomial ordering). We see that one needs to be careful when using square-free reduction with* DRI *because even though it is reasonable to expect better performance due to lower degrees in square-free reduced polynomials, performing this step may make the Gröbner basis computation more difficult for some problems.*

Remark 46. *Notice that Prop. 42 does not have an analogue for* DRI*. In other words, if a polynomial equation $h=0$ is invariant for $\mathbf{p}$, its irreducible factors need not define invariant equations themselves. Geometrically, this means that if a variety is invariant under the flow of $\mathbf{p}$, its irreducible components need not be invariants under the flow of $\mathbf{p}$. For instance, consider the irreducible polynomials $q_1=y-1$ and $q_2=x^2+(y-1)^2$. The equation $q_1q_2=0$ which is equivalent to $y=1$, is invariant for $\mathbf{p}=(1,0)$, since the premise of the proof rule* DRI *holds true for $N=3$. However, the equation $q_2=0$, which is equivalent to $x=0\wedge y=1$, is not an invariant equation for $\mathbf{p}$. The reason for the invariance of $q_1q_2=0$, which is equivalent to $q_1=0\vee q_2=0$, stems from q_1 not from q_2.*

7.4. Order parity decomposition

Similar to square-free reduction for invariant polynomial equations, one may sometimes remove roots of multiplicities greater than 1 from polynomial inequalities $p \leq 0$, thereby simplifying their description and removing singularities on their boundary. To do this, we will require some definitions, due to Dolzmann and Sturm (see [7]).

Definition 47 (Square-free decomposition [7])**.** *Given a polynomial $h \in \mathbb{Z}[x_1, \ldots, x_n]$, the square-free decomposition is given by*

$$(h_1, \ldots, h_n) \textit{ s.t. } \prod_{i=1}^{n} h_i^i = h,$$

where all h_i are square-free and relatively prime, i.e. $\gcd(h_i, h_j) = 1$.

Note that while superficially similar to square-free reduction, the square-free decomposition is quite different. To see this, note that the exponent in the product matches the index. Thus, the order in a square-free decomposition encodes the exponent to which the factor h_i is raised in the original polynomial h, i.e. the factors raised to odd powers will have odd index in the decomposition; respectively for even exponents.

Definition 48 (Parity decomposition [7])**.** *Given a polynomial $h \in \mathbb{Z}[x_1, \ldots, x_n]$ with square-free decomposition $(h_1, \ldots, h_n)$, the parity decomposition is given by*

$$\left(\prod_{\textit{odd } i} h_i, \prod_{\textit{even } i} h_i \right).$$

Proposition 49 (Square-free equivalent [7])**.** *Let $h \in \mathbb{Z}[x_1, \ldots, x_n]$ and let (h_o, h_e) be the parity decomposition of h. Then the following equivalences hold:*

1. $h = 0 \equiv_{\mathbb{R}} \mathrm{SF}(h) = 0$,
2. $h \neq 0 \equiv_{\mathbb{R}} \mathrm{SF}(h) \neq 0$,
3. $h > 0 \equiv_{\mathbb{R}} h_o h_e^2 > 0 \equiv_{\mathbb{R}} h_o > 0 \wedge h_e \neq 0$,
4. $h \geq 0 \equiv_{\mathbb{R}} h_o h_e^2 \geq 0 \equiv_{\mathbb{R}} h_o \geq 0 \vee h_e = 0$,
5. $h < 0 \equiv_{\mathbb{R}} h_o h_e^2 < 0 \equiv_{\mathbb{R}} h_o < 0 \wedge h_e \neq 0$,
6. $h \leq 0 \equiv_{\mathbb{R}} h_o h_e^2 \leq 0 \equiv_{\mathbb{R}} h_o \leq 0 \vee h_e = 0$.

The resulting (rightmost) equivalent formulas are guaranteed to only feature square-free polynomials and are called square-free equivalents.

For a semi-algebraic set S given by a quantifier-free formula of real arithmetic, we define $\mathrm{SFEQ}[S]$ to be the *square-free equivalent* formula obtained by applying the equivalences in Proposition 49 to each atomic formula in S. Using the SFEQ reduction as a pre-processing step for the proof rule NSSBC is denoted $\mathrm{SFEQ}\,\mathrm{NSSBC}$ and accordingly for $\mathrm{SFEQ}\,\mathrm{DI}$ and $\mathrm{SFEQ}\,\mathrm{Nagumo}$.

Theorem 50. $\mathrm{SFEQ}\,\mathrm{NSSBC} \succ \mathrm{NSSBC}$.

Proof. If $\mathfrak{L}_{\boldsymbol{p}}(h) < 0$ is true when h is an active component ($h = 0$), it is necessarily the case that h is square-free. Thus $\mathrm{SFEQ}(h) = h$ (which then equals $\mathrm{SF}(h)$) and, therefore, $\mathrm{SFEQ}\,\mathrm{NSSBC} \not\succcurlyeq \mathrm{NSSBC}$. Let $\dot{\boldsymbol{x}} = \boldsymbol{p}(\boldsymbol{x}) = (-x_1, -x_2)$ and consider the set $S \equiv (x_1^2 + x_2^2 - 1)^3 \leq 0$. Applying NSSBC fails to prove the positive invariance property. Computing the order parity decomposition, we get $\mathrm{SFEQ}(S) \leq 0 \equiv (x_1^2 + x_2^2 - 1) \leq 0$, for which positive invariance under the flow of $\boldsymbol{p}(\boldsymbol{x})$ is proved easily using NSSBC. □

Example 51 (Positive invariant defined by polynomial inequality)**.** *Let us consider a system with an unstable limit cycle around a stable origin:*

$$\begin{aligned}\dot{x}_1 &= -x_1 - x_2 + x_1 x_2^2 + x_1^3,\\ \dot{x}_2 &= x_1 - x_2 + x_1^2 x_2 + x_2^3.\end{aligned}$$

Suppose we wanted to show that the set of states satisfying the following inequality is positively invariant:

$$(x_1^2 + x_2^2 - 1)^2 (x_1^2 + x_2^2 - \frac{1}{2})^3 \leq 0.$$

Let us refer to this set as $h \leq 0$. As can be seen from the phase portrait in Figure 11, the set $h \leq 0$ is indeed positively invariant under the flow; however, h is not square-free, but $h \leq 0$ has the following square-free equivalent:

$$\begin{aligned}\mathrm{SFEQ}[(x_1^2 + x_2^2 - 1)^2 (x_1^2 + x_2^2 - \frac{1}{2})^3 \leq 0] \equiv\\ \Big(x_1^2 + x_2^2 - \frac{1}{2} \leq 0 \ \vee \ x_1^2 + x_2^2 - 1 = 0\Big).\end{aligned}$$

This is an example of a positively invariant set described by a non-strict polynomial inequality where applying NSSBC *will fail. In fact, the barrier certificate approach [26] breaks down completely, i.e. no barrier certificate exists for showing positive invariance of this set.*

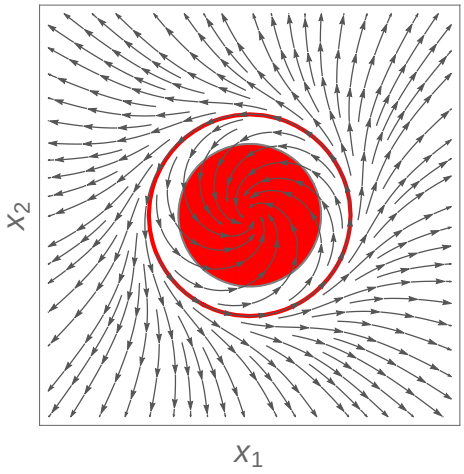


Figure 11: Positively invariant set given by $h \leq 0$ (in red).

It is perhaps remarkable is that the output of $\mathrm{SFEQ}(h) \leq 0$ *yields two sub-problems, both of which we can solve using only sufficient proof rules: one is a non-strict inequality* $x_1^2 + x_2^2 - \frac{1}{2} \leq 0$ *for which one can apply the method of strict barrier certificates to prove its positive invariance; the other is a polynomial equality defining a smooth invariant curve* $x_1^2 + x_2^2 - 1 = 0$*, which can also be handled (using e.g. the proof rule* Lie*).*

By performing the above steps one proves that both disjuncts are positively invariant under the flow, and hence their disjunction is also positively invariant, concluding the proof that $h \leq 0$ *describes a positively invariant set. A formal proof of this property within a proof calculus needs an inference rule such as* NSSBC*, some appropriate rule for equational invariants, such as e.g.* Lie*,* P-c *or* DRI*, as well as the following special case of the generalization rule [21]:*

$$(Inv_\vee)\ \frac{S_1 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}(\boldsymbol{x})]\, S_1 \qquad S_2 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}(\boldsymbol{x})]\, S_2}{S_1 \vee S_2 \to [\dot{\boldsymbol{x}} = \boldsymbol{p}(\boldsymbol{x})]\, (S_1 \vee S_2)}.$$

Theorem 52. $\mathrm{SFEQ}\,\mathrm{DI} \prec\succ \mathrm{DI}$

Proof. Corollary to Proposition 40, since FI is a special case of DI and $\mathrm{SFEQ}[h = 0] \equiv \mathrm{SF}(h) = 0$. □

Theorem 53. $\mathrm{SFEQ}\,\mathrm{Nagumo} \sim \mathrm{Nagumo}$.

Proof. Nagumo is necessary and sufficient for proving positive invariance of closed sets and SFEQ returns a description of an equivalent set (over the reals).

Thus, a closed set S is positively invariant using Nagumo if and only if an equivalent closed set $\mathrm{SFEQ}[S]$ is positively invariant using Nagumo. □

Theorem 54. $\mathrm{SFEQ}\,\mathrm{LZZ} \sim \mathrm{LZZ}$.

Proof. Elementary, since LZZ is necessary and sufficient for proving positive invariance and $\mathrm{SFEQ}[S]$ gives an equivalent set in $\mathbb{R}^n$. □

8. Experimental Comparison

To complement the theoretical deductive power comparison with a practical provability study, we empirically compare the running time performance of all the proof rules discussed in this paper on a heterogeneous collection of benchmarks (76 for algebraic sets and 20 for semi-algebraic sets).

Many premises of the considered proof rules are universally quantified sentences over the theory of real arithmetic. The purely existential fragment of real quantifier elimination has been shown to exhibit singly exponential time complexity in the number of variables [1]. However, in practice this has not yet led to an efficient decision procedure, so typically it is much more efficient to use CAD [3, 4], which has doubly-exponential running time in the number of variables. Theoretically, the upper bound on the complexity of deciding a sentence in the universal theory of $\mathbb{R}$ is given by $(sd)^{O(n)}$, where s is the number of polynomials in the formula, d their maximum degree and n the number of variables [1].

Notice, in addition, that the proof rules, C-c, P-c, DRI and LZZ involve reasoning about multivariate polynomial ideal membership, which is an EXPSPACE-complete problem over $\mathbb{Q}$ [18]. Gröbner basis algorithms allow us to perform membership checks in ideals generated by multivariate polynomials. Significant advances have been made in algorithms for computing Gröbner bases [9] which in practice can be expected to perform very well. Our experimentation relies on the implementation of the CAD algorithm in Mathematica (version 10.0.1).

The examples we used originate from a number of sources—many come from textbooks on Dynamical Systems; some from the literature on formal verification of hybrid systems; others have been hand-crafted to tease out sweetspots of certain proof rules. The most interesting experimental question we seek to address here is whether the greater generality of the more deductively powerful proof rules also comes at a substantially higher computational cost when assessed across the entire spectrum of examples. As a complement to the theoretical deductive power relationships between the different proof rules (Section 6), we also seek to identify some nuances in the complexity of the conditions in the premises, which the

coarse-grained complexity bounds miss, being highly sensitive to the number of variables.

The proof rule Nagumo is intractable since it requires computing the contingent cone to a given semi-algebraic set. All algebraic sets are of the form $h = 0$, for which LZZ and DRI will ultimately result in the same conditions; only DRI and its optimized implementation DRI_{opt} (see Section 7.3) will be considered in the benchmarks.[6] We have also established that NSSBC cannot discharge any invariant algebraic set and that DI applied to candidates of the form $h = 0$ is equivalent to FI. Thus, two comparisons are of interest: the set of proof rules for algebraic sets (Section 8.1) and the set of poof rules for semi-algebraic sets (Section 8.2).

From our experiments it emerges that the proof rules exhibit different (and at times surprising) trade-offs between generality and efficiency.

8.1. Running Time Performance for Algebraic Sets

In this section, the prefix SF is implicit for all Lie-based proof rules. We consider 4 equally sized classes of invariant sets: (1) 24 smooth invariants, where Lie is both necessary and sufficient, (2) 17 isolated equilibria as trivial (for humans, not machines) equational invariants for which both Lie° and Lie^{*} provide necessary and sufficient conditions, (3) 17 other singularities and high integrals, (4) 18 functional invariants, where FI is necessary and sufficient. Figure 12 compares the number of invariant varieties that each rule could prove within 60 seconds. The vertical axis shows cumulative time spent on the problems. All runs were performed on an Intel Core i5 1.7GHz machine with 4Gb RAM. Generally, we observe DRI performing very well across the entire spectrum of problem classes. This is very encouraging, but also at first sight appears to defy intuition since it implies that one does not necessarily sacrifice performance when opting to use a more deductively powerful rule. In this graph, we also see that overall Lie° appears to offer an interesting compromise between deductive power and efficiency—it is able to prove a significant body of problems that are out of scope for Lie, while avoiding the complexity penalty which affects Lie^{*} (due to introducing an extra variable).

A more careful analysis of the benchmarks reveals interesting relationships that are obscured in the "big picture"; to see them, one needs to consider the

[6] We refer the reader to [11] for a more detailed discussion of the differences and similarities between the Liu, Zhan & Zhao characterization [16] and the differential radical characterization [10].

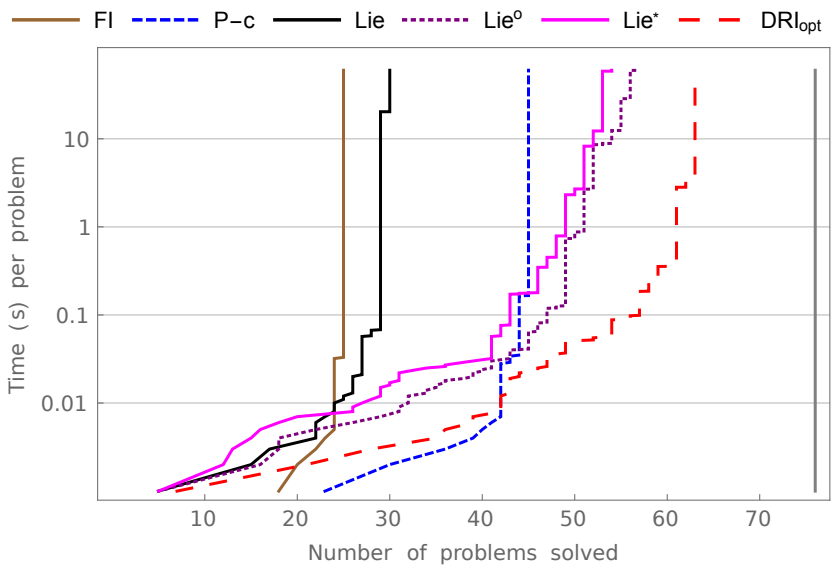


Figure 12: Experimental performance of proof rules: problems solved per time (log scale)

individual classes of invariants for which some of the sufficient conditions in the rules are in fact *necessary and sufficient*. Together with DRI, this yields two *decision procedures* for each class and allows us to focus only on running time performance and assess the practicality of each proof rule. In Fig. 13, we observe the rules Lie$^\circ$ and Lie* performing very well in proving invariance of isolated equilibria. This is to be expected as Lie$^\circ$ in particular was formulated with this problem class in mind. It is interesting that DRI remains highly competitive here; though its performance is slightly worse in our set of benchmarks.

It is clear that because proof rules Lie$^\circ$ and Lie* generalize Lie, they will be able to prove every problem in the smooth invariant benchmarks. The running time performance of the three rules is almost identical, with Lie offering a slight speed-up over its generalizations. The premises of Lie$^\circ$ and Lie* impose conditions on states in the singular locus, which is the empty set for smooth invariants; this, in practice, appears to be slightly more expensive than checking an equivalent property that the gradient is non-vanishing on the variety (as in the premise of Lie).

The proof rules FI and P-c, corresponding to conditions with historical origins in the study of integrability of dynamical systems, can be seen to perform very well in proving functional invariants, while performing very poorly in bench-

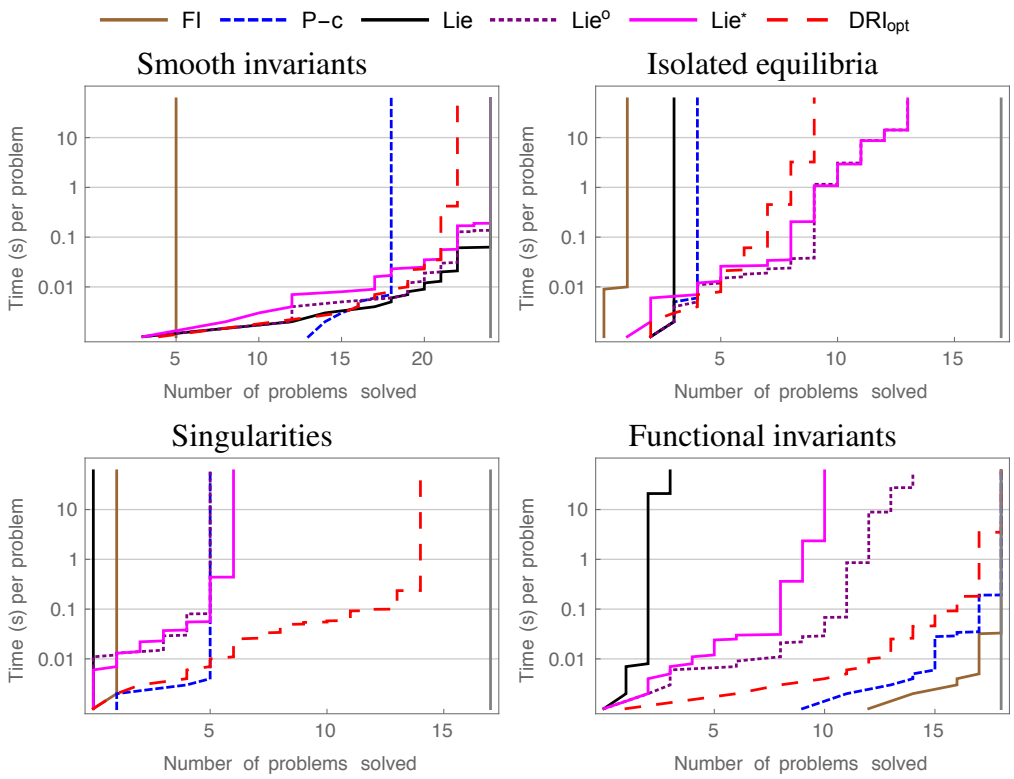


Figure 13: Number of problems solved per class (log scale).

marks for isolated equilibria. In proofs of smooth invariants their behaviour is radically different, with FI proving only a handful of examples and P-c succeeding in proving most of the problems very efficiently. This can be explained by the fact that P-c generalizes FI and is therefore more deductively powerful. P-c appears slightly slower at proving functional invariants, but shows very impressive running time performance for some problems from the smooth invariant benchmarks, where it is the fastest proof rule for many of problems where it succeeds. Comparing running time performance with DRI, we see that DRI is only slightly slower at proving functional invariants than FI and P-c. Again, the performance gap between DRI and the two rules appears to be insignificant for most problems. Theoretically, when P-c proves an invariant, DRI applies conditions that are identical to the premise of P-c. Hence, although DRI is a generalization, this does not come at a significant extra cost for the classes where P-c shows good running

time performance. The slightly greater running time of DRI compared to that of P-c can be accounted for by the fact that in our implementation DRI computes the Gröbner basis for *every* order N including for $N = 1$ where such computation is unnecessary.

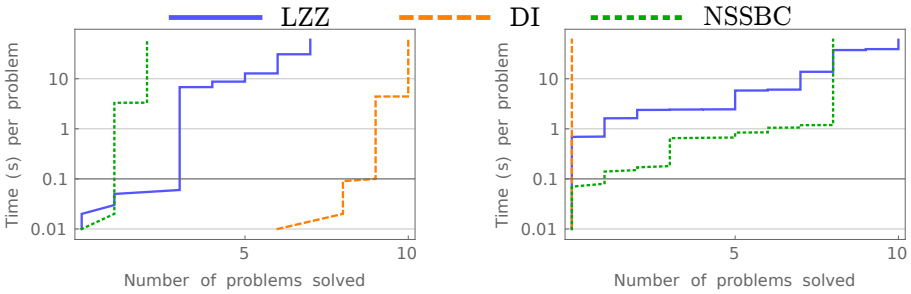
For functional invariants, FI (i.e. the equality fragment of DI) benefits from the fact that the condition in its premise, which requires to show that the Lie derivative evaluates to zero everywhere, is equivalent to showing that the Lie derivative is the zero polynomial, which can be checked very efficiently by symbolic computation, without a decision procedure for real arithmetic.

In the examples featuring singularities and high integrals in the benchmarks we see DRI as the clear winner, simply because there was no other rule that was tailored to work on this class. Indeed, the structure of these invariant sets can be rather involved, making it difficult to characterize in a single proof rule; however, sometimes it is possible to exploit the structure of high integrals inside a proof system and arrive at efficient proofs that outperform DRI [11].

It is not surprising that DRI should ultimately overtake all the other rules in terms of deductive power (it is, after all, necessary and sufficient); what is remarkable is that the performance we observe for DRI is often very competitive to that of the sufficient rules when they also succeed at a proof. This observation suggests a possible strategy for proof search in a proof system: give precedence to DRI and switch to other sufficient rules if DRI takes longer than some time-out value. The rationale behind this decision is our empirical observation that DRI performs consistently well on all problem classes we considered, but it is also sometimes possible to save time by using a proof rule which is less deductively powerful. It is important to note here that the overall proof system benefits from including the sufficient proof rules, rather than relying solely upon DRI.

8.2. Running Time Performance for Semi-algebraic Sets

In Fig. 14 we compare the running time performance of the proof rule LZZ versus the sufficient conditions DI (Fig. 14a) and NSSBC (Fig. 14b). Two different sets of 10 benchmarks each were selected to exploit the sweetspots of DI and NSSBC respectively. We observe that whenever DI can prove invariance in the problem at hand, it is much faster than LZZ. This is expected: the quantifier elimination problems required by the proof rule LZZ are much more involved than those found in the premise of DI. This should be balanced by the fact that DI is more restrictive. In the set of benchmarks for NSSBC, one can observe that DI does not prove any of the problems. In Fig. 14b, one can also notice that LZZ still performs well compared to NSSBC. Indeed, the premise of the proof rule NSSBC



(a) LZZ vs DI (b) LZZ vs NSSBC

Figure 14: Number of problems solved in each class (times on log scale).

can involve complicated real arithmetic problems that are sometimes even more difficult than those appearing in the premise of the proof rule LZZ. Generally, the size of the conditions in the premise of NSSBC grows rapidly with the size of the formula describing the invariant candidate. The distribution property in Theorem 19 avoids this problem in LZZ.

9. Conclusion

This article investigated an important aspect of deductive safety verification of continuous and hybrid dynamical systems. Namely, given the abundance of existing sufficient conditions for invariant checking and the recently developed *necessary and sufficient* conditions for real algebraic [10] and semi-algebraic [16] invariants, it is crucial to know whether the gains in deductive power come at the price of greater computational complexity and poor running time performance that would hinder practical applications. The work presented in this article leads us to arrive at the following conclusions:

- Empirically, we observe that the deductively powerful rule for algebraic invariants (DRI) performs very well in checking invariance of polynomial equalities.
- P-c is made redundant by DRI (DRI strictly increases the deductive power of P-c while being equally efficient).
- Reducing polynomials to square-free form is always beneficial to the proof rule Lie and its generalizations, where it yields improvements in both the deductive power and the running time performance.

- Using the square-free reduction with the proof rules FI and C-c yields new *incomparable* proof rules, whereas SF with P-c is as powerful as P-c alone.

- Performing square-free reduction of an invariant candidate may introduce a performance penalty for DRI and therefore cannot be regarded as an optimization, even though there are instances for which it yields a speed-up. The same can be said of order parity decomposition applied to an invariant candidate supplied to LZZ.

- Sufficient rules DI and NSSBC can afford a speed-up on certain problems, but the overall running time performance of the decision procedure LZZ is observed to be good.

- Using a decision procedure LZZ appears to be more efficient than using the sufficient condition NSSBC when the positively invariant candidate set is described by a large formula.

Our next step is to use these highlighted insights to build efficient proof strategies that intelligently combine different proof methods to efficiently construct formal proofs, e.g., by favoring the most deductively complete rules that come without significant practical performance penalties on the most common cases of invariants.

Acknowledgments. The authors would like to thank Dr. Ashish Tiwari at SRI International for his kind and informative response to our technical query and extend special thanks to Dr. Paul B. Jackson at the LFCS, University of Edinburgh, for his valuable help in improving the manuscript.

[1] Basu, S., Pollack, R., Roy, M.-F., 1996. On the combinatorial and algebraic complexity of quantifier elimination. J. ACM 43 (6), 1002–1045.

[2] Blanchini, F., Miani, S., 2008. Set-Theoretic Methods in Control. Systems & Control : Foundations & Applications. Birkhäuser.

[3] Collins, G. E., 1975. Hauptvortrag: Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In: Automata Theory and Formal Languages. Vol. 33 of LNCS. Springer, pp. 134–183.

[4] Collins, G. E., Hong, H., Sep. 1991. Partial cylindrical algebraic decomposition for quantifier elimination. J. Symb. Comput. 12 (3), 299–328.

[5] Cox, D. A., Little, J., O'Shea, D., 1997. Ideals, Varieties, and Algorithms - an introduction to computational algebraic geometry and commutative algebra (2. ed.). Springer.

[6] Darboux, J.-G., 1878. Mémoire sur les équations différentielles algébriques du premier ordre et du premier degré. Bulletin des Sciences Mathématiques et Astronomiques 2 (1), 151–200.
URL http://eudml.org/doc/84988

[7] Dolzmann, A., Sturm, T., 1995. Simplification of quantifier-free formulas over ordered fields. Journal of Symbolic Computation 24, 209–231.

[8] Dumortier, F., Llibre, J., Artés, J. C., 2006. Qualitative Theory of Planar Differential Systems. Springer.

[9] Faugère, J. C., 2002. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: ISSAC. ACM, New York, NY, USA, pp. 75–83.

[10] Ghorbal, K., Platzer, A., 2014. Characterizing algebraic invariants by differential radical invariants. In: TACAS. Vol. 8413. Springer, pp. 279–294.

[11] Ghorbal, K., Sogokon, A., Platzer, A., 2014. Invariance of conjunctions of polynomial equalities for algebraic differential equations. In: SAS. Vol. 8723 of LNCS. Springer, pp. 151–167.

[12] Ghorbal, K., Sogokon, A., Platzer, A., 2015. A hierarchy of proof rules for checking differential invariance of algebraic sets. In: VMCAI. Vol. 8931 of LNCS. Springer, pp. 431–448.

[13] Goriely, A., 2001. Integrability and Nonintegrability of Dynamical Systems. Advanced series in nonlinear dynamics. World Scientific.

[14] Lie, S., 1893. Vorlesungen über continuierliche Gruppen mit Geometrischen und anderen Anwendungen. Teubner, Leipzig.

[15] Lindelöf, E., 1894. Sur l'application de la méthode des approximations successives aux équations différentielles ordinaires du premier ordre. Comptes rendus hebdomadaires des séances de l'Académie des sciences 116, 454–458.

[16] Liu, J., Zhan, N., Zhao, H., 2011. Computing semi-algebraic invariants for polynomial dynamical systems. In: EMSOFT. ACM, pp. 97–106.

[17] Matringe, N., Moura, A. V., Rebiha, R., 2010. Generating invariants for non-linear hybrid systems by linear algebraic methods. In: SAS. Vol. 6337 of LNCS. Springer, pp. 373–389.

[18] Mayr, E. W., 1989. Membership in polynomial ideals over Q is exponential space complete. In: Monien, B., Cori, R. (Eds.), STACS. Vol. 349 of LNCS. Springer, pp. 400–406.

[19] Nagumo, M., May 1942. Über die Lage der Integralkurven gewöhnlicher Differentialgleichungen (in German). In: Proceedings of the Physico-Mathematical Society of Japan. Vol. 24. pp. 551–559.

[20] Olver, P. J., 2000. Applications of Lie Groups to Differential Equations. Springer.

[21] Platzer, A., 2008. Differential dynamic logic for hybrid systems. J. Autom. Reasoning 41 (2), 143–189.

[22] Platzer, A., 2010. Differential-algebraic dynamic logic for differential-algebraic programs. J. Log. Comput. 20 (1), 309–352.

[23] Platzer, A., 2012. A differential operator approach to equational differential invariants - (invited paper). In: ITP. Vol. 7406 of LNCS. Springer, pp. 28–48.

[24] Platzer, A., 2012. The structure of differential invariants and differential cut elimination. Logical Methods in Computer Science 8 (4), 1–38.

[25] Prajna, S., Jadbabaie, A., 2004. Safety verification of hybrid systems using barrier certificates. In: In Hybrid Systems: Computation and Control. Springer, pp. 477–492.

[26] Prajna, S., Jadbabaie, A., Pappas, G., 2007. A framework for worst-case and stochastic safety verification using barrier certificates. Automatic Control, IEEE Transactions on 52 (8), 1415–1428.

[27] Richardson, D., 12 1968. Some undecidable problems involving elementary functions of a real variable. Journal of Symbolic Logic 33 (4), 514–520.

[28] Sankaranarayanan, S., Sipma, H. B., Manna, Z., 2008. Constructing invariants for hybrid systems. Form. Methods Syst. Des. 32 (1), 25–55.

[29] Taly, A., Tiwari, A., 2009. Deductive verification of continuous dynamical systems. In: FSTTCS. Vol. 4 of LIPIcs. pp. 383–394.

[30] Tarski, A., 1951. A decision method for elementary algebra and geometry. Bull. Amer. Math. Soc. 59.

[31] Tiwari, A., 2008. Abstractions for hybrid systems. Form. Methods Syst. Des. 32 (1), 57–83.

[32] Walter, W., 1998. Ordinary Differential Equations. Springer New York.

[33] Wu, Z., 2010. Tangent cone and contingent cone to the intersection of two closed sets. Nonlinear Analysis: Theory, Methods & Applications 73 (5), 1203 – 1220.