

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>
1477-8424/& 2015 Elsevier Ltd. All rights reserved.

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 $\mathbf{x}_0 \in X_0$ cannot enter the unsafe region, that is $\mathbf{x}(\mathbf{x}_0, t) \notin X_u$ for all $t \geq 0$, where $\mathbf{x}(\mathbf{x}_0, t)$ is the state of the system at time t w.r.t. the initial value \mathbf{x}_0 . The safety verification problem is in this case equivalent to showing that the intersection of the reachable set $\{\mathbf{x}(\mathbf{x}_0, t) \in X \mid t \geq 0\}$ with the set of unsafe states is empty. However, solutions to ordinary differential equations will rarely be available in closed form¹; 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 \mathbf{x}_0 of the system are the *smallest* positively invariant sets one can hope to find that include \mathbf{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

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

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

46 2. Preliminaries

47 We consider autonomous² polynomial vector fields (see Def. 1 below).

48 Let $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$, and $\mathbf{x}(t) = (x_1(t), \dots, x_n(t))$, where $x_i : \mathbb{R} \rightarrow \mathbb{R}$, $t \mapsto x_i(t)$. The ring of polynomials over the reals will be denoted
 49 by $\mathbb{R}[x_1, \dots, x_n]$.
 50

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

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

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

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

²That 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.

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

$$S \rightarrow [\dot{\mathbf{x}} = \mathbf{p}] S. \quad (2)$$

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

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

$$\liminf_{\lambda \rightarrow 0^+} \frac{\text{dist}(S, \mathbf{x} + \lambda \mathbf{v})}{\lambda} = 0,$$

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

73 **Theorem 3** (Nagumo’s Theorem). *Given a continuous system $\dot{\mathbf{x}} = \mathbf{p}(\mathbf{x})$ and
 74 assuming that solutions exist and are unique inside some open set $O \subseteq \mathbb{R}^n$, let
 75 $S \subset O$ be a closed set. Then, S is positively invariant under the flow of the system
 76 if and only if $\mathbf{p}(\mathbf{x})$ is sub-tangential to S (or equivalently, $\mathbf{p}(\mathbf{x}) \in K_{\mathbf{x}}(S)$, where
 77 $K_{\mathbf{x}}(S)$ is the set of all sub-tangential vectors to S at \mathbf{x} , known as the contingent
 78 cone) for all $\mathbf{x} \in \text{bdr}(S)$, where $\text{bdr}(S)$ is the boundary of S .³*

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

$$(\text{Nagumo}) \frac{\forall \mathbf{x} \in \text{bdr}(S). \mathbf{p}(\mathbf{x}) \in K_{\mathbf{x}}(S)}{S \rightarrow [\dot{\mathbf{x}} = \mathbf{p}] S}.$$

81 More recently, a different characterization of positively invariant sets (de-
 82 scribed in detail in subsequent sections) was reported in [16].

83 In the important special case where a closed set S is described by the equation
 84 $h = 0$, with $h \in \mathbb{R}[x_1 \dots, x_n]$, positive invariance of $h = 0$ is semantically
 85 equivalent to the validity of the formula:

$$(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0). \quad (3)$$

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

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

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

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

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

101 3. Proof Rules for Algebraic Sets

102 We recall five important proof rules for checking invariance of polynomial
103 equalities, or equivalently the validity of Equation 3. In Figure 1, FI refers to in-
104 variant polynomial functions.⁴ The premise of the Polynomial-scale consecution
105 proof rule [28], P-c in Figure 1, requires $\mathfrak{L}_{\mathbf{p}}(h)$ to be in the ideal generated by h .
106 The condition given in the premise is only sufficient (but is eminently suitable for
107 *generating* invariant varieties [17]). We also consider the constant-scale consecu-
108 tion proof rule [28, 31], denoted by C-c. The premise of proof rule C-c requires
109 that $\mathfrak{L}_{\mathbf{p}}(h) = \lambda h$, where λ is a scalar, not a polynomial as in P-c. It is therefore a
110 simple special case of P-c. When $\lambda = 0$, one obtains the premise of the proof rule
111 FI. It is worth noting that the condition in the premise of P-c, including its special
112 case C-c, was mentioned as early as 1878 [6] and used extensively in the study of
113 integrability of dynamical systems (e.g. see *second integrals* in [13, Chapter 2]).
114 It serves as a natural extension to invariant functions, also known as *first integrals*,
115 which are covered by the proof rule FI. The proof rule Lie gives Lie's criterion
116 [14, 20] for invariance of $h = 0$; this proof rule will be discussed in more depth

⁴We used the notation DI₌ for the same proof rule in [12].

$$\begin{array}{l}
\text{(FI)} \frac{\mathcal{L}_{\mathbf{p}}(h) = 0}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)} \quad \text{(C-c)} \frac{\exists \lambda \in \mathbb{R}, \mathcal{L}_{\mathbf{p}}(h) = \lambda h}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)} \\
\text{(Lie)} \frac{h = 0 \rightarrow (\mathcal{L}_{\mathbf{p}}(h) = 0 \wedge \nabla h \neq \mathbf{0})}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)} \quad \text{(P-c)} \frac{\mathcal{L}_{\mathbf{p}}(h) \in \langle h \rangle}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)} \\
\text{(DRI)} \frac{h = 0 \rightarrow \bigwedge_{i=0}^{N-1} \mathcal{L}_{\mathbf{p}}^{(i)}(h) = 0}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)}
\end{array}$$

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

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

123 4. Extending Lie's Criterion

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

129 $h(\mathbf{x}) > 0$ for all $\mathbf{x} \in \mathbb{R}^n \setminus \{\mathbf{a}\}$. Functions whose real roots characterize
130 isolated points have vanishing gradient at these roots, in this case \mathbf{a} , and thus the
131 formula $h = 0 \rightarrow \nabla h = \mathbf{0}$ holds. This violates the regularity condition in the
132 premise of the proof rule Lie, namely:

$$h = 0 \longrightarrow \nabla h \neq \mathbf{0} . \quad (5)$$

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

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

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

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

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

146 4.1. Handling Singularities

147 Equilibria are points in the state space where the vector field vanishes ($\mathbf{p} =$
 148 $\mathbf{0}$) so that there is no motion. However, as seen above, Lie’s criterion cannot
 149 generally be applied to prove invariance properties of isolated equilibria because
 150 their description involves singularities. One simple way to resolve this issue is
 151 to drop the non-vanishing gradient condition and replace it with the proviso that
 152 there be no flow (that is $\mathbf{p} = \mathbf{0}$) in the variables of the invariant candidate on
 153 the singular locus; this will allow singularities in the invariant candidate and will
 154 provide a *sound* proof method in which there is no need to check for non-vanishing
 155 gradient. Below we present two extensions to the proof rule Lie and justify their
 156 soundness after recalling some basic geometric notions.

Definition 5 (Lie^o: Lie + Equilibria).

$$(\text{Lie}^{\circ}) \frac{h = 0 \rightarrow (\mathcal{L}_{\mathbf{p}}(h) = 0 \wedge (SL(h) \rightarrow \bigwedge_{x_i \in \text{vars}(h)} p_i = 0))}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)},$$

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

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

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

$$(\text{Lie}^*) \frac{h = 0 \rightarrow (\mathcal{L}_{\mathbf{p}}(h) = 0 \wedge (\text{SL}(h) \rightarrow h(\mathbf{x} + \lambda \mathbf{p}) = 0))}{(h = 0) \rightarrow [\dot{\mathbf{x}} = \mathbf{p}](h = 0)} .$$

161 To prove soundness of Lie° and Lie^* , we appeal to the Nagumo theorem. Let
 162 us observe that given $\mathbf{x} \in \text{bdr}(S)$, if $\mathbf{x} + \lambda \mathbf{p}(\mathbf{x}) \in S$ for all $\lambda \in \mathbb{R}$, then
 163 $\text{dist}(S, \mathbf{x} + \lambda \mathbf{p}(\mathbf{x})) = 0$ and so $\mathbf{p}(\mathbf{x})$ is sub-tangential to S at \mathbf{x} . This obser-
 164 vation is important for algebraic sets, for which $\text{bdr}(S) = S$, and the condition
 165 $\mathbf{x} + \lambda \mathbf{p}(\mathbf{x}) \in S$ translates to $h(\mathbf{x} + \lambda \mathbf{p}(\mathbf{x})) = 0$. This is the main idea behind the
 166 soundness of the proof rule Lie^* .

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

168 *Proof.* A point on the variety is either regular or singular. For regular points
 169 (these form an *open subset* of the variety), since $\mathcal{L}_{\mathbf{p}}(h)(\mathbf{x}) = 0$, the vector $\mathbf{p}(\mathbf{x})$
 170 is sub-tangent to the variety at \mathbf{x} (in fact, it is even *tangent*, so the condition
 171 we check is exactly that which is used in Lie). At singular points $\mathbf{x} \in V_{\mathbb{R}}(h)$
 172 if $h(\mathbf{x} + \lambda \mathbf{p}(\mathbf{x})) = 0$ holds for all λ then $\text{dist}(V_{\mathbb{R}}(h), \mathbf{x} + \lambda \mathbf{p}(\mathbf{x})) = 0$ for all
 173 λ , from which it follows that $\liminf_{\lambda \rightarrow 0^+} \frac{\text{dist}(V_{\mathbb{R}}(h), \mathbf{x} + \lambda \mathbf{p}(\mathbf{x}))}{\lambda} = 0$ and thus $\mathbf{p}(\mathbf{x})$ is
 174 sub-tangential to $V_{\mathbb{R}}(h)$ at \mathbf{x} . Assuming solutions exist and are unique, the variety
 175 $V_{\mathbb{R}}(h)$ is positively invariant under the vector field \mathbf{p} by Nagumo's theorem. \square

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

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

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

183 5. Proof rules for semi-algebraic sets

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

187 *5.1. Differential Invariants*

188 Differential induction with differential invariants (henceforth DI) was intro-
 189 duced in [22, Theorem 1].

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

$$(DI) \frac{D(S)_{\dot{\mathbf{x}}}^{\mathbf{p}}}{S \rightarrow [\dot{\mathbf{x}} = \mathbf{p}] S} .$$

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

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

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

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

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

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

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

213 5.2. Non-Smooth Strict Barrier Certificate

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

221 Given a closed semi-algebraic set $S \equiv \bigvee_{i=1}^k \bigwedge_{j=1}^{m(i)} h_{ij} \leq 0$ with polynomials
 222 $h_{ij} \in \mathbb{R}[x_1, \dots, x_n]$, we can equivalently rewrite S by a sub-level set of a contin-
 223 uous function, namely

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

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

$$\begin{aligned} & (h_1 > \max(h_2, \dots, h_m) \rightarrow \mathcal{L}_{\mathbf{p}}(h_1) < 0) \\ \wedge & (h_1 < \max(h_2, \dots, h_m) \rightarrow \mathcal{L}_{\mathbf{p}}(\max(h_2, \dots, h_m)) < 0) \\ \wedge & (h_1 = \max(h_2, \dots, h_m) \rightarrow \mathcal{L}_{\mathbf{p}}(h_1) < 0 \wedge \mathcal{L}_{\mathbf{p}}(\max(h_2, \dots, h_m)) < 0) \end{aligned} \quad (7)$$

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

$$\begin{aligned} \mathcal{L}_{\mathbf{p}}(\max(h_1, h_2)) < 0 \stackrel{\text{def}}{=} & \wedge (h_1 > h_2 \rightarrow \mathcal{L}_{\mathbf{p}}(h_1) < 0) \\ & \wedge (h_1 < h_2 \rightarrow \mathcal{L}_{\mathbf{p}}(h_2) < 0) \\ & \wedge (h_1 = h_2 \rightarrow \mathcal{L}_{\mathbf{p}}(h_1) < 0 \wedge \mathcal{L}_{\mathbf{p}}(h_2) < 0) \end{aligned}$$

228 We similarly define the set $\mathcal{L}_{\mathbf{p}}(\min(g_1, \dots, g_m)) < 0$ by $\mathcal{L}_{\mathbf{p}}(g_1) < 0$ if $m = 1$,
 229 and for $m \geq 2$,

$$\begin{aligned} & (g_1 < \min(g_2, \dots, g_m) \rightarrow \mathcal{L}_{\mathbf{p}}(g_1) < 0) \\ \wedge & (g_1 > \min(g_2, \dots, g_m) \rightarrow \mathcal{L}_{\mathbf{p}}(\min(g_2, \dots, g_m)) < 0) \\ \wedge & (g_1 = \min(g_2, \dots, g_m) \rightarrow \mathcal{L}_{\mathbf{p}}(g_1) < 0 \vee \mathcal{L}_{\mathbf{p}}(\min(g_2, \dots, g_m)) < 0) \end{aligned} \quad . \quad (8)$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

250 5.3. Nagumo-like Conditions for Closed Semi-algebraic Sets

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

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

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

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

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

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

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

259 from which it follows that if \mathbf{v} is sub-tangential to S_1 at \mathbf{x}_0 , then it is also
 260 sub-tangential to $S_1 \cup S_2$. Thus, $K_{\mathbf{x}}(S_1) \subseteq K_{\mathbf{x}}(S_1 \cup S_2)$ for all $\mathbf{x} \in S_1$; by the
 261 same argument one shows $K_{\mathbf{x}}(S_2) \subseteq K_{\mathbf{x}}(S_1 \cup S_2)$ for all $\mathbf{x} \in S_2$, from which
 262 one concludes that the inclusion $K_{\mathbf{x}}(S_1) \cup K_{\mathbf{x}}(S_2) \subseteq K_{\mathbf{x}}(S_1 \cup S_2)$ holds for all
 263 $\mathbf{x} \in S_1 \cup S_2$. \square

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

$$K_{\mathbf{x}}(S_1) \cap K_{\mathbf{x}}(S_2) \not\subseteq K_{\mathbf{x}}(S_1 \cap S_2).$$

264 *Proof.* Consider $S_1 \equiv \{\mathbf{x} \mid x_2 + x_1^2 = 0\}$ and $S_2 \equiv \{\mathbf{x} \mid x_2 - x_1^2 = 0\}$. The two
 265 sets intersect at $\mathbf{0} \in \mathbb{R}^2$. At the origin, the intersection of the contingent cones
 266 is given by the real line, i.e. $K_{\mathbf{0}}(S_1) \cap K_{\mathbf{0}}(S_2) = \{\mathbf{x} \mid x_2 = 0\}$, whereas the
 267 contingent cone to the intersection of the two sets is given by the zero vector,
 268 $K_{\mathbf{0}}(S_1 \cap S_2) = \{\mathbf{0}\}$. See Figure 2 for an illustration and [33] for an overview this
 269 problem. \square

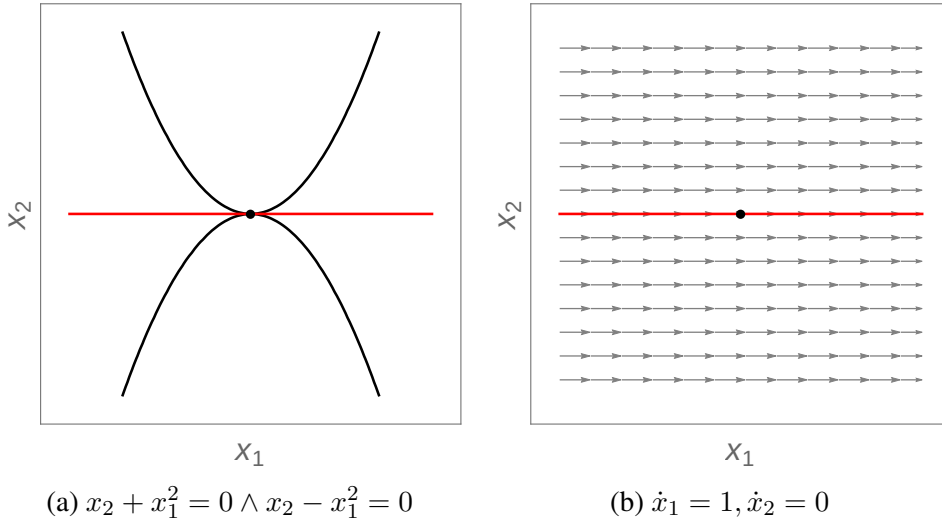


Figure 2: Closure properties of the contingent cone at an intersection of two closed sets. The intersection of the contingent cones to the two sets is shown in red. The contingent cone to the intersection itself is $\{\mathbf{0}\}$.

270 In general, given a closed set S which is presented as a finite union of inter-
 271 sections of closed sets S_{ij} , i.e.

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

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

$$\bigcup_{i=1}^k \bigcap_{j=1}^{m(i)} K_{\mathbf{x}}(S_{ij}) \subseteq K_{\mathbf{x}}\left(\bigcup_{i=1}^k \bigcap_{j=1}^{m(i)} S_{ij}\right). \quad (10)$$

for all \mathbf{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

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

272 It is possible to formulate inference rules based on Nagumo's theorem which
 273 allow one to prove positive invariance of a large class of closed semi-algebraic
 274 sets. This has previously been investigated in [29], where a number of inference
 275 rules are presented for checking positive invariance of closed sets of the form
 276 $h \geq 0$. For instance, it is shown that the following is a sound inference (similar to
 277 Lie):

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

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

294 *5.4. Liu, Zhan & Zhao Decision Procedure*

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

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

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

309 *If $\mathbf{x}(0) = \mathbf{x}_0$, then in case 1 one has $h(\mathbf{x}(t)) < 0$ for all $t \in (0, \epsilon)$ for some $\epsilon > 0$;*
 310 *case 2 is analogous, but with $h(\mathbf{x}(t)) > 0$ for all $t \in (0, \epsilon)$. In case 3, one is*
 311 *guaranteed that $h(\mathbf{x}(t)) = 0$ 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 $h(\varphi_t(\mathbf{x}_0))$ around $t = 0$ is given by

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

312 and *converges* on some non-empty open interval of t containing zero. Thus, the
 313 most significant term to become sign-definite will determine the sign of the entire
 314 sum on some sufficiently small interval. See [16, Proof of Proposition 9]. See
 315 also [29, Proof of Theorem 7], which employed very much the same ideas as [16].
 316 □

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

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

$$\begin{aligned} \text{In}_{\mathbf{p}}(S) &\equiv \{\mathbf{x} \in \mathbb{R}^n \mid \exists \epsilon > 0. \forall t \in (0, \epsilon). \mathbf{x}(t) \in S\}, \\ \text{In}_{(-\mathbf{p})}(S) &\equiv \{\mathbf{x} \in \mathbb{R}^n \mid \exists \epsilon > 0. \forall t \in (0, \epsilon). \mathbf{x}(-t) \in S\}, \end{aligned}$$

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

$$\text{(LZZ)} \frac{(\text{In}_{(-\mathbf{p})}(S) \rightarrow S) \wedge (S \rightarrow \text{In}_{\mathbf{p}}(S))}{S \rightarrow [\dot{\mathbf{x}} = \mathbf{p}] S}.$$

322

To develop some intuition for the construction of $\text{In}_{\mathbf{p}}(S)$, 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 $\text{In}_{\mathbf{p}}(h \leq 0)$ as the set of states in \mathbb{R}^n that satisfy the following *infinite* set of conditions (cf. [29, Theorem 7, Theorem 8]):

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

The *decidability* of checking the conditions in Proposition 17 (i.e. the premise of LZZ) hinges on the ability to construct *semi-algebraic sets* $\text{In}_{\mathbf{p}}(S)$ whenever S is semi-algebraic. In [16] the authors make the crucial observation that whenever h is a polynomial and $\dot{\mathbf{x}} = \mathbf{p}(\mathbf{x})$ is a system of polynomial ODEs, then the Lie derivatives $\mathfrak{L}_{\mathbf{p}}^{(i)}(h)$ 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 $\text{In}_{\mathbf{p}}(h \leq 0)$ can be characterized by a *finite* disjunction [16]:

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

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:

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

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

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

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

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

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

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

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

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

337 Thus, by computing N for a given polynomial h and a system $\dot{\mathbf{x}} = \mathbf{p}(\mathbf{x})$,
 338 one may construct a *semi-algebraic* set $\text{In}_{\mathbf{p}}(h \leq 0)$. In Fig. 3d we detail the
 339 computation for $N = 3$ and depict the different “pieces” involved to form $\text{In}_{\mathbf{p}}(h \leq$
 340 $0)$, which is, in this particular case, the same as $h \leq 0$ as shown in Fig. 4b.

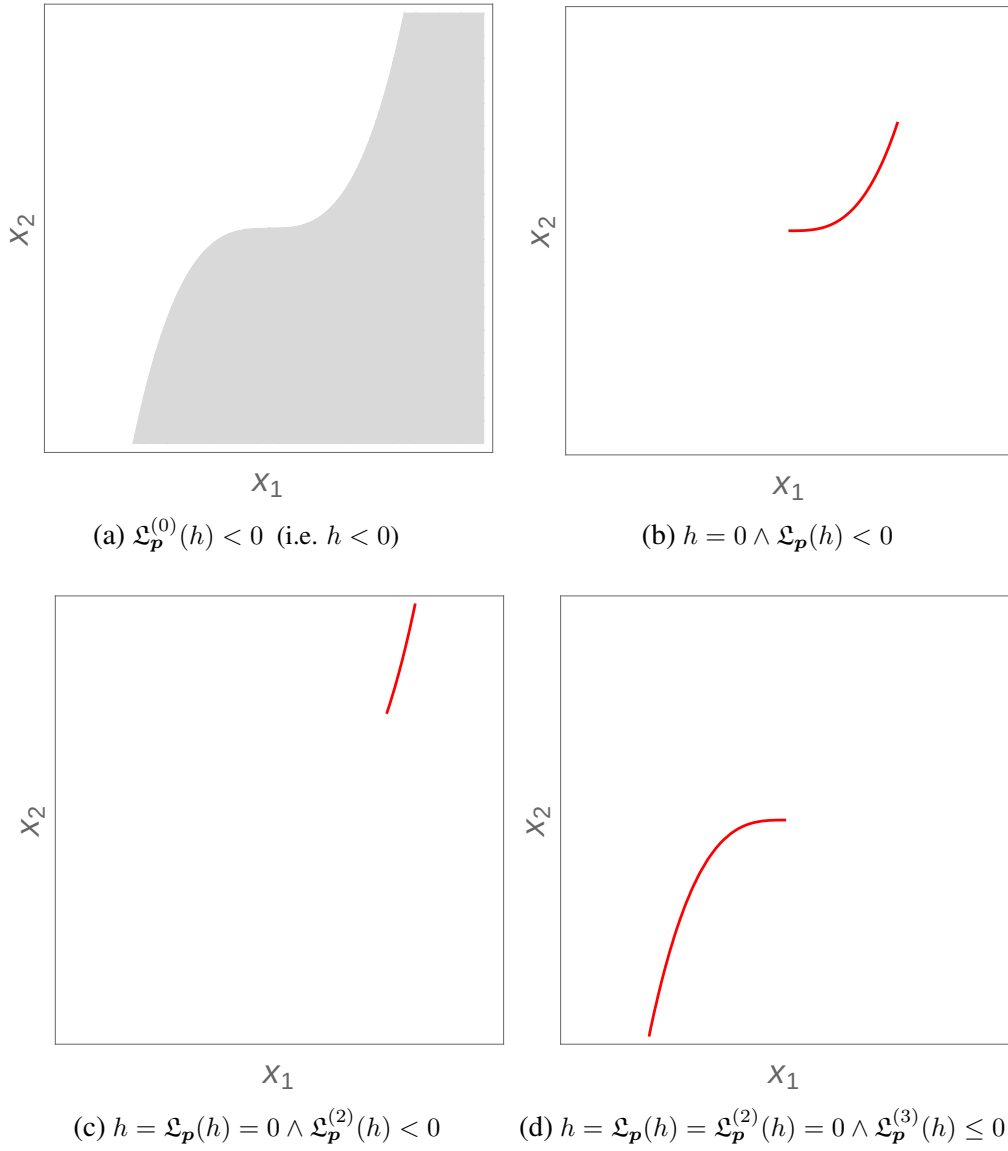


Figure 3: Sign conditions on Lie derivatives in the construction of $\text{In}_p(h \leq 0)$ with $N = 3$.

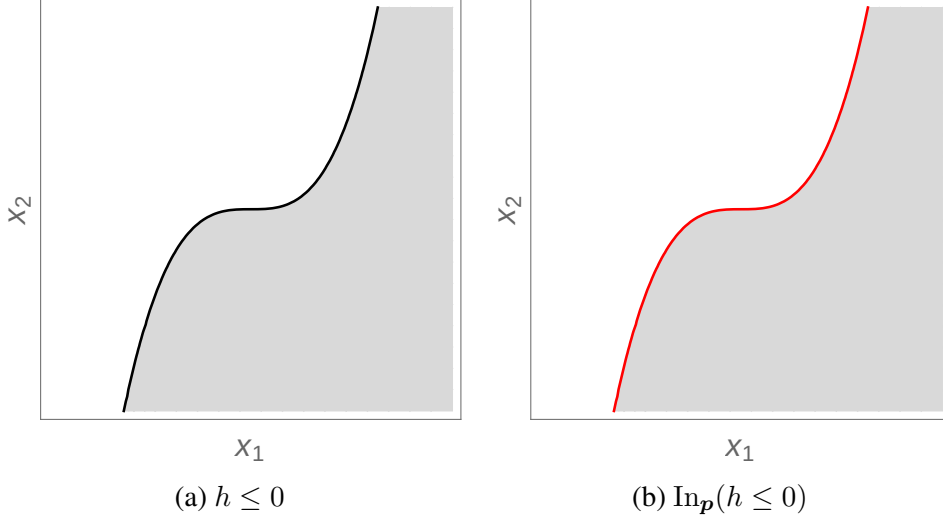


Figure 4: Constructing $\text{In}_{\mathbf{p}}(h \leq 0)$ using higher-order Lie derivatives.

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

Theorem 19 ([16]). *Given a polynomial system $\dot{\mathbf{x}} = \mathbf{p}(\mathbf{x})$ 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*

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

344

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

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

348 and the solution to $\dot{\mathbf{x}} = -\mathbf{p}(\mathbf{x})$ is given by $\mathbf{x}(-t)$, where $\mathbf{x}(t)$ is the solution to
 349 $\dot{\mathbf{x}} = \mathbf{p}(\mathbf{x})$. Once all the semi-algebraic sets in the premise of LZZ are constructed,
 350 the validity of the premise can be decided using a decision procedure for real
 351 arithmetic [30].

352 **6. Hierarchy**

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

359 Given two proof rules R_1 and R_2 of the form

$$(R_1) \frac{P_1}{(S_1 : T_1) \longrightarrow [\dot{\mathbf{x}} = \mathbf{p}](S_1 : T_1)} \quad (R_2) \frac{P_2}{(S_2 : T_2) \longrightarrow [\dot{\mathbf{x}} = \mathbf{p}](S_2 : T_2)} \quad (11)$$

360 where P_i refers to the premise of the proof rule R_i , and the conclusion has the form
 361 $(S_i : T_i) \longrightarrow [\dot{\mathbf{x}} = \mathbf{p}](S_i : T_i)$, where $S_i : T_i$ denotes that the set S_i is of type T_i
 362 (the typical types we are considering in this work are algebraic and semi-algebraic
 363 sets).

364 **Definition 20** (Partial order over proof rules). *Let R_1 and R_2 be two proof rules*
 365 *of the form of Eq. (11). We say that R_2 generalizes R_1 and write $R_2 \succcurlyeq R_1$ (or*
 366 *$R_1 \preccurlyeq R_2$), if the premise of R_1 implies the premise of R_2 ($P_1 \rightarrow P_2$), and T_1*
 367 *is a subtype of T_2 (for instance, the type algebraic set is a subtype of the type*
 368 *semi-algebraic set).*

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

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

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

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

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

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

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

392 For convenience, the propositions of this section are summarized in the compar-
 393 ison matrices in Fig. 6 and Fig. 8. For instance, Prop. 25 proves that $\text{FI} \prec \succ \text{Lie}$.
 394 Cells without numbers are proved by transitivity of the partial order. For instance,
 395 $\text{FI} \prec \text{DRI}$ can be proved using $\text{FI} \prec \text{C-c}$ (Prop. 21) and $\text{C-c} \prec \text{P-c}$ (Prop. 22)
 396 and $\text{P-c} \prec \text{DRI}$ (Prop. 24). The Hasse diagram (Fig. 5) gives the lattice structure
 397 where arrows represent strictly increasing deductive power; every missing edge in
 398 the graph represents $\prec \succ$, as shown in the comparison matrix.

399 6.1. Proof Rules for Algebraic Sets

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

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

408 *Proof.* The premise of the rule C-c requires the existence of some $\lambda \in \mathbb{R}$, such
 409 that $\mathcal{L}_{\mathbf{p}}(h) = \lambda h$. In particular, $\lambda = 0$ gives the premise of FI. Thus, $\text{FI} \preceq \text{C-c}$.
 410 To see that $\text{FI} \not\preceq \text{C-c}$, consider the one-dimensional vector field $\mathbf{p} = (x)$, we
 411 have $\mathcal{L}_{\mathbf{p}}(x) = 1x$, and hence C-c ($\lambda = 1$) concludes that $x = 0$ is an invariant.
 412 However, FI cannot prove the invariance of $x = 0$ because x is not a conserved
 413 quantity in the system. \square

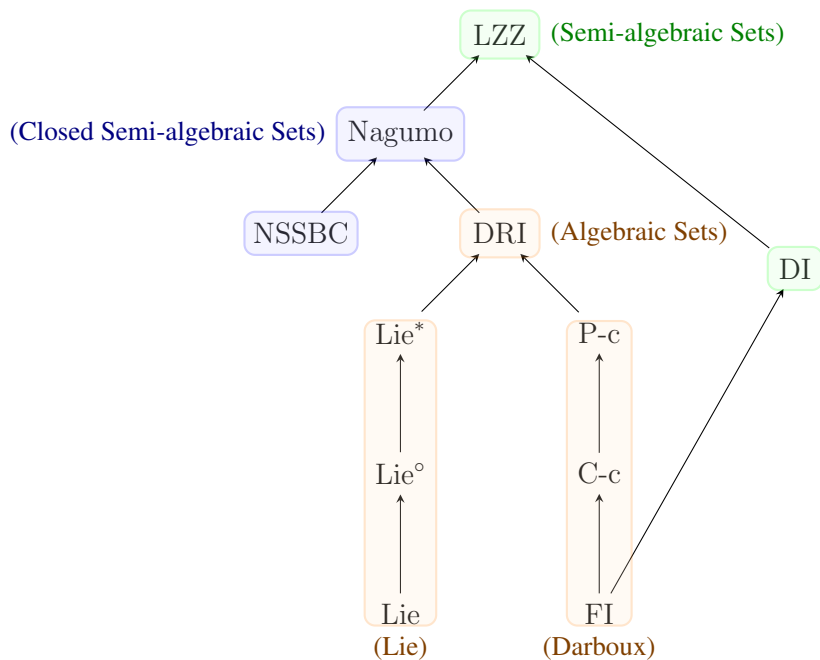


Figure 5: Hasse diagram. An arrow $R_1 \rightarrow R_2$ means $R_1 \prec R_2$; absence of connecting arrow(s) means $(\prec \succ)$.

414 **Proposition 22.** $C\text{-}c \prec P\text{-}c$.

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

422 **Proposition 23.** $\text{Lie} \prec \text{Lie}^\circ$ and $\text{Lie}^\circ \prec \text{Lie}^*$.

423 *Proof.* We already established that $\text{Lie} \preceq \text{Lie}^\circ$ (Prop. 8) and $\text{Lie}^\circ \preceq \text{Lie}^*$ (Prop. 7);
 424 we give two counterexamples to establish the strict inclusion. **(I)** $\text{Lie} \not\preceq \text{Lie}^\circ$.
 425 Whenever the variety has a singularity, the proof rule Lie will fail. Lie° is tai-
 426 lored to prove invariance of equilibrium points in addition to regular points of the
 427 variety. For instance, for $\mathbf{p} = ((-1 + x_1)x_2, x_2(1 + x_2))$, Lie fails to prove that
 428 $h = (-1 + x_1)^2 + (1 + x_2)^2 = 0$ is invariant as the gradient ∇h vanishes at $(1, -1)$

	FI	C-c	P-c	Lie	Lie ^o	Lie*	DRI
FI	~ 21	⋪	⋪	⋪⋪ 25	⋪⋪ 28	⋪⋪ 27	⋪
C-c	⋪ 21	~	⋪	⋪⋪ 29	⋪⋪ 30	⋪⋪ 30	⋪
P-c	⋪ 22	⋪	~	⋪⋪ 29	⋪⋪ 30	⋪⋪ 30	⋪ 24
Lie	⋪⋪ 25	⋪⋪ 29	⋪⋪ 29	~	⋪ 23	⋪	⋪
Lie ^o	⋪⋪ 28	⋪⋪ 30	⋪⋪ 30	⋪ 23	~	⋪ 23	⋪
Lie*	⋪⋪ 27	⋪⋪ 30	⋪⋪ 30	⋪	⋪ 23	~	⋪ 24
DRI	⋪	⋪	⋪	⋪	⋪	⋪	~

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

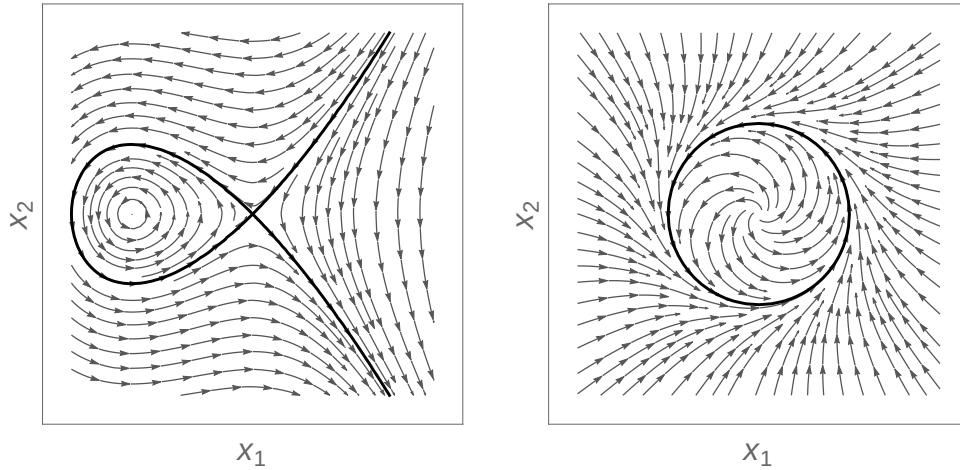
429 and $h((1, -1)) = 0$. However, at $(1, -1)$ we also have $p_1 = p_2 = 0$, and hence
430 the premise of Lie^o is satisfied, and $h = 0$ is proved to be an invariant under the
431 flow of \mathbf{p} . **(II)** $\text{Lie}^o \not\preceq \text{Lie}^*$. In addition to equilibria, Lie^* goes one step further
432 and handles all singular points, \mathbf{x} , where the vector $\mathbf{x} + \lambda\mathbf{p}$ is in the variety $V_{\mathbb{R}}(h)$
433 for all $\lambda \in \mathbb{R}$ (that is $h(\mathbf{x} + \lambda\mathbf{p}) = 0$, for all λ). For instance, consider the poly-
434 nomial $h = x_1x_2x_3$, its singular locus is given by the three axes $x_1 = x_2 = 0$,
435 $x_1 = x_3 = 0$ and $x_2 = x_3 = 0$. For the vector field $\mathbf{p} = (x_1, x_2, x_3)$, the equi-
436 librium point is at the origin $(0, 0, 0)$, which obviously does not contain the entire
437 singular locus of h . Thus, Lie^o fails but Lie^* succeeds because $h(\mathbf{x} + \lambda\mathbf{p}) = 0$
438 when \mathbf{x} is a point of one of the axes. \square

439 **Proposition 24.** $\text{P-c} \prec \text{DRI}$ and $\text{Lie}^* \prec \text{DRI}$.

440 *Proof.* DRI is both necessary and sufficient [10], so we know that $\text{P-c} \preceq \text{DRI}$ and
441 $\text{Lie}^* \preceq \text{DRI}$. To prove the claim it is left to show that **(I)** $\text{P-c} \not\preceq \text{DRI}$. Consider
442 the following two-dimensional vector field: $\mathbf{p} = ((-1+x_1)(1+x_1), (-1+x_2)(1+x_2))$.
443 The candidate invariant (given by the roots of the Motzkin polynomial)
444 $h = 1 - 3x_1^2x_2^2 + x_1^4x_2^2 + x_1^2x_2^4 = 0$ cannot be proved using P-c, as $\mathfrak{L}_{\mathbf{p}}(h) \notin \langle h \rangle$.
445 However, the invariance property may be proved using DRI. For this, we need
446 to consider the second-order Lie derivative of h and we prove that $\mathfrak{L}_{\mathbf{p}}^{(2)}(h) \in$
447 $\langle h, \mathfrak{L}_{\mathbf{p}}(h) \rangle$. Thus, the premise of DRI holds for $N = 2$. **(II)** $\text{Lie}^* \not\preceq \text{DRI}$.
448 Consider the following three-dimensional vector field $\mathbf{p} = (-x_2 + x_1(1 - x_1^2 -$

449 $x_2^2), x_1 + x_2(1 - x_1^2 - x_2^2), x_3)$. We want to prove that $h = (-1 + x_1^2 + x_2^2)^2 + x_3^2 = 0$
 450 is an invariant. In this case, the variety $V_{\mathbb{R}}(h)$ is exactly equal to the singular locus
 451 of h which is the two-dimensional unit circle $-1 + x_1^2 + x_2^2 = 0$. However, at
 452 all points of this unit circle, the vector field \mathbf{p} is equal to $(-x_2, x_1, 0) \neq 0$, which
 453 prevents us from using Lie* (because $h((x_1, x_2, 0) + \lambda(-x_2, x_1, 0)) \neq 0$ for some
 454 $\lambda \in \mathbb{R}$). The rule DRI proves the invariance of $h = 0$ with $N = 2$. \square

455 To appreciate the difference between FI and Lie, let us note that while the condi-
 456 tion in the premise of FI may seem strong (i.e. too conservative), singularities
 457 in the invariant candidate do not present a problem for FI, whereas the premise
 458 of Lie rules out such candidates altogether (see Fig. 7). Indeed, the proof rule Lie
 459 cannot prove that $0 = 0$ (the whole space is invariant), whereas this is the most
 460 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.

461 **Proposition 25** (FI and Lie are incomparable.). $\text{FI} \prec \succ \text{Lie}$.

462 *Proof.* (I) $\text{FI} \not\prec \text{Lie}$. For the vector field $\mathbf{p} = (-2x_2, -2x_1 - 3x_1^2)$, the equation
 463 $x_1^2 + x_1^3 - x_2^2 = 0$ is provable with FI but not Lie, see Fig. 7 (left). (II) $\text{FI} \not\prec \text{Lie}$.
 464 For the vector field $\mathbf{p} = (x_1 - x_1^3 - x_2 - x_1x_2^2, x_1 + x_2 - x_1^2x_2 - x_2^3)$, the invariance

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

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

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

472 *Proof.* Consider three proof rules R_1, R_2 and R_3 . If $R_2 \preceq R_3$, using $R_1 \preceq R_2$, one
 473 gets by transitivity $R_1 \preceq R_3$, which contradicts the assumption $R_3 \prec \succ R_1$. \square

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

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

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

482 *Proof.* By Lem. 26, from $\text{Lie} \preceq \text{Lie}^\circ$ (Prop. 8) and $\text{FI} \prec \succ \text{Lie}$ (Prop. 25), we
 483 get $\text{Lie}^\circ \not\preceq \text{FI}$. On the other hand, if $\text{FI} \preceq \text{Lie}^\circ$ then, by transitivity $\text{FI} \preceq \text{Lie}^*$
 484 (since $\text{Lie}^\circ \preceq \text{Lie}^*$ by Prop. 7), which contradicts $\text{FI} \prec \succ \text{Lie}^*$ (Prop. 27). Thus,
 485 $\text{FI} \not\preceq \text{Lie}^\circ$, and the proposition follows. \square

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

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

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

494 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).

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

496 *Proof.* Since $\text{FI} \prec d$, if $d \preceq \ell$, then $\text{FI} \preceq \ell$. However, $\text{FI} \prec \succ \ell$ (Prop. 27 and
497 Prop. 28). Thus $d \not\preceq \ell$. Similarly, since $\ell \succ \text{Lie}$, if $d \succ \ell$, then $d \succ \text{Lie}$ which
498 contradicts $d \prec \succ \text{Lie}$ (Prop. 29). Hence $d \not\preceq \ell$ and the proposition follows. \square

499 **Remark 31.** Provided that the invariant candidate has no singular points, Lie's
500 criterion is known to be both necessary and sufficient to prove invariance prop-
501 erties of level sets [20, Theorem 2.8]. Also, FI characterizes invariant functions
502 [23] but not all invariant equations. On the other hand, for algebraic differ-
503 ential equations, the differential radical criterion in DRI fully characterizes all
504 invariant algebraic sets [10]. Thus, as established in Prop. 24, DRI increases the
505 deductive power of both Darboux-based rules $\{\text{FI}, C\text{-c}, P\text{-c}\}$ and Lie-based rules
506 $\{\text{Lie}, \text{Lie}^\circ, \text{Lie}^*\}$, which form different families.

507 6.2. Proof Rules for Semi-Algebraic Sets

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

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

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

511 **Proposition 32.** $\text{NSSBC} \prec \text{Nagumo}$.

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

514 sets and polynomial ODE. Hence NSSBC \approx Nagumo. To see why the inequality
 515 is strict, consider any vector field with an invariant algebraic set (recall that
 516 algebraic sets are special closed semi-algebraic sets with empty interior). The
 517 proof rule NSSBC cannot work for such invariant sets precisely because it re-
 518 quires $\mathcal{L}_p(h) < 0$ whenever $h = 0$. In fact, $h = 0 \rightarrow \mathcal{L}_p(h) = 0$ is a necessary
 519 condition for any invariant algebraic set. \square

520 **Proposition 33.** Nagumo \prec LZZ and DI \prec LZZ.

521 *Proof.* For semi-algebraic sets, the proof rule LZZ characterizes (arbitrary) invari-
 522 ant semi-algebraic sets for polynomial ODE. The Nagumo theorem only charac-
 523 terizes closed semi-algebraic sets. Hence the strict inequality. Similarly, DI gives
 524 only a sufficient condition and is therefore strictly less powerful than LZZ. \square

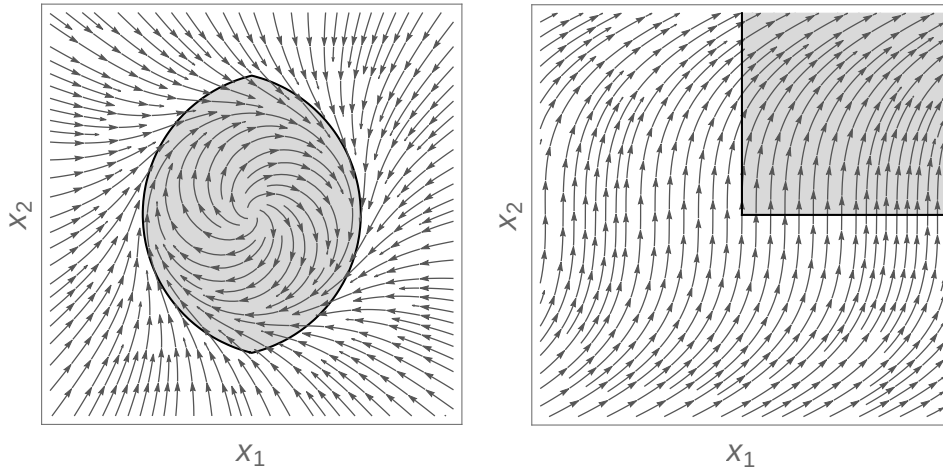
525 **Proposition 34.** NSSBC \prec DI.

Proof. DI $\not\prec$ NSSBC. Consider the system

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

526 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
 527 positively invariant set under the flow of the system (see Fig. 9a). The invariance
 528 property cannot be proved using the rule DI, but is easily proved using NSSBC
 529 (and LZZ).

530 NSSBC $\not\prec$ DI. Consider the system $\mathbf{p}(\mathbf{x}) = (x_2^2, 2)$ and let $S_2 \equiv x_2 \geq 0 \wedge$
 531 $x_1 \geq 0$. Positive invariance of S_2 is proved easily using either DI (and LZZ), but
 532 cannot be proved using NSSBC. Intuitively, this can be seen because at the origin
 533 the vector $\mathbf{p}(\mathbf{0})$ does not point strictly into the interior of $S_2 \equiv \max(-x_2, -x_1) \leq$
 534 0 , since $\mathcal{L}_p(-x_1) = -x_2^2|_0 = 0$ (see Fig. 9b). \square



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

(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).

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

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

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

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

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

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

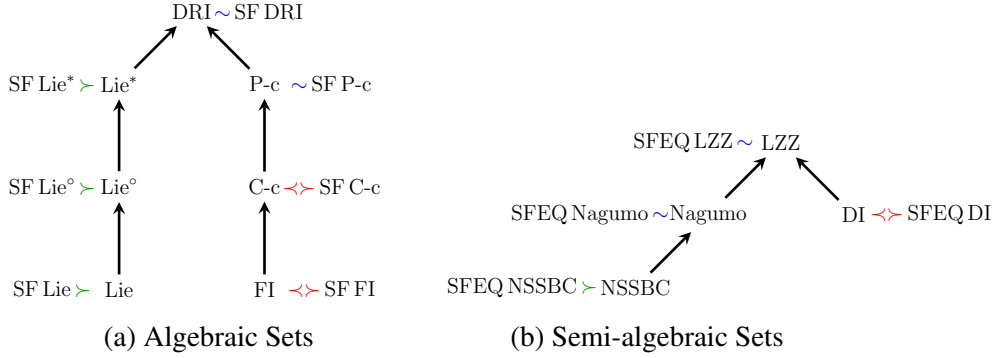


Figure 10: Square-free Reduction (Summary)

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

556 **Remark 38.** *The premises of the proof rules for algebraic sets could be used to*
 557 *work with a larger class of invariant sets, namely those of the form $h \geq 0$ in*
 558 *addition to algebraic sets. For instance, if $\mathcal{L}_p(h) \in \langle h \rangle$, then necessarily $h \geq$*
 559 *0 is an invariant of the system. In fact, the invariance of $h = 0$ implies the*
 560 *invariance of $h \bowtie 0$ for $\bowtie \in \{\leq, <, \geq, >\}$. Such extra proof rules do not bring any*
 561 *additional insight to the realm of proof rules depicted in Fig. 5 and are therefore*
 562 *not represented.*

563 7. Square-free Reduction

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

568 7.1. Square-free Reduction with Lie-based Proof Rules

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

572 to prove that $h = x^2 - 6x + 9 = 0$ is invariant, no matter what vector field one
573 considers. The reason for this is simple: $x^2 - 6x + 9$ factorizes into $(x - 3)^2$. The
574 problem here lies in the polynomial h itself, rather than the real variety $V_{\mathbb{R}}(h)$. In
575 fact, $V_{\mathbb{R}}(h)$ is exactly the singular locus of h and the proof rule `Lie` fails because
576 *all* points inside $V_{\mathbb{R}}(h)$ are singular points. More generally, the chain rule implies
577 $\nabla h^k \cdot \mathbf{p} = kh^{k-1} \nabla h \cdot \mathbf{p}$, which has the consequence that any polynomial h which
578 is not square-free will have vanishing gradient at the real roots of factors with
579 multiplicity greater than 1.

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

$$\text{SF}(h) = \frac{h}{\text{gcd}(h, \frac{\partial h}{\partial x_1}, \dots, \frac{\partial h}{\partial x_n})}. \quad (12)$$

583 Intuitively, in performing square-free reduction we hope to shrink the singular
584 locus of the original polynomial. If $\text{SL}(\text{SF}(h))$ is the empty set (which is the case
585 for $h = x^2 - 6x + 9$ in the example given above), the proof rule `Lie` applies to
586 $\text{SF}(h)$ but not to h . In general, $\text{SF}(h)$ may satisfy the assumptions of the proof
587 rules `Lie`[◦] or `Lie`^{*}, where h fails to do so. It is always sound to conclude that $h = 0$
588 is invariant from the knowledge that $\text{SF}(h) = 0$ is invariant, since real varieties
589 remain unaltered under square-free reduction of their defining polynomials [5],
590 i.e. $V_{\mathbb{R}}(h) \equiv V_{\mathbb{R}}(\text{SF}(h))$. Thus, replacing h with $\text{SF}(h)$ in the premise of `Lie`,
591 `Lie`[◦] and `Lie`^{*} does not compromise soundness (it is a use of the generalization
592 proof rule [21]) and enlarges the class of polynomials that these proof rules can
593 work with.

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

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

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

605 7.2. Square-free Reduction with Darboux-based proof rules

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

610 **Proposition 40.** FI \prec SFFI.

611 *Proof.* (I) FI $\not\prec$ SFFI. The polynomial $h = x^2y$ is an invariant function for
 612 the vector field $\mathbf{p} = (\frac{\partial h}{\partial y}, -\frac{\partial h}{\partial x}) = (x^2, -2xy)$, thus FI proves the invariance of
 613 $h = 0$. However, SF(h) is not an invariant function for the same vector field, since
 614 $\mathcal{L}_{\mathbf{p}}(\text{SF}(h)) = \mathcal{L}_{\mathbf{p}}(xy) = -x^2y \neq 0$, thus SFFI fails to prove the invariance of
 615 $h = 0$. (II) SFFI $\not\prec$ FI. Similarly, the polynomial $h = xy$ is an invariant function
 616 for the vector field $\mathbf{p} = (\frac{\partial h}{\partial y}, -\frac{\partial h}{\partial x}) = (x, -y)$, thus SFFI proves the invariance
 617 of $x^2y = 0$, since SF(x^2y) = h . However, FI fails to prove the invariance of
 618 $x^2y = 0$, because $\mathcal{L}_{\mathbf{p}}(x^2y) = x^2y \neq 0$. \square

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

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

626 **Proposition 41.** C-c \prec SFC-c.

627 *Proof.* (I) C-c $\not\prec$ SFC-c. The proof rule C-c proves the invariance of $h = x^2y =$
 628 0 for the vector field $\mathbf{p} = (x^2, y(1 - 2x))$ as $\mathcal{L}_{\mathbf{p}}(h) = 1h$. However, C-c cannot
 629 prove SF(h) = 0, since $\mathcal{L}_{\mathbf{p}}(\text{SF}(h)) = \mathcal{L}_{\mathbf{p}}(xy) = (1 - x) \text{SF}(h)$. (II) SFC-c $\not\prec$
 630 C-c. For the same h , C-c proves the invariance of SF(h) = 0 for the vector field
 631 $\mathbf{p} = (x^2, y(1 - x))$ as $\mathcal{L}_{\mathbf{p}}(\text{SF}(h)) = \mathcal{L}_{\mathbf{p}}(xy) = 1 \text{SF}(h)$. However, without the SF
 632 reduction C-c alone fails to prove the invariance of $h = 0$ for the considered \mathbf{p} , as
 633 $\mathcal{L}_{\mathbf{p}}(h) = (x + 1)h$. \square

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

638 also Darboux for the same vector field. Our findings are stated in Prop. 42 and its
 639 corollary Prop. 43.⁵

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

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

$$\mathfrak{L}_{\mathbf{p}}(h) = \mathfrak{L}_{\mathbf{p}}(q_1^{m_1} \cdots q_r^{m_r}) \quad (13)$$

$$= \sum_{i=1}^r \left(m_i \mathfrak{L}_{\mathbf{p}}(q_i) q_i^{m_i-1} \prod_{j \neq i} q_j^{m_j} \right) \quad (14)$$

$$= \sum_{i=1}^r m_i \mathfrak{L}_{\mathbf{p}}(q_i) q_i^{m_i-1} \frac{h}{q_i^{m_i}} \quad (15)$$

$$= h \sum_{i=1}^r m_i \frac{\mathfrak{L}_{\mathbf{p}}(q_i)}{q_i} \quad (16)$$

$$\in \langle h \rangle, \quad (17)$$

643 and h is also Darboux for \mathbf{p} .

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

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

646 For a fixed i , q_i divides $\text{SF}(h)$, it thus divides the left hand side of Eq. (18). More-
 647 over, q_i divides $\frac{\text{SF}(h)}{q_j}$, for all $j \neq i$. It thus necessarily divides $m_i \frac{\text{SF}(h)}{q_i} \mathfrak{L}_{\mathbf{p}}(q_i)$.
 648 If q_i divides $\frac{\text{SF}(h)}{q_i}$, then there exists $j \neq i$ such that q_i divides q_j , which contra-
 649 dicts the fact that all factors q_1, \dots, q_r are irreducible. Thus, q_i divides $\mathfrak{L}_{\mathbf{p}}(q_i)$ and
 650 $\mathfrak{L}_{\mathbf{p}}(q_i) \in \langle q_i \rangle$. \square

651 **Proposition 43.** P-c \sim SFP-c.

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

652 *Proof.* The proof rule P-c proves the invariance of $h = 0$ for \mathbf{p} if and only if
 653 the polynomial h is Darboux. However, by Prop. 42, h is Darboux if and only if
 654 $\text{SF}(h)$ is also Darboux. Therefore, SFP-c could be used equivalently to prove the
 655 invariance of $h = 0$. \square

656 **Remark 44.** *The condition $\mathfrak{L}_{\mathbf{p}}(h) \in \langle \text{SF}(h) \rangle$ —which is weaker than $\mathfrak{L}_{\mathbf{p}}(h) \in$
 657 $\langle h \rangle$ —is not sufficient to prove the invariance of $h = 0$. It is therefore an unsound
 658 proof rule. Consider the polynomial $h = (-1 + x^2)^2$ and the 1-dimensional
 659 vector field $\dot{x} = x$. Although $\mathfrak{L}_{\mathbf{p}}(h) = 4(-1 + x^2)x^2 \in \langle -1 + x^2 \rangle = \langle \text{SF}(h) \rangle$,
 660 the equation $h = 0$ is not invariant, however, because $x(t) = \pm e^t$. Notice that
 661 the proof rule P-c (with or without the square-free reduction) is unable to prove
 662 or disprove the invariance of $h = 0$.*

663 7.3. Square-free Reduction On Differential Radical Invariants (DRI)

664 Square-free reduction cannot increase the deductive power of the proof rule
 665 DRI because its premise is necessary and sufficient to prove invariance of real
 666 algebraic sets, which is unaffected by applying SF reduction. However, the com-
 667 putational impact of using square-free reduction with DRI remains an interesting
 668 question. Empirically, we observed a better performance of DRI when the SF
 669 reduction is applied first. In addition to lowering the degrees of the involved poly-
 670 nomials (as it did for Lie-based proof rules), we observed that the order N_{SF} for
 671 $\text{SF}(h)$ is always lower than the order N for h . We, therefore, conjecture $N_{\text{SF}} \leq N$.
 672 However, we identified an example (cf. Ex. 45 below) for which square-free re-
 673 duction resulted in a significant ($\times 100$) computational overhead due to the ideal
 674 membership checking (which we perform using Gröbner bases with reverse lex-
 675 icographic monomial ordering). In our implementation of DRI, called DRI_{opt} in
 676 the sequel, we use the square-free reduction only as a pre-processing step for the
 677 quantifier elimination problems in the premise of DRI.

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

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

and let

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

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

688 **Remark 46.** Notice that Prop. 42 does not have an analogue for DRI. In other
689 words, if a polynomial equation $h = 0$ is invariant for \mathbf{p} , its irreducible factors
690 need not define invariant equations themselves. Geometrically, this means that if
691 a variety is invariant under the flow of \mathbf{p} , its irreducible components need not be
692 invariants under the flow of \mathbf{p} . For instance, consider the irreducible polynomials
693 $q_1 = y - 1$ and $q_2 = x^2 + (y - 1)^2$. The equation $q_1q_2 = 0$ which is equivalent
694 to $y = 1$, is invariant for $\mathbf{p} = (1, 0)$, since the premise of the proof rule DRI
695 holds true for $N = 3$. However, the equation $q_2 = 0$, which is equivalent to
696 $x = 0 \wedge y = 1$, is not an invariant equation for \mathbf{p} . The reason for the invariance
697 of $q_1q_2 = 0$, which is equivalent to $q_1 = 0 \vee q_2 = 0$, stems from q_1 not from q_2 .

698 **7.4. Order parity decomposition**

699 Similar to square-free reduction for invariant polynomial equations, one may
700 sometimes remove roots of multiplicities greater than 1 from polynomial inequalities $p \leq 0$, thereby simplifying their description and removing singularities on
701 their boundary. To do this, we will require some definitions, due to Dolzmann and
702 Sturm (see [7]).
703

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

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

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

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

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

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

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

- 713 1. $h = 0 \equiv_{\mathbb{R}} \text{SF}(h) = 0$,
- 714 2. $h \neq 0 \equiv_{\mathbb{R}} \text{SF}(h) \neq 0$,
- 715 3. $h > 0 \equiv_{\mathbb{R}} h_o h_e^2 > 0 \equiv_{\mathbb{R}} h_o > 0 \wedge h_e \neq 0$,
- 716 4. $h \geq 0 \equiv_{\mathbb{R}} h_o h_e^2 \geq 0 \equiv_{\mathbb{R}} h_o \geq 0 \vee h_e = 0$,
- 717 5. $h < 0 \equiv_{\mathbb{R}} h_o h_e^2 < 0 \equiv_{\mathbb{R}} h_o < 0 \wedge h_e \neq 0$,
- 718 6. $h \leq 0 \equiv_{\mathbb{R}} h_o h_e^2 \leq 0 \equiv_{\mathbb{R}} h_o \leq 0 \vee h_e = 0$.

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

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

726 **Theorem 50.** SFEQ NSSBC \succ NSSBC.

727 *Proof.* If $\mathfrak{L}_p(h) < 0$ is true when h is an active component ($h = 0$), it is nec-
 728 essarily the case that h is square-free. Thus $\text{SFEQ}(h) = h$ (which then equals
 729 $\text{SF}(h)$) and, therefore, SFEQ NSSBC \succ NSSBC. Let $\dot{\mathbf{x}} = \mathbf{p}(\mathbf{x}) = (-x_1, -x_2)$
 730 and consider the set $S \equiv (x_1^2 + x_2^2 - 1)^3 \leq 0$. Applying NSSBC fails to prove the
 731 positive invariance property. Computing the order parity decomposition, we get
 732 $\text{SFEQ}(S) \leq 0 \equiv (x_1^2 + x_2^2 - 1) \leq 0$, for which positive invariance under the flow
 733 of $\mathbf{p}(\mathbf{x})$ is proved easily using NSSBC. \square

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

$$\begin{aligned}\dot{x}_1 &= -x_1 - x_2 + x_1x_2^2 + x_1^3, \\ \dot{x}_2 &= x_1 - x_2 + x_1^2x_2 + x_2^3.\end{aligned}$$

*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:*

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

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

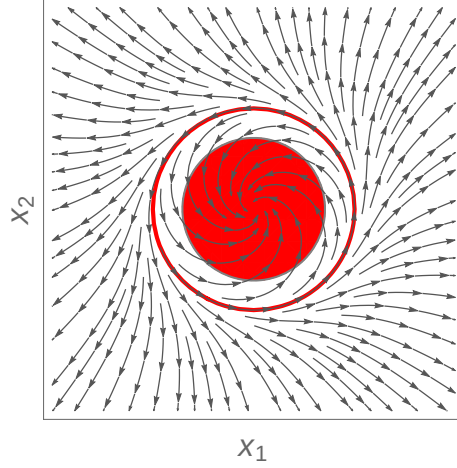


Figure 11: Positively invariant set given by $h \leq 0$ (in red).

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

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

$$(Inv_{\vee}) \frac{S_1 \rightarrow [\dot{\mathbf{x}} = \mathbf{p}(\mathbf{x})] S_1 \quad S_2 \rightarrow [\dot{\mathbf{x}} = \mathbf{p}(\mathbf{x})] S_2}{S_1 \vee S_2 \rightarrow [\dot{\mathbf{x}} = \mathbf{p}(\mathbf{x})] (S_1 \vee S_2)}.$$

750 **Theorem 52.** $\text{SFEQ DI} \prec \succ \text{DI}$

751 *Proof.* Corollary to Proposition 40, since FI is a special case of DI and $\text{SFEQ}[h =$
 752 $0] \equiv \text{SF}(h) = 0$. \square

753 **Theorem 53.** $\text{SFEQ Nagumo} \sim \text{Nagumo}$.

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

756 Thus, a closed set S is positively invariant using Nagumo if and only if an equiv-
757 alent closed set $\text{SFEQ}[S]$ is positively invariant using Nagumo. \square

758 **Theorem 54.** $\text{SFEQ LZZ} \sim \text{LZZ}$.

759 *Proof.* Elementary, since LZZ is necessary and sufficient for proving positive in-
760 variance and $\text{SFEQ}[S]$ gives an equivalent set in \mathbb{R}^n . \square

761 8. Experimental Comparison

762 To complement the theoretical deductive power comparison with a practical
763 provability study, we empirically compare the running time performance of all the
764 proof rules discussed in this paper on a heterogeneous collection of benchmarks
765 (76 for algebraic sets and 20 for semi-algebraic sets).

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

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

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

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

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

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

804 *8.1. Running Time Performance for Algebraic Sets*

805 In this section, the prefix SF is implicit for all Lie-based proof rules. We con-
806 sider 4 equally sized classes of invariant sets: (1) 24 smooth invariants, where
807 Lie is both necessary and sufficient, (2) 17 isolated equilibria as trivial (for hu-
808 mans, not machines) equational invariants for which both Lie° and Lie^* provide
809 necessary and sufficient conditions, (3) 17 other singularities and high integrals,
810 (4) 18 functional invariants, where FI is necessary and sufficient. Figure 12 com-
811 pares the number of invariant varieties that each rule could prove within 60 sec-
812 onds. The vertical axis shows cumulative time spent on the problems. All runs
813 were performed on an Intel Core i5 1.7GHz machine with 4Gb RAM. Gener-
814 ally, we observe DRI performing very well across the entire spectrum of problem
815 classes. This is very encouraging, but also at first sight appears to defy intuition
816 since it implies that one does not necessarily sacrifice performance when opting
817 to use a more deductively powerful rule. In this graph, we also see that over-
818 all Lie° appears to offer an interesting compromise between deductive power and
819 efficiency—it is able to prove a significant body of problems that are out of scope
820 for Lie, while avoiding the complexity penalty which affects Lie^* (due to intro-
821 ducing an extra variable).

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

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

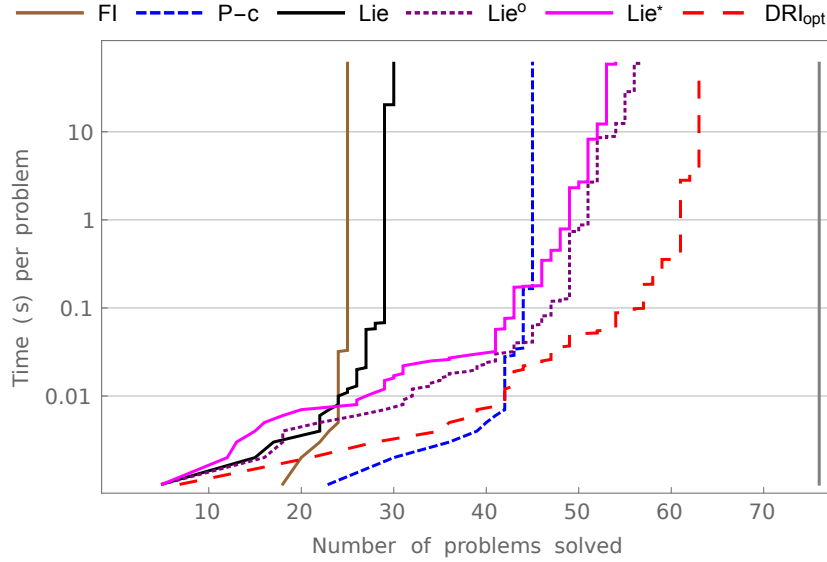


Figure 12: Experimental performance of proof rules: problems solved per time (log scale)

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

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

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

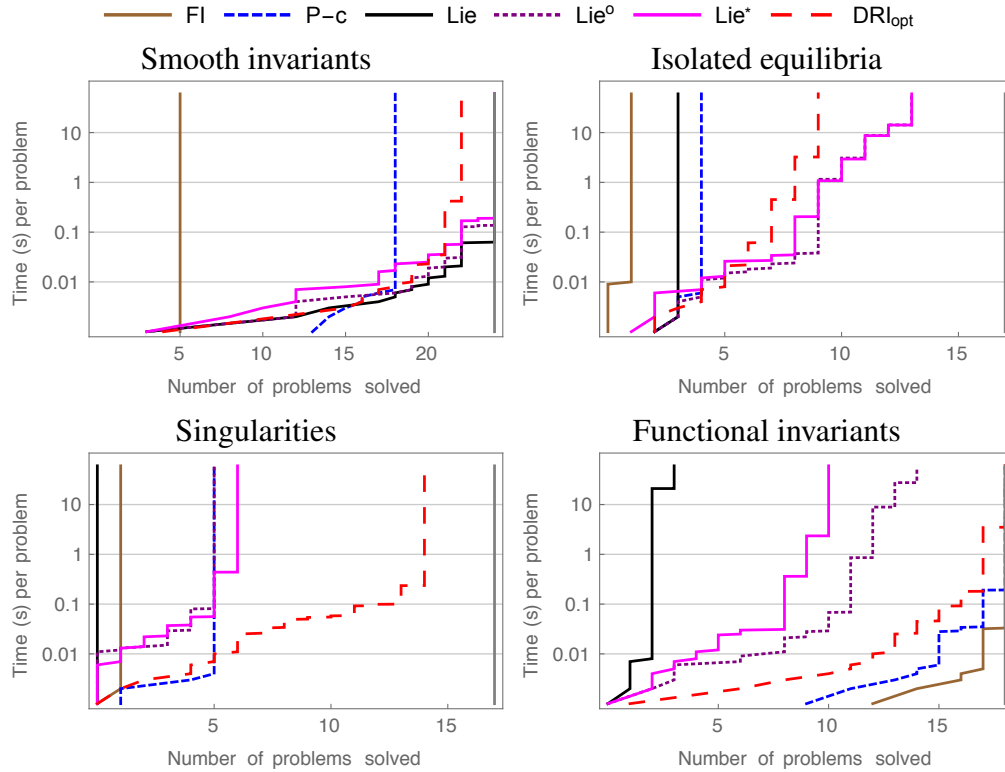


Figure 13: Number of problems solved per class (log scale).

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

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

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

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

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

882 8.2. *Running Time Performance for Semi-algebraic Sets*

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

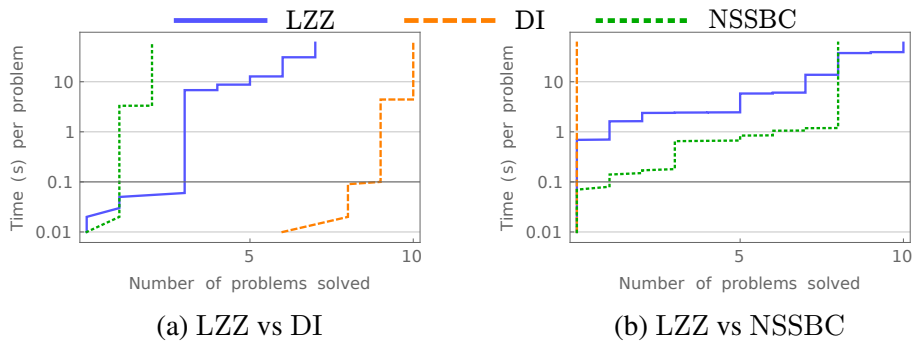


Figure 14: Number of problems solved in each class (times on log scale).

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

898 9. Conclusion

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

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

- 915 • Using the square-free reduction with the proof rules FI and C-c yields new
916 *incomparable* proof rules, whereas SF with P-c is as powerful as P-c alone.
- 917 • Performing square-free reduction of an invariant candidate may introduce
918 a performance penalty for DRI and therefore cannot be regarded as an op-
919 timization, even though there are instances for which it yields a speed-up.
920 The same can be said of order parity decomposition applied to an invariant
921 candidate supplied to LZZ.
- 922 • Sufficient rules DI and NSSBC can afford a speed-up on certain problems,
923 but the overall running time performance of the decision procedure LZZ is
924 observed to be good.
- 925 • Using a decision procedure LZZ appears to be more efficient than using the
926 sufficient condition NSSBC when the positively invariant candidate set is
927 described by a large formula.

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

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

- 937 [1] Basu, S., Pollack, R., Roy, M.-F., 1996. On the combinatorial and algebraic
938 complexity of quantifier elimination. *J. ACM* 43 (6), 1002–1045.
- 939 [2] Blanchini, F., Miani, S., 2008. *Set-Theoretic Methods in Control. Systems
940 & Control : Foundations & Applications.* Birkhäuser.
- 941 [3] Collins, G. E., 1975. Hauptvortrag: Quantifier elimination for real closed
942 fields by cylindrical algebraic decomposition. In: *Automata Theory and For-
943 mal Languages.* Vol. 33 of LNCS. Springer, pp. 134–183.
- 944 [4] Collins, G. E., Hong, H., Sep. 1991. Partial cylindrical algebraic decompo-
945 sition for quantifier elimination. *J. Symb. Comput.* 12 (3), 299–328.

- 946 [5] Cox, D. A., Little, J., O’Shea, D., 1997. Ideals, Varieties, and Algorithms -
947 an introduction to computational algebraic geometry and commutative alge-
948 bra (2. ed.). Springer.
- 949 [6] Darboux, J.-G., 1878. Mémoire sur les équations différentielles algébriques
950 du premier ordre et du premier degré. Bulletin des Sciences Mathématiques
951 et Astronomiques 2 (1), 151–200.
952 URL <http://eudml.org/doc/84988>
- 953 [7] Dolzmann, A., Sturm, T., 1995. Simplification of quantifier-free formulas
954 over ordered fields. Journal of Symbolic Computation 24, 209–231.
- 955 [8] Dumortier, F., Llibre, J., Artés, J. C., 2006. Qualitative Theory of Planar
956 Differential Systems. Springer.
- 957 [9] Faugère, J. C., 2002. A new efficient algorithm for computing Gröbner bases
958 without reduction to zero (F5). In: ISSAC. ACM, New York, NY, USA, pp.
959 75–83.
- 960 [10] Ghorbal, K., Platzer, A., 2014. Characterizing algebraic invariants by differ-
961 ential radical invariants. In: TACAS. Vol. 8413. Springer, pp. 279–294.
- 962 [11] Ghorbal, K., Sogokon, A., Platzer, A., 2014. Invariance of conjunctions of
963 polynomial equalities for algebraic differential equations. In: SAS. Vol. 8723
964 of LNCS. Springer, pp. 151–167.
- 965 [12] Ghorbal, K., Sogokon, A., Platzer, A., 2015. A hierarchy of proof rules for
966 checking differential invariance of algebraic sets. In: VMCAI. Vol. 8931 of
967 LNCS. Springer, pp. 431–448.
- 968 [13] Goriely, A., 2001. Integrability and Nonintegrability of Dynamical Systems.
969 Advanced series in nonlinear dynamics. World Scientific.
- 970 [14] Lie, S., 1893. Vorlesungen über continuierliche Gruppen mit Geometrischen
971 und anderen Anwendungen. Teubner, Leipzig.
- 972 [15] Lindelöf, E., 1894. Sur l’application de la méthode des approximations suc-
973 cessives aux équations différentielles ordinaires du premier ordre. Comptes
974 rendus hebdomadaires des séances de l’Académie des sciences 116, 454–
975 458.

- 976 [16] Liu, J., Zhan, N., Zhao, H., 2011. Computing semi-algebraic invariants for
977 polynomial dynamical systems. In: EMSOFT. ACM, pp. 97–106.
- 978 [17] Matringe, N., Moura, A. V., Rebiha, R., 2010. Generating invariants for non-
979 linear hybrid systems by linear algebraic methods. In: SAS. Vol. 6337 of
980 LNCS. Springer, pp. 373–389.
- 981 [18] Mayr, E. W., 1989. Membership in polynomial ideals over \mathbb{Q} is exponential
982 space complete. In: Monien, B., Cori, R. (Eds.), STACS. Vol. 349 of LNCS.
983 Springer, pp. 400–406.
- 984 [19] Nagumo, M., May 1942. Über die Lage der Integralkurven gewöhnlicher
985 Differentialgleichungen (in German). In: Proceedings of the Physico-
986 Mathematical Society of Japan. Vol. 24. pp. 551–559.
- 987 [20] Olver, P. J., 2000. Applications of Lie Groups to Differential Equations.
988 Springer.
- 989 [21] Platzer, A., 2008. Differential dynamic logic for hybrid systems. *J. Autom.*
990 *Reasoning* 41 (2), 143–189.
- 991 [22] Platzer, A., 2010. Differential-algebraic dynamic logic for differential-
992 algebraic programs. *J. Log. Comput.* 20 (1), 309–352.
- 993 [23] Platzer, A., 2012. A differential operator approach to equational differential
994 invariants - (invited paper). In: ITP. Vol. 7406 of LNCS. Springer, pp. 28–48.
- 995 [24] Platzer, A., 2012. The structure of differential invariants and differential cut
996 elimination. *Logical Methods in Computer Science* 8 (4), 1–38.
- 997 [25] Prajna, S., Jadbabaie, A., 2004. Safety verification of hybrid systems us-
998 ing barrier certificates. In: *In Hybrid Systems: Computation and Control*.
999 Springer, pp. 477–492.
- 1000 [26] Prajna, S., Jadbabaie, A., Pappas, G., 2007. A framework for worst-case and
1001 stochastic safety verification using barrier certificates. *Automatic Control*,
1002 *IEEE Transactions on* 52 (8), 1415–1428.
- 1003 [27] Richardson, D., 12 1968. Some undecidable problems involving elementary
1004 functions of a real variable. *Journal of Symbolic Logic* 33 (4), 514–520.

- 1005 [28] Sankaranarayanan, S., Sipma, H. B., Manna, Z., 2008. Constructing invari-
1006 ants for hybrid systems. *Form. Methods Syst. Des.* 32 (1), 25–55.
- 1007 [29] Taly, A., Tiwari, A., 2009. Deductive verification of continuous dynamical
1008 systems. In: *FSTTCS*. Vol. 4 of *LIPIcs*. pp. 383–394.
- 1009 [30] Tarski, A., 1951. A decision method for elementary algebra and geometry.
1010 *Bull. Amer. Math. Soc.* 59.
- 1011 [31] Tiwari, A., 2008. Abstractions for hybrid systems. *Form. Methods Syst. Des.*
1012 32 (1), 57–83.
- 1013 [32] Walter, W., 1998. *Ordinary Differential Equations*. Springer New York.
- 1014 [33] Wu, Z., 2010. Tangent cone and contingent cone to the intersection of two
1015 closed sets. *Nonlinear Analysis: Theory, Methods & Applications* 73 (5),
1016 1203 – 1220.