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)

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* (Sankaranarayanan et al., 2008; Platzer, 2010, 2012a; Tiwari, 2008).

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 (Ghorbal et al., 2015) to include proof rules that are concerned with checking positive invariance

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

of semi-algebraic sets. In addition to recalling proof rules reported previously, we introduce in Section 5.2 a new sufficient condition that we term NSSBC for Non-smooth Strict Barrier Certificate. NSSBC is able to prove positive invariance in a special class of closed semi-algebraic sets and can be seen as a generalization of strict barrier certificates introduced by Prajna (Prajna et al., 2007). We also investigate in Section 7.4 the effect of *square-free decomposition*—which generalizes the square-free reduction—on the deductive power of proof rules. Finally, we complement our theoretical results with a practical assessment of the proof rule performance on a set of benchmarks and explore interesting connections between the deductive power and the practical running time performance (Section 8.2).

2. Preliminaries

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

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 by $\mathbb{R}[x_1, \dots, x_n]$.

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

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

Since polynomial functions are smooth (C^∞ , i.e. they have derivatives up to any order), they are locally Lipschitz-continuous. By the Cauchy-Lipschitz theorem (a.k.a. Picard-Lindelöf) (Lindelöf, 1894), there exists a unique maximal solution to the initial value problem ($\dot{\mathbf{x}} = \mathbf{p}$, $\mathbf{x}(0) = \mathbf{x}_0$) defined for t in some non-empty open interval; it is often denoted by $\mathbf{x}(t)$, or more explicitly as $\varphi_t(\mathbf{x}_0)$.

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 is a (*positive*) *invariant* under the flow of $\mathbf{p}$. If S is described by a quantifier-free formula of real arithmetic (i.e. is a semi-algebraic set satisfying a finite boolean combination of polynomial equalities and inequalities), positive invariance of S

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 (Platzer, 2008):

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

65 A result about positive invariance of *closed* sets under the flow of locally
 66 Lipschitz-continuous ODEs, known as the Nagumo theorem (Nagumo, 1942; Wal-
 67 ter, 1998, Chapter 10, XV–XVI, pp. 117–119), gives a powerful (but generally in-
 68 tractable) geometric characterization of positively invariant closed sets. Nagumo’s
 69 theorem requires 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 (Liu et al., 2011).

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 (Sankaranarayanan et al., 2008), P-c in Figure 1, requires $\mathfrak{L}_{\mathbf{p}}(h)$ to be in
 106 the ideal generated by h . The condition given in the premise is only sufficient (but
 107 is eminently suitable for *generating* invariant varieties (Matringe et al., 2010)). We
 108 also consider the constant-scale consecution proof rule (Sankaranarayanan et al.,
 109 2008; Tiwari, 2008), denoted by C-c. The premise of proof rule C-c requires that
 110 $\mathfrak{L}_{\mathbf{p}}(h) = \lambda h$, where λ is a scalar, not a polynomial as in P-c. It is therefore a
 111 simple special case of P-c. When $\lambda = 0$, one obtains the premise of the proof
 112 rule FI. It is worth noting that the condition in the premise of P-c, including
 113 its special case C-c, was mentioned as early as 1878 (Darboux, 1878) and used
 114 extensively in the study of integrability of dynamical systems (e.g. see *second in-*
 115 *tegrals* in (Goriely, 2001, Chapter 2)). It serves as a natural extension to invariant
 116 functions, also known as *first integrals*, which are covered by the proof rule FI.

⁴We used the notation DI₌ for the same proof rule in (Ghorbal et al., 2015).

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

Figure 1: Proof rules for checking the invariance of $h = 0$ w.r.t. $\mathbf{p}$: FI, C-c and P-c (Sankaranarayanan et al., 2008, Lemma 2), Lie (Olver, 2000, Theorem 2.8), DRI (Ghorbal and Platzer, 2014, Theorem 2)

117 The proof rule Lie gives Lie’s criterion (Lie, 1893; Olver, 2000) for invariance of
 118 $h = 0$; this proof rule will be discussed in more depth and extended to handle
 119 tricky cases in Section 4. The last rule, DRI in Fig. 1, was recently introduced
 120 and characterizes (i.e. gives necessary and sufficient conditions for) invariant real
 121 varieties under the flow of polynomial vector fields (Ghorbal and Platzer, 2014).
 122 The number N in the premise of DRI is the maximum length of the ascending
 123 chain of polynomial ideals $\langle h \rangle \subset \langle h, \mathfrak{L}_{\mathbf{p}}(h) \rangle \subset \langle h, \mathfrak{L}_{\mathbf{p}}(h), \mathfrak{L}_{\mathbf{p}}^{(2)}(h) \rangle \subset \dots$, which
 124 is finite and computable (Ghorbal and Platzer, 2014).

125 4. Extending Lie’s Criterion

126 One immediate deficiency of the proof rule Lie (Fig. 1) is its inability to prove
 127 invariance properties for isolated points (e.g. system equilibria) for the simple
 128 reason that a description of such a point $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{R}^n$, e.g. given by the
 129 sum-of-squares equation $h(\mathbf{x}) = (x_1 - a_1)^2 + \dots + (x_n - a_n)^2 = 0$, will have an
 130 extremum at $\mathbf{a}$, i.e. $h(\mathbf{a}) = 0$ and
 131 $h(\mathbf{x}) > 0$ for all $\mathbf{x} \in \mathbb{R}^n \setminus \{\mathbf{a}\}$. Functions whose real roots characterize
 132 isolated points have vanishing gradient at these roots, in this case $\mathbf{a}$, and thus the
 133 formula $h = 0 \rightarrow \nabla h = \mathbf{0}$ holds. This violates the regularity condition in the
 134 premise of the proof rule Lie, namely:

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

135 In fact, $h = 0 \rightarrow \mathfrak{L}_{\mathbf{p}}(h) = 0$ is a necessary condition when $h = 0$ is an invariant
 136 equation. Note that simply removing Eq. (5) from the premise of the proof rule Lie

137 is unsound (see e.g. (Platzer, 2012a)); that is, the condition $h = 0 \rightarrow \mathfrak{L}_{\mathbf{p}}(h) = 0$
 138 alone is insufficient to prove the invariance property for $h = 0$. Unsoundness in
 139 the above naïve attempt at a generalization is a consequence of *singularities* that
 140 may be present in the variety $V_{\mathbb{R}}(h)$. Singularities of $V_{\mathbb{R}}(h)$ are points $\mathbf{x} \in V_{\mathbb{R}}(h)$
 141 where 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 $\text{SL}(h)$, is the set of singular points, that is, points $\mathbf{x}$ satisfying*

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

142 Points that are not singular are called regular. At singular points, the Lie derivative
 143 of h along any vector field is $\mathbf{0} \cdot \mathbf{p} = 0$. To avoid these degenerate cases, the
 144 regularity condition (Eq. (5)) rules out singularities altogether. In the next section
 145 we present two extensions of Lie’s criterion that, in a similar vein to (Taly and
 146 Tiwari, 2009), partially overcome the strong regularity condition by treating the
 147 points on the singular locus separately.

148 4.1. Handling Singularities

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

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

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

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

160 The Lie^o proof rule can be generalized further at the expense of adding an
 161 extra variable by replacing the “no flow” condition ($p_i = 0$) for points on the
 162 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).

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

163 To prove soundness of Lie° and Lie^* , we appeal to the Nagumo theorem. Let
 164 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
 165 $\text{dist}(S, \mathbf{x} + \lambda \mathbf{p}(\mathbf{x})) = 0$ and so $\mathbf{p}(\mathbf{x})$ is sub-tangential to S at $\mathbf{x}$. This obser-
 166 vation is important for algebraic sets, for which $\text{bdr}(S) = S$, and the condition
 167 $\mathbf{x} + \lambda \mathbf{p}(\mathbf{x}) \in S$ translates to $h(\mathbf{x} + \lambda \mathbf{p}(\mathbf{x})) = 0$. This is the main idea behind the
 168 soundness of the proof rule Lie^* .

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

170 *Proof.* A point on the variety is either regular or singular. For regular points
 171 (these form an *open subset* of the variety), since $\mathfrak{L}_{\mathbf{p}}(h)(\mathbf{x}) = 0$, the vector $\mathbf{p}(\mathbf{x})$
 172 is sub-tangent to the variety at $\mathbf{x}$ (in fact, it is even *tangent*, so the condition
 173 we check is exactly that which is used in Lie). At singular points $\mathbf{x} \in V_{\mathbb{R}}(h)$
 174 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
 175 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
 176 sub-tangential to $V_{\mathbb{R}}(h)$ at $\mathbf{x}$. Assuming solutions exist and are unique, the variety
 177 $V_{\mathbb{R}}(h)$ is positively invariant under the vector field $\mathbf{p}$ by Nagumo's theorem. $\square$

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

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

181 **Remark 9.** *It is worth remarking that the proof rules presented in this section,*
 182 *as well as Lie and FI , also work for non-polynomial vector fields and invariant*
 183 *candidates which themselves are not polynomial but sufficiently smooth. However,*
 184 *in such cases the resulting arithmetic may no longer be decidable (Richardson,*
 185 *1968).*

186 5. Proof rules for semi-algebraic sets

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

190 *5.1. Differential Invariants*

191 Differential induction with differential invariants (henceforth DI) was intro-
 192 duced in (Platzer, 2010, Theorem 1).

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

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

196 In DI, S is a quantifier-free first-order formula in the theory of real arithmetic
 197 and D is the *derivation operator* (Platzer, 2012a, Definition 3.2), which is defined
 198 as follows:

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

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

201 **Remark 11.** *Note that if S has the form $h \leq 0$ for a polynomial h , then the*
 202 *requirements in the premise of DI are exactly the conditions that a barrier certifi-*
 203 *cate (Prajna and Jadbabaie, 2004) has to satisfy. Thus, for this case, differential*
 204 *invariants include barrier certificates as a special case (Platzer, 2010). Barrier*
 205 *certificates are, however, also accompanied with interesting techniques for gener-*
 206 *ating such invariant regions.*

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

210 In practice, although differential invariants allow one to work with sets that
 211 are expressed using formulas with boolean operators, the conditions are very con-
 212 servative (because they are required to hold everywhere in the state space, rather
 213 than only on the boundary of the set defined by S) and may fail to hold even for
 214 seemingly simple positively invariant sets. That is why differential invariants are
 215 used in conjunction with differential cuts (Platzer, 2010, 2012b), a process of suc-
 216 cessively augmenting the system dynamics with provable invariants, which we do
 217 not consider here.

218 5.2. Non-Smooth Strict Barrier Certificate

219 Another criterion, which we term *non-smooth strict barrier certificate*, may
 220 be seen as a generalization of the strict barrier certificates criterion (Prajna and
 221 Jadbabaie, 2004; Prajna et al., 2007) (limited to closed sets of the form $h \leq 0$) to
 222 generic closed semi-algebraic sets. Notice that our generalization only concerns
 223 the sufficient conditions for checking the invariance of supplied candidates. In
 224 particular, we do not extend nor adapt the computation techniques (convex op-
 225 timization) underlying the barrier certificates generation to the new criterion we
 226 present in the sequel.

227 Given a closed semi-algebraic set $S \equiv \bigvee_{i=1}^k \bigwedge_{j=1}^{m(i)} h_{ij} \leq 0$ with polynomials
 228 $h_{ij} \in \mathbb{R}[x_1, \dots, x_n]$, we can equivalently rewrite S by a sub-level set of a contin-
 229 uous function, namely

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

needs to hold for at least some $i_* \in I_*$ (otherwise the premise of the proof rule is not satisfied). Without loss of generality, assume that at $\mathbf{x}_0$ there is one such i_* . The condition guarantees that for all polynomial arguments of the $\max$ function, their Lie derivative is strictly negative at $\mathbf{x}_0$. Since Lie derivatives of polynomials under polynomial vector fields are also polynomial functions (and thus continuous), there exists an open neighbourhood around $\mathbf{x}_0$ inside which $\mathfrak{L}_p(h_{i_*j}) < 0$ is true for all $j \in \{1, \dots, m(i_*)\}$. Thus, if the system is initialized at $\mathbf{x}_0$, it is guaranteed to enter the region where

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

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

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

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

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

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

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

$$0 \leq \frac{\text{dist}(S_1 \cup S_2, \mathbf{x}_0 + t\mathbf{v})}{t} \leq \frac{\text{dist}(S_1, \mathbf{x}_0 + t\mathbf{v})}{t} \quad \text{and by assumption}$$

$$0 \leq \liminf_{t \rightarrow 0^+} \frac{\text{dist}(S_1 \cup S_2, \mathbf{x}_0 + t\mathbf{v})}{t} \leq \liminf_{t \rightarrow 0^+} \frac{\text{dist}(S_1, \mathbf{x}_0 + t\mathbf{v})}{t} = 0.$$

from which it follows that if $\mathbf{v}$ is sub-tangential to S_1 at $\mathbf{x}_0$, then it is also 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 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 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 $\mathbf{x} \in S_1 \cup S_2$. $\square$

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

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

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 sets intersect at $\mathbf{0} \in \mathbb{R}^2$. At the origin, the intersection of the contingent cones is given by the real line, i.e. $K_{\mathbf{0}}(S_1) \cap K_{\mathbf{0}}(S_2) = \{\mathbf{x} \mid x_2 = 0\}$, whereas the contingent cone to the intersection of the two sets is given by the zero vector, $K_{\mathbf{0}}(S_1 \cap S_2) = \{\mathbf{0}\}$. See Figure 2 for an illustration and (Wu, 2010) for an overview this problem. $\square$

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

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

one would like to determine if $\mathbf{p}(\mathbf{x}) \in K_{\mathbf{x}}(S)$ 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

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

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 $\{0\}$.

278 It is possible to formulate inference rules based on Nagumo's theorem which
 279 allow one to prove positive invariance of a large class of closed semi-algebraic
 280 sets. This has previously been investigated in (Taly and Tiwari, 2009), where a
 281 number of inference rules are presented for checking positive invariance of closed
 282 sets of the form $h \geq 0$. For instance, it is shown that the following is a sound
 283 inference (similar to Lie):

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

284 along with other rules with more general premises, all of which seek to check
 285 membership of $p(x)$ in the contingent cone $K_x(h \geq 0)$. The lifting of the condi-
 286 tions to formulas with boolean connectives (leading to a potential proof rule for
 287 closed semi-algebraic sets) described in (Taly and Tiwari, 2009, p. 393) essen-
 288 tially requires each S_{ij} to be of the form $h_{ij} \geq 0$ and assumes the soundness-
 289 critical property (10). Soundness issues may arise when this assumption fails
 290 to hold (as in Fig. 2). This deficiency can be fixed by e.g. requiring the matrix
 291 of partial derivatives of active components on the boundary to be full rank, i.e.
 292 $rk(\nabla h_1, \nabla h_2, \dots, \nabla h_k) = k$ whenever the polynomials $h_1, h_2, \dots, h_k$ evaluate
 293 to 0 on the boundary (this need only apply to conjunctive components). A num-
 294 ber of other possible *sufficient conditions* for removing this source of unsound-

ness has been studied in non-smooth analysis (Wu, 2010) (see also *practical sets* in (Blanchini and Miani, 2008)). However, in practice, even ensuring the full-rank property for a matrix with polynomial entries is computationally expensive. Furthermore, even with conditions for soundness in place, the result may not be applied to reason about positive invariance of semi-algebraic sets that are neither closed nor open.

5.4. Liu, Zhan & Zhao Decision Procedure

In (Liu et al., 2011), it was shown that checking whether a given semi-algebraic set is positively invariant under the flow of a polynomial vector field is *decidable*. The conditions one is required to check are phrased in terms of set inclusion of semi-algebraic sets, which can be determined using a decision procedure for real arithmetic. The result builds on ideas described earlier in (Taly and Tiwari, 2009) and crucially depends on the property of solutions to differential equations with analytic right-hand sides being themselves analytic. In the remainder of this section, we rephrase and provide a detailed illustration of the main components of the result presented in (Liu et al., 2011).

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

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

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 $\epsilon > 0$; case 2 is analogous, but with $h(\mathbf{x}(t)) > 0$ for all $t \in (0, \epsilon)$. In case 3, one is 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

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

and converges on some non-empty open interval of t containing zero. Thus, the most significant term to become sign-definite will determine the sign of the entire sum on some sufficiently small interval. See (Liu et al., 2011, Proof of Proposition 9). See also (Taly and Tiwari, 2009, Proof of Theorem 7), which employed very much the same ideas as (Liu et al., 2011). $\square$

325 The following theorem is a simple corollary to (Liu et al., 2011, Theorem 19).

Theorem 17 (Liu, Zhan & Zhao (Liu et al., 2011)). *Given a polynomial system $\dot{\mathbf{x}} = \mathbf{p}(\mathbf{x})$, and a semi-algebraic set $S \subseteq \mathbb{R}^n$, define*

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

326 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
 327 time t . The set S is positively invariant under the flow of the system if and only
 328 if the inclusions $\text{In}_{(-\mathbf{p})}(S) \subseteq S \subseteq \text{In}_{\mathbf{p}}(S)$ hold, which implies soundness (and
 329 relative completeness) of the following rule of inference:

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

330

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. (Taly and Tiwari, 2009, Theorem 7, Theorem 8)):

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

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 (Liu et al., 2011) 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 (Liu et al., 2011):

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

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:

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

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

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

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

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

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

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

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

339 **Remark 18.** *The ascending chain property is crucial in making it possible to rea-*
 340 *son about sign conditions of infinitely many higher-order Lie derivatives by only*
 341 *considering a finite number of sign conditions. The same idea was independently*
 342 *pursued in (Ghorbal and Platzer, 2014) to give a necessary and sufficient cri-*
 343 *terion for invariance of real algebraic sets under the flow of polynomial ODEs*
 344 *(summarized in the proof rule DRI; discussed earlier).*

345 Thus, by computing N for a given polynomial h and a system $\dot{\mathbf{x}} = \mathbf{p}(\mathbf{x})$,
 346 one may construct a *semi-algebraic* set $\text{In}_{\mathbf{p}}(h \leq 0)$. In Fig. 3d we detail the
 347 computation for $N = 3$ and depict the different “pieces” involved to form $\text{In}_{\mathbf{p}}(h \leq$
 348 $0)$, which is, in this particular case, the same as $h \leq 0$ as shown in Fig. 4b.

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

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

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

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

349 In order to construct $\text{In}_p(\cdot)$ for semi-algebraic sets with boolean structure,
 350 an important distribution property, proved in (Liu et al., 2011, Theorem 20), is
 351 required. For convenience, the property is stated below.

Theorem 19 ((Liu et al., 2011)). *Given a polynomial system $\dot{x} = p(x)$ 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*

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

352

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

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

356 and the solution to $\dot{x} = -p(x)$ is given by $x(-t)$, where $x(t)$ is the solution to
 357 $\dot{x} = p(x)$. Once all the semi-algebraic sets in the premise of LZZ are constructed,
 358 the validity of the premise can be decided using a decision procedure for real
 359 arithmetic (Tarski, 1951).

6. Hierarchy

In this section, we compare the deductive power of the existing (Fig. 1) as well as the newly-introduced proof rules (Lie° and Lie^* in Section 4, and NSSBC in Section 5.2) for checking the invariance of algebraic and semi-algebraic sets. This study should be complemented by another comparison that considers the interaction between the different proof rules in the context of a formal proof system in a similar vein to (Platzer, 2012b). We leave this for future work.

Given two proof rules R_1 and R_2 of the form

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

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

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

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

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

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

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

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

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

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

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

6.1. Proof Rules for Algebraic Sets

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

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

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

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

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

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

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

431 *Proof.* We already established that $\text{Lie} \preceq \text{Lie}^\circ$ (Prop. 8) and $\text{Lie}^\circ \preceq \text{Lie}^*$ (Prop. 7);
 432 we give two counterexamples to establish the strict inclusion. **(I)** $\text{Lie} \not\preceq \text{Lie}^\circ$.
 433 Whenever the variety has a singularity, the proof rule Lie will fail. Lie° is tai-
 434 lored to prove invariance of equilibrium points in addition to regular points of the
 435 variety. For instance, for $\mathbf{p} = ((-1 + x_1)x_2, x_2(1 + x_2))$, Lie fails to prove that
 436 $h = (-1 + x_1)^2 + (1 + x_2)^2 = 0$ is invariant as the gradient ∇h vanishes at $(1, -1)$

	FI	C-c	P-c	Lie	Lie [°]	Lie*	DRI
FI	~	⋈ 21	⋈	⋈ 25	⋈ 28	⋈ 27	⋈
C-c	⋈ 21	~	⋈ 22	⋈ 29	⋈ 30	⋈ 30	⋈
P-c	⋈ 22	⋈	~	⋈ 29	⋈ 30	⋈ 30	⋈ 24
Lie	⋈ 25	⋈ 29	⋈ 29	~	⋈ 23	⋈	⋈
Lie [°]	⋈ 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).

437 and $h((1, -1)) = 0$. However, at $(1, -1)$ we also have $p_1 = p_2 = 0$, and hence
438 the premise of Lie° is satisfied, and $h = 0$ is proved to be an invariant under the
439 flow of $\mathbf{p}$. (II) $\text{Lie}^\circ \not\preceq \text{Lie}^*$. In addition to equilibria, Lie^* goes one step further
440 and handles all singular points, $\mathbf{x}$, where the vector $\mathbf{x} + \lambda \mathbf{p}$ is in the variety $V_{\mathbb{R}}(h)$
441 for all $\lambda \in \mathbb{R}$ (that is $h(\mathbf{x} + \lambda \mathbf{p}) = 0$, for all λ). For instance, consider the poly-
442 nomial $h = x_1 x_2 x_3$, its singular locus is given by the three axes $x_1 = x_2 = 0$,
443 $x_1 = x_3 = 0$ and $x_2 = x_3 = 0$. For the vector field $\mathbf{p} = (x_1, x_2, x_3)$, the equi-
444 librium point is at the origin $(0, 0, 0)$, which obviously does not contain the entire
445 singular locus of h . Thus, Lie° fails but Lie^* succeeds because $h(\mathbf{x} + \lambda \mathbf{p}) = 0$
446 when $\mathbf{x}$ is a point of one of the axes. $\square$

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

448 *Proof.* DRI is both necessary and sufficient (Ghorbal and Platzer, 2014), so we
449 know that $\text{P-c} \preceq \text{DRI}$ and $\text{Lie}^* \preceq \text{DRI}$. To prove the claim it is left to show
450 that (I) $\text{P-c} \not\preceq \text{DRI}$. Consider the following two-dimensional vector field: $\mathbf{p} =$
451 $((-1 + x_1)(1 + x_1), (-1 + x_2)(1 + x_2))$. The candidate invariant (given by the
452 roots of the Motzkin polynomial) $h = 1 - 3x_1^2 x_2^2 + x_1^4 x_2^2 + x_1^2 x_2^4 = 0$ cannot
453 be proved using P-c, as $\mathcal{L}_{\mathbf{p}}(h) \notin \langle h \rangle$. However, the invariance property may be
454 proved using DRI. For this, we need to consider the second-order Lie derivative
455 of h and we prove that $\mathcal{L}_{\mathbf{p}}^{(2)}(h) \in \langle h, \mathcal{L}_{\mathbf{p}}(h) \rangle$. Thus, the premise of DRI holds
456 for $N = 2$. (II) $\text{Lie}^* \not\preceq \text{DRI}$. Consider the following three-dimensional vector

457 field $\mathbf{p} = (-x_2 + x_1(1 - x_1^2 - x_2^2), x_1 + x_2(1 - x_1^2 - x_2^2), x_3)$. We want to prove
 458 that $h = (-1 + x_1^2 + x_2^2)^2 + x_3^2 = 0$ is an invariant. In this case, the variety
 459 $V_{\mathbb{R}}(h)$ is exactly equal to the singular locus of h which is the two-dimensional
 460 unit circle $-1 + x_1^2 + x_2^2 = 0$. However, at all points of this unit circle, the vector
 461 field $\mathbf{p}$ is equal to $(-x_2, x_1, 0) \neq 0$, which prevents us from using Lie* (because
 462 $h((x_1, x_2, 0) + \lambda(-x_2, x_1, 0)) \neq 0$ for some $\lambda \in \mathbb{R}$). The rule DRI proves the
 463 invariance of $h = 0$ with $N = 2$. $\square$

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

Figure 7: Invariant functions and invariant equations.

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

471 *Proof.* (I) $\text{FI} \not\prec \text{Lie}$. For the vector field $\mathbf{p} = (-2x_2, -2x_1 - 3x_1^2)$, the equation
 472 $x_1^2 + x_2^2 - 1 = 0$ is provable with FI but not Lie, see Fig. 7 (left). (II) $\text{FI} \not\prec \text{Lie}$.
 473 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

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

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

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

481 *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
 482 gets by transitivity $R_1 \preceq R_3$, which contradicts the assumption $R_3 \prec \succ R_1$. $\square$

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

484 *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
 485 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
 486 following example proves that $\text{FI} \not\preceq \text{Lie}^*$: Consider the three-dimensional vector
 487 field $\mathbf{p} = (x_2, -x_1, 0)$. The invariance of the equation $x_3^2 + (-1 + x_1^2 + x_2^2 + x_3^2)^2 = 0$
 488 cannot be established using Lie^* (the singular locus is a circle in $\mathbb{R}^3$), but is easily
 489 provable using FI as $\mathfrak{L}_{\mathbf{p}}(h)$ vanishes. $\square$

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

491 *Proof.* By Lem. 26, from $\text{Lie} \preceq \text{Lie}^\circ$ (Prop. 8) and $\text{FI} \prec \succ \text{Lie}$ (Prop. 25), we
 492 get $\text{Lie}^\circ \not\preceq \text{FI}$. On the other hand, if $\text{FI} \preceq \text{Lie}^\circ$ then, by transitivity $\text{FI} \preceq \text{Lie}^*$
 493 (since $\text{Lie}^\circ \preceq \text{Lie}^*$ by Prop. 7), which contradicts $\text{FI} \prec \succ \text{Lie}^*$ (Prop. 27). Thus,
 494 $\text{FI} \not\preceq \text{Lie}^\circ$, and the proposition follows. $\square$

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

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

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

503 The remaining cases follow from the results established above.

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

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

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

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

Remark 31. Provided that the invariant candidate has no singular points, Lie's criterion is known to be both necessary and sufficient to prove invariance properties of level sets (Olver, 2000, Theorem 2.8). Also, FI characterizes invariant functions (Platzer, 2012a) but not all invariant equations. On the other hand, for algebraic differential equations, the differential radical criterion in DRI fully characterizes all invariant algebraic sets (Ghorbal and Platzer, 2014). Thus, as established in Prop. 24, DRI increases the deductive power of both Darboux-based rules $\{\text{FI}, \text{C-c}, \text{P-c}\}$ and Lie-based rules $\{\text{Lie}, \text{Lie}^\circ, \text{Lie}^*\}$, which form different families.

6.2. Proof Rules for Semi-Algebraic Sets

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

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

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

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

522 *Proof.* The Nagumo theorem characterizes closed positively invariant sets under
 523 the flow of locally Lipschitz ODEs. In particular, this covers closed semi-algebraic
 524 sets and polynomial ODE. Hence $\text{NSSBC} \preceq \text{Nagumo}$. To see why the inequality
 525 is strict, consider any vector field with an invariant algebraic set (recall that
 526 algebraic sets are special closed semi-algebraic sets with empty interior). The
 527 proof rule NSSBC cannot work for such invariant sets precisely because it re-
 528 quires $\mathcal{L}_{\mathbf{p}}(h) < 0$ whenever $h = 0$. In fact, $h = 0 \rightarrow \mathcal{L}_{\mathbf{p}}(h) = 0$ is a necessary
 529 condition for any invariant algebraic set. $\square$

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

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

535 **Proposition 34.** $\text{NSSBC} \prec \succ \text{DI}$.

Proof. $\text{DI} \not\preceq \text{NSSBC}$. Consider the system

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

536 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
 537 positively invariant set under the flow of the system (see Fig. 9a). The invariance
 538 property cannot be proved using the rule DI, but is easily proved using NSSBC
 539 (and LZZ).

540 $\text{NSSBC} \not\preceq \text{DI}$. Consider the system $\mathbf{p}(\mathbf{x}) = (x_2^2, 2)$ and let $S_2 \equiv x_2 \geq 0 \wedge$
 541 $x_1 \geq 0$. Positive invariance of S_2 is proved easily using either DI (and LZZ), but
 542 cannot be proved using NSSBC. Intuitively, this can be seen because at the origin
 543 the vector $\mathbf{p}(\mathbf{0})$ does not point strictly into the interior of $S_2 \equiv \max(-x_2, -x_1) \leq$
 544 0 , since $\mathcal{L}_{\mathbf{p}}(-x_1) = -x_2^2|_0 = 0$ (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).

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

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

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

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

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

559 **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)

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

566 **Remark 38.** *The premises of the proof rules for algebraic sets could be used to*
 567 *work with a larger class of invariant sets, namely those of the form $h \geq 0$ in*
 568 *addition to algebraic sets. For instance, if $\mathcal{L}_p(h) \in \langle h \rangle$, then necessarily $h \geq$*
 569 *0 is an invariant of the system. In fact, the invariance of $h = 0$ implies the*
 570 *invariance of $h \bowtie 0$ for $\bowtie \in \{\leq, <, \geq, >\}$. Such extra proof rules do not bring any*
 571 *additional insight to the realm of proof rules depicted in Fig. 5 and are therefore*
 572 *not represented.*

573 7. Square-free Reduction

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

578 7.1. Square-free Reduction with Lie-based Proof Rules

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

582 to prove that $h = x^2 - 6x + 9 = 0$ is invariant, no matter what vector field one
 583 considers. The reason for this is simple: $x^2 - 6x + 9$ factorizes into $(x - 3)^2$. The
 584 problem here lies in the polynomial h itself, rather than the real variety $V_{\mathbb{R}}(h)$. In
 585 fact, $V_{\mathbb{R}}(h)$ is exactly the singular locus of h and the proof rule Lie fails because
 586 *all* points inside $V_{\mathbb{R}}(h)$ are singular points. More generally, the chain rule implies
 587 $\nabla h^k \cdot \mathbf{p} = kh^{k-1} \nabla h \cdot \mathbf{p}$, which has the consequence that any polynomial h which
 588 is not square-free will have vanishing gradient at the real roots of factors with
 589 multiplicity greater than 1.

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

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

593 Intuitively, in performing square-free reduction we hope to shrink the singular
 594 locus of the original polynomial. If $\text{SL}(\text{SF}(h))$ is the empty set (which is the case
 595 for $h = x^2 - 6x + 9$ in the example given above), the proof rule Lie applies to
 596 $\text{SF}(h)$ but not to h . In general, $\text{SF}(h)$ may satisfy the assumptions of the proof
 597 rules Lie° or Lie^* , where h fails to do so. It is always sound to conclude that $h = 0$
 598 is invariant from the knowledge that $\text{SF}(h) = 0$ is invariant, since real varieties
 599 remain unaltered under square-free reduction of their defining polynomials (Cox
 600 et al., 1997), i.e. $V_{\mathbb{R}}(h) \equiv V_{\mathbb{R}}(\text{SF}(h))$. Thus, replacing h with $\text{SF}(h)$ in the
 601 premise of Lie, Lie° and Lie^* does not compromise soundness (it is a use of the
 602 generalization proof rule (Platzer, 2008)) and enlarges the class of polynomials
 603 that these proof rules can work with.

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

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

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

615 7.2. Square-free Reduction with Darboux-based proof rules

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

620 **Proposition 40.** $\text{FI} \prec \succ \text{SFFI}$.

621 *Proof.* (I) $\text{FI} \not\prec \text{SFFI}$. The polynomial $h = x^2y$ is an invariant function for
622 the vector field $\mathbf{p} = (\frac{\partial h}{\partial y}, -\frac{\partial h}{\partial x}) = (x^2, -2xy)$, thus FI proves the invariance of
623 $h = 0$. However, $\text{SF}(h)$ is not an invariant function for the same vector field, since
624 $\mathcal{L}_{\mathbf{p}}(\text{SF}(h)) = \mathcal{L}_{\mathbf{p}}(xy) = -x^2y \neq 0$, thus SFFI fails to prove the invariance of
625 $h = 0$. (II) $\text{SFFI} \not\prec \text{FI}$. Similarly, the polynomial $h = xy$ is an invariant function
626 for the vector field $\mathbf{p} = (\frac{\partial h}{\partial y}, -\frac{\partial h}{\partial x}) = (x, -y)$, thus SFFI proves the invariance
627 of $x^2y = 0$, since $\text{SF}(x^2y) = h$. However, FI fails to prove the invariance of
628 $x^2y = 0$, because $\mathcal{L}_{\mathbf{p}}(x^2y) = x^2y \neq 0$. $\square$

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

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

636 **Proposition 41.** $\text{C-c} \prec \succ \text{SFC-c}$.

637 *Proof.* (I) $\text{C-c} \not\prec \text{SFC-c}$. The proof rule C-c proves the invariance of $h = x^2y =$
638 0 for the vector field $\mathbf{p} = (x^2, y(1 - 2x))$ as $\mathcal{L}_{\mathbf{p}}(h) = 1h$. However, C-c cannot
639 prove $\text{SF}(h) = 0$, since $\mathcal{L}_{\mathbf{p}}(\text{SF}(h)) = \mathcal{L}_{\mathbf{p}}(xy) = (1 - x)\text{SF}(h)$. (II) $\text{SFC-c} \not\prec$
640 C-c . For the same h , C-c proves the invariance of $\text{SF}(h) = 0$ for the vector field
641 $\mathbf{p} = (x^2, y(1 - x))$ as $\mathcal{L}_{\mathbf{p}}(\text{SF}(h)) = \mathcal{L}_{\mathbf{p}}(xy) = 1\text{SF}(h)$. However, without the SF
642 reduction C-c alone fails to prove the invariance of $h = 0$ for the considered $\mathbf{p}$, as
643 $\mathcal{L}_{\mathbf{p}}(h) = (x + 1)h$. $\square$

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

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

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

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

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

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

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

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

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

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 that $\text{SF}(h) = q_1 \cdots q_r$. Using Eq. (16), one gets

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

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

Proposition 43. $\text{P-c} \sim \text{SFP-c}$.

⁵See (Dumortier et al., 2006, Proposition 8.4) for a similar proposition over the complex numbers.

662 *Proof.* The proof rule P-c proves the invariance of $h = 0$ for $\mathbf{p}$ if and only if
 663 the polynomial h is Darboux. However, by Prop. 42, h is Darboux if and only if
 664 $\text{SF}(h)$ is also Darboux. Therefore, SFP-c could be used equivalently to prove the
 665 invariance of $h = 0$. $\square$

666 **Remark 44.** *The condition $\mathfrak{L}_{\mathbf{p}}(h) \in \langle \text{SF}(h) \rangle$ —which is weaker than $\mathfrak{L}_{\mathbf{p}}(h) \in$
 667 $\langle h \rangle$ —is not sufficient to prove the invariance of $h = 0$. It is therefore an unsound
 668 proof rule. Consider the polynomial $h = (-1 + x^2)^2$ and the 1-dimensional
 669 vector field $\dot{x} = x$. Although $\mathfrak{L}_{\mathbf{p}}(h) = 4(-1 + x^2)x^2 \in \langle -1 + x^2 \rangle = \langle \text{SF}(h) \rangle$,
 670 the equation $h = 0$ is not invariant, however, because $x(t) = \pm e^t$. Notice that
 671 the proof rule P-c (with or without the square-free reduction) is unable to prove
 672 or disprove the invariance of $h = 0$.*

673 7.3. Square-free Reduction On Differential Radical Invariants (DRI)

674 Square-free reduction cannot increase the deductive power of the proof rule
 675 DRI because its premise is necessary and sufficient to prove invariance of real
 676 algebraic sets, which is unaffected by applying SF reduction. However, the com-
 677 putational impact of using square-free reduction with DRI remains an interesting
 678 question. Empirically, we observed a better performance of DRI when the SF
 679 reduction is applied first. In addition to lowering the degrees of the involved poly-
 680 nomials (as it did for Lie-based proof rules), we observed that the order N_{SF} for
 681 $\text{SF}(h)$ is always lower than the order N for h . We, therefore, conjecture $N_{\text{SF}} \leq N$.
 682 However, we identified an example (cf. Ex. 45 below) for which square-free re-
 683 duction resulted in a significant ($\times 100$) computational overhead due to the ideal
 684 membership checking (which we perform using Gröbner bases with reverse lex-
 685 icographic monomial ordering). In our implementation of DRI, called DRI_{opt} in
 686 the sequel, we use the square-free reduction only as a pre-processing step for the
 687 quantifier elimination problems in the premise of DRI.

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

$$\begin{aligned}
\dot{x}_1 &= -24(x_1 + x_3)(x_3^6 - 3x_1^2x_2^2x_3^2 + x_1^2x_2^4 + x_1^4x_2^2)x_4x_5(x_7^2 + x_2 - 12341)^{16}(x_4x_5^2 - 12x_6x_8)^{11}, \\
\dot{x}_2 &= 144(x_1 + x_3)(x_3^6 - 3x_1^2x_2^2x_3^2 + x_1^2x_2^4 + x_1^4x_2^2)(x_7^2 + x_2 - 12341)^{16}x_8(x_4x_5^2 - 12x_6x_8)^{11}, \\
\dot{x}_3 &= -32(x_1 + x_3)(x_3^6 - 3x_1^2x_2^2x_3^2 + x_1^2x_2^4 + x_1^4x_2^2)x_7(x_7^2 + x_2 - 12341)^{15}(x_4x_5^2 - 12x_6x_8)^{12}, \\
\dot{x}_4 &= 144(x_1 + x_3)(x_3^6 - 3x_1^2x_2^2x_3^2 + x_1^2x_2^4 + x_1^4x_2^2)x_6(x_7^2 + x_2 - 12341)^{16}(x_4x_5^2 - 12x_6x_8)^{11}, \\
\dot{x}_5 &= (x_1 + x_3)(2x_1x_2^4 + 4x_1^3x_2^2 - 6x_1x_3^2x_2^2)(x_4x_5^2 - 12x_6x_8)^{12}(x_7^2 + x_2 - 12341)^{16} \\
&\quad + (x_3^6 - 3x_1^2x_2^2x_3^2 + x_1^2x_2^4 + x_1^4x_2^2)(x_4x_5^2 - 12x_6x_8)^{12}(x_7^2 + x_2 - 12341)^{16}, \\
\dot{x}_6 &= (x_1 + x_3)(2x_2x_1^4 + 4x_2^3x_1^2 - 6x_2x_3^2x_1^2)(x_4x_5^2 - 12x_6x_8)^{12}(x_7^2 + x_2 - 12341)^{16} \\
&\quad + 16(x_1 + x_3)(x_3^6 - 3x_1^2x_2^2x_3^2 + x_1^2x_2^4 + x_1^4x_2^2)(x_4x_5^2 - 12x_6x_8)^{12}(x_7^2 + x_2 - 12341)^{15}, \\
\dot{x}_7 &= (x_1 + x_3)(6x_3^5 - 6x_1^2x_2^2x_3)(x_4x_5^2 - 12x_6x_8)^{12}(x_7^2 + x_2 - 12341)^{16} \\
&\quad + (x_3^6 - 3x_1^2x_2^2x_3^2 + x_1^2x_2^4 + x_1^4x_2^2)(x_4x_5^2 - 12x_6x_8)^{12}(x_7^2 + x_2 - 12341)^{16}, \\
\dot{x}_8 &= 12(x_1 + x_3)(x_3^6 - 3x_1^2x_2^2x_3^2 + x_1^2x_2^4 + x_1^4x_2^2)x_5^2(x_7^2 + x_2 - 12341)^{16}(x_4x_5^2 - 12x_6x_8)^{11},
\end{aligned}$$

and let

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

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

698 **Remark 46.** Notice that Prop. 42 does not have an analogue for DRI. In other
699 words, if a polynomial equation $h = 0$ is invariant for $\mathbf{p}$, its irreducible factors
700 need not define invariant equations themselves. Geometrically, this means that if
701 a variety is invariant under the flow of $\mathbf{p}$, its irreducible components need not be
702 invariants under the flow of $\mathbf{p}$. For instance, consider the irreducible polynomials
703 $q_1 = y - 1$ and $q_2 = x^2 + (y - 1)^2$. The equation $q_1q_2 = 0$ which is equivalent
704 to $y = 1$, is invariant for $\mathbf{p} = (1, 0)$, since the premise of the proof rule DRI
705 holds true for $N = 3$. However, the equation $q_2 = 0$, which is equivalent to
706 $x = 0 \wedge y = 1$, is not an invariant equation for $\mathbf{p}$. The reason for the invariance
707 of $q_1q_2 = 0$, which is equivalent to $q_1 = 0 \vee q_2 = 0$, stems from q_1 not from q_2 .

708 **7.4. Order parity decomposition**

709 Similar to square-free reduction for invariant polynomial equations, one may
 710 sometimes remove roots of multiplicities greater than 1 from polynomial inequalities $p \leq 0$, thereby simplifying their description and removing singularities on
 711 their boundary. To do this, we will require some definitions, due to Dolzmann and
 712 Sturm (see (Dolzmann and Sturm, 1995)).
 713

Definition 47 (Square-free decomposition (Dolzmann and Sturm, 1995)). *Given a polynomial $h \in \mathbb{Z}[x_1, \dots, x_n]$, the square-free decomposition is given by*

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

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

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

Definition 48 (Parity decomposition (Dolzmann and Sturm, 1995)). *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*

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

721 **Proposition 49** (Square-free equivalent (Dolzmann and Sturm, 1995)). *Let $h \in$
 722 $\mathbb{Z}[x_1, \dots, x_n]$ and let (h_o, h_e) be the parity decomposition of h . Then the following
 723 equivalences hold:*

- 724 1. $h = 0 \equiv_{\mathbb{R}} \text{SF}(h) = 0$,
- 725 2. $h \neq 0 \equiv_{\mathbb{R}} \text{SF}(h) \neq 0$,
- 726 3. $h > 0 \equiv_{\mathbb{R}} h_o h_e^2 > 0 \equiv_{\mathbb{R}} h_o > 0 \wedge h_e \neq 0$,
- 727 4. $h \geq 0 \equiv_{\mathbb{R}} h_o h_e^2 \geq 0 \equiv_{\mathbb{R}} h_o \geq 0 \vee h_e = 0$,
- 728 5. $h < 0 \equiv_{\mathbb{R}} h_o h_e^2 < 0 \equiv_{\mathbb{R}} h_o < 0 \wedge h_e \neq 0$,
- 729 6. $h \leq 0 \equiv_{\mathbb{R}} h_o h_e^2 \leq 0 \equiv_{\mathbb{R}} h_o \leq 0 \vee h_e = 0$.

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

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

737 **Theorem 50.** $\text{SFEQ NSSBC} \succ \text{NSSBC}$.

738 *Proof.* If $\mathcal{L}_p(h) < 0$ is true when h is an active component ($h = 0$), it is nec-
 739 essarily the case that h is square-free. Thus $\text{SFEQ}(h) = h$ (which then equals
 740 $\text{SF}(h)$) and, therefore, $\text{SFEQ NSSBC} \succ \text{NSSBC}$. Let $\dot{\mathbf{x}} = \mathbf{p}(\mathbf{x}) = (-x_1, -x_2)$
 741 and consider the set $S \equiv (x_1^2 + x_2^2 - 1)^3 \leq 0$. Applying NSSBC fails to prove the
 742 positive invariance property. Computing the order parity decomposition, we get
 743 $\text{SFEQ}(S) \leq 0 \equiv (x_1^2 + x_2^2 - 1) \leq 0$, for which positive invariance under the flow
 744 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:

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

745 *This is an example of a positively invariant set described by a non-strict poly-*
 746 *nomial inequality where applying NSSBC will fail. In fact, the barrier certificate*

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

747 approach (Prajna et al., 2007) breaks down completely, i.e. no barrier certificate
 748 exists for showing positive invariance of this set.

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

755 By performing the above steps one proves that both disjuncts are positively
 756 invariant under the flow, and hence their disjunction is also positively invariant,
 757 concluding the proof that $h \leq 0$ describes a positively invariant set. A formal
 758 proof of this property within a proof calculus needs an inference rule such as
 759 NSSBC, some appropriate rule for equational invariants, such as e.g. Lie, P-c
 760 or DRI, as well as the following special case of the generalization rule (Platzer,
 761 2008):

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

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

763 *Proof.* Corollary to Proposition 40, since FI is a special case of DI and $\text{SFEQ}[h =$
 764 $0] \equiv \text{SF}(h) = 0$. $\square$

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

766 *Proof.* Nagumo is necessary and sufficient for proving positive invariance of
767 closed sets and SFEQ returns a description of an equivalent set (over the reals).
768 Thus, a closed set S is positively invariant using Nagumo if and only if an equiv-
769 alent closed set $\text{SFEQ}[S]$ is positively invariant using Nagumo. $\square$

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

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

773 8. Experimental Comparison

774 To complement the theoretical deductive power comparison with a practical
775 provability study, we empirically compare the running time performance of all the
776 proof rules discussed in this paper on a heterogeneous collection of benchmarks
777 (76 for algebraic sets and 20 for semi-algebraic sets).

778 Many premises of the considered proof rules are universally quantified sen-
779 tences over the theory of real arithmetic. The purely existential fragment of real
780 quantifier elimination has been shown to exhibit singly exponential time com-
781 plexity in the number of variables (Basu et al., 1996). However, in practice this
782 has not yet led to an efficient decision procedure, so typically it is much more
783 efficient to use CAD (Collins, 1975; Collins and Hong, 1991), which has doubly-
784 exponential running time in the number of variables. Theoretically, the upper
785 bound on the complexity of deciding a sentence in the universal theory of $\mathbb{R}$ is
786 given by $(sd)^{O(n)}$, where s is the number of polynomials in the formula, d their
787 maximum degree and n the number of variables (Basu et al., 1996).

788 Notice, in addition, that the proof rules, C-c, P-c, DRI and LZZ involve rea-
789 soning about multivariate polynomial ideal membership, which is an EXPSPACE-
790 complete problem over $\mathbb{Q}$ (Mayr, 1989). Gröbner basis algorithms allow us to
791 perform membership checks in ideals generated by multivariate polynomials. Sig-
792 nificant advances have been made in algorithms for computing Gröbner bases
793 (Faugère, 2002) which in practice can be expected to perform very well. Our ex-
794 perimentation relies on the implementation of the CAD algorithm in Mathematica
795 (version 10.0.1).

796 The examples we used originate from a number of sources—many come from
797 textbooks on Dynamical Systems; some from the literature on formal verification

798 of hybrid systems; others have been hand-crafted to tease out sweetspots of cer-
799 tain proof rules. The most interesting experimental question we seek to address
800 here is whether the greater generality of the more deductively powerful proof rules
801 also comes at a substantially higher computational cost when assessed across the
802 entire spectrum of examples. As a complement to the theoretical deductive power
803 relationships between the different proof rules (Section 6), we also seek to iden-
804 tify some nuances in the complexity of the conditions in the premises, which the
805 coarse-grained complexity bounds miss, being highly sensitive to the number of
806 variables.

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

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

818 8.1. Running Time Performance for Algebraic Sets

819 In this section, the prefix SF is implicit for all Lie-based proof rules. We con-
820 sider 4 equally sized classes of invariant sets: (1) 24 smooth invariants, where
821 Lie is both necessary and sufficient, (2) 17 isolated equilibria as trivial (for hu-
822 mans, not machines) equational invariants for which both Lie° and Lie^* provide
823 necessary and sufficient conditions, (3) 17 other singularities and high integrals,
824 (4) 18 functional invariants, where FI is necessary and sufficient. Figure 12 com-
825 pares the number of invariant varieties that each rule could prove within 60 sec-
826 onds. The vertical axis shows cumulative time spent on the problems. All runs
827 were performed on an Intel Core i5 1.7GHz machine with 4Gb RAM. Gener-
828 ally, we observe DRI performing very well across the entire spectrum of problem
829 classes. This is very encouraging, but also at first sight appears to defy intuition
830 since it implies that one does not necessarily sacrifice performance when opting

⁶We refer the reader to (Ghorbal et al., 2014) for a more detailed discussion of the differences and similarities between the Liu, Zhan & Zhao characterization (Liu et al., 2011) and the differential radical characterization (Ghorbal and Platzer, 2014).

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

831 to use a more deductively powerful rule. In this graph, we also see that over-
832 all Lie° appears to offer an interesting compromise between deductive power and
833 efficiency—it is able to prove a significant body of problems that are out of scope
834 for Lie , while avoiding the complexity penalty which affects Lie^* (due to intro-
835 ducing an extra variable).

836 A more careful analysis of the benchmarks reveals interesting relationships
837 that are obscured in the “big picture”; to see them, one needs to consider the
838 individual classes of invariants for which some of the sufficient conditions in the
839 rules are in fact *necessary and sufficient*. Together with DRI, this yields two
840 *decision procedures* for each class and allows us to focus only on running time
841 performance and assess the practicality of each proof rule. In Fig. 13, we observe
842 the rules Lie° and Lie^* performing very well in proving invariance of isolated
843 equilibria. This is to be expected as Lie° in particular was formulated with this
844 problem class in mind. It is interesting that DRI remains highly competitive here;
845 though its performance is slightly worse in our set of benchmarks.

846 It is clear that because proof rules Lie° and Lie^* generalize Lie , they will be
847 able to prove every problem in the smooth invariant benchmarks. The running
848 time performance of the three rules is almost identical, with Lie offering a slight
849 speed-up over its generalizations. The premises of Lie° and Lie^* impose condi-

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

850 tions on states in the singular locus, which is the empty set for smooth invariants;
851 this, in practice, appears to be slightly more expensive than checking an equiva-
852 lent property that the gradient is non-vanishing on the variety (as in the premise
853 of Lie).

854 The proof rules FI and P-c, corresponding to conditions with historical ori-
855 gins in the study of integrability of dynamical systems, can be seen to perform
856 very well in proving functional invariants, while performing very poorly in bench-
857 marks for isolated equilibria. In proofs of smooth invariants their behaviour is
858 radically different, with FI proving only a handful of examples and P-c succeed-
859 ing in proving most of the problems very efficiently. This can be explained by the
860 fact that P-c generalizes FI and is therefore more deductively powerful. P-c ap-
861 pears slightly slower at proving functional invariants, but shows very impressive
862 running time performance for some problems from the smooth invariant bench-

marks, where it is the fastest proof rule for many of problems where it succeeds. Comparing running time performance with DRI, we see that DRI is only slightly slower at proving functional invariants than FI and P-c. Again, the performance gap between DRI and the two rules appears to be insignificant for most problems. Theoretically, when P-c proves an invariant, DRI applies conditions that are identical to the premise of P-c. Hence, although DRI is a generalization, this does not come at a significant extra cost for the classes where P-c shows good running time performance. The slightly greater running time of DRI compared to that of P-c can be accounted for by the fact that in our implementation DRI computes the Gröbner basis for *every* order N including for $N = 1$ where such computation is unnecessary.

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

In the examples featuring singularities and high integrals in the benchmarks we see DRI as the clear winner, simply because there was no other rule that was tailored to work on this class. Indeed, the structure of these invariant sets can be rather involved, making it difficult to characterize in a single proof rule; however, sometimes it is possible to exploit the structure of high integrals inside a proof system and arrive at efficient proofs that outperform DRI (Ghorbal et al., 2014).

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

8.2. Running Time Performance for Semi-algebraic Sets

In Fig. 14 we compare the running time performance of the proof rule LZZ versus the sufficient conditions DI (Fig. 14a) and NSSBC (Fig. 14b). Two different sets of 10 benchmarks each were selected to exploit the sweetspots of DI

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

and NSSBC respectively. We observe that whenever DI can prove invariance in the problem at hand, it is much faster than LZZ. This is expected: the quantifier elimination problems required by the proof rule LZZ are much more involved than those found in the premise of DI. This should be balanced by the fact that DI is more restrictive. In the set of benchmarks for NSSBC, one can observe that DI does not prove any of the problems. In Fig. 14b, one can also notice that LZZ still performs well compared to NSSBC. Indeed, the premise of the proof rule NSSBC can involve complicated real arithmetic problems that are sometimes even more difficult than those appearing in the premise of the proof rule LZZ. Generally, the size of the conditions in the premise of NSSBC grows rapidly with the size of the formula describing the invariant candidate. The distribution property in Theorem 19 avoids this problem in LZZ.

9. Conclusion

This article investigated an important aspect of deductive safety verification of continuous and hybrid dynamical systems. Namely, given the abundance of existing sufficient conditions for invariant checking and the recently developed *necessary and sufficient* conditions for real algebraic (Ghorbal and Platzer, 2014) and semi-algebraic (Liu et al., 2011) invariants, it is crucial to know whether the gains in deductive power come at the price of greater computational complexity and poor running time performance that would hinder practical applications. The work presented in this article leads us to arrive at the following conclusions:

- Empirically, we observe that the deductively powerful rule for algebraic invariants (DRI) performs very well in checking invariance of polynomial

923 equalities.

- 924 • P-c is made redundant by DRI (DRI strictly increases the deductive power
925 of P-c while being equally efficient).
- 926 • Reducing polynomials to square-free form is always beneficial to the proof
927 rule Lie and its generalizations, where it yields improvements in both the
928 deductive power and the running time performance.
- 929 • Using the square-free reduction with the proof rules FI and C-c yields new
930 *incomparable* proof rules, whereas SF with P-c is as powerful as P-c alone.
- 931 • Performing square-free reduction of an invariant candidate may introduce
932 a performance penalty for DRI and therefore cannot be regarded as an op-
933 timization, even though there are instances for which it yields a speed-up.
934 The same can be said of order parity decomposition applied to an invariant
935 candidate supplied to LZZ.
- 936 • Sufficient rules DI and NSSBC can afford a speed-up on certain problems,
937 but the overall running time performance of the decision procedure LZZ is
938 observed to be good.
- 939 • Using a decision procedure LZZ appears to be more efficient than using the
940 sufficient condition NSSBC when the positively invariant candidate set is
941 described by a large formula.

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

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

951 Basu, S., Pollack, R., Roy, M.-F., 1996. On the combinatorial and algebraic com-
952 plexity of quantifier elimination. J. ACM 43 (6), 1002–1045.

953 Blanchini, F., Miani, S., 2008. Set-Theoretic Methods in Control. Systems & Con-
954 trol : Foundations & Applications. Birkhäuser.

- 955 Collins, G. E., 1975. Hauptvortrag: Quantifier elimination for real closed fields
956 by cylindrical algebraic decomposition. In: Automata Theory and Formal Lan-
957 guages. Vol. 33 of LNCS. Springer, pp. 134–183.
- 958 Collins, G. E., Hong, H., Sep. 1991. Partial cylindrical algebraic decomposition
959 for quantifier elimination. *J. Symb. Comput.* 12 (3), 299–328.
- 960 Cox, D. A., Little, J., O’Shea, D., 1997. Ideals, Varieties, and Algorithms - an
961 introduction to computational algebraic geometry and commutative algebra (2.
962 ed.). Springer.
- 963 Darboux, J.-G., 1878. Mémoire sur les équations différentielles algébriques du
964 premier ordre et du premier degré. *Bulletin des Sciences Mathématiques et As-
965 tronomiques* 2 (1), 151–200.
966 URL <http://eudml.org/doc/84988>
- 967 Dolzmann, A., Sturm, T., 1995. Simplification of quantifier-free formulas over
968 ordered fields. *Journal of Symbolic Computation* 24, 209–231.
- 969 Dumortier, F., Llibre, J., Artés, J. C., 2006. Qualitative Theory of Planar Differ-
970 ential Systems. Springer.
- 971 Faugère, J. C., 2002. A new efficient algorithm for computing Gröbner bases with-
972 out reduction to zero (F5). In: ISSAC. ACM, New York, NY, USA, pp. 75–83.
- 973 Ghorbal, K., Platzer, A., 2014. Characterizing algebraic invariants by differential
974 radical invariants. In: TACAS. Vol. 8413. Springer, pp. 279–294.
- 975 Ghorbal, K., Sogokon, A., Platzer, A., 2014. Invariance of conjunctions of poly-
976 nomial equalities for algebraic differential equations. In: SAS. Vol. 8723 of
977 LNCS. Springer, pp. 151–167.
- 978 Ghorbal, K., Sogokon, A., Platzer, A., 2015. A hierarchy of proof rules for check-
979 ing differential invariance of algebraic sets. In: VMCAI. Vol. 8931 of LNCS.
980 Springer, pp. 431–448.
- 981 Goriely, A., 2001. Integrability and Nonintegrability of Dynamical Systems. Ad-
982 vanced series in nonlinear dynamics. World Scientific.
- 983 Lie, S., 1893. Vorlesungen über continuierliche Gruppen mit Geometrischen und
984 anderen Anwendungen. Teubner, Leipzig.

- 985 Lindelöf, E., 1894. Sur l'application de la méthode des approximations succes-
 986 sives aux équations différentielles ordinaires du premier ordre. Comptes rendus
 987 hebdomadaires des séances de l'Académie des sciences 116, 454–458.
- 988 Liu, J., Zhan, N., Zhao, H., 2011. Computing semi-algebraic invariants for poly-
 989 nomial dynamical systems. In: EMSOFT. ACM, pp. 97–106.
- 990 Matringe, N., Moura, A. V., Rebiha, R., 2010. Generating invariants for non-
 991 linear hybrid systems by linear algebraic methods. In: SAS. Vol. 6337 of LNCS.
 992 Springer, pp. 373–389.
- 993 Mayr, E. W., 1989. Membership in polynomial ideals over $\mathbb{Q}$ is exponential space
 994 complete. In: Monien, B., Cori, R. (Eds.), STACS. Vol. 349 of LNCS. Springer,
 995 pp. 400–406.
- 996 Nagumo, M., May 1942. Über die Lage der Integralkurven gewöhnlicher Differ-
 997 entialgleichungen (in German). In: Proceedings of the Physico-Mathematical
 998 Society of Japan. Vol. 24. pp. 551–559.
- 999 Olver, P. J., 2000. Applications of Lie Groups to Differential Equations. Springer.
- 1000 Platzer, A., 2008. Differential dynamic logic for hybrid systems. J. Autom. Rea-
 1001 soning 41 (2), 143–189.
- 1002 Platzer, A., 2010. Differential-algebraic dynamic logic for differential-algebraic
 1003 programs. J. Log. Comput. 20 (1), 309–352.
- 1004 Platzer, A., 2012a. A differential operator approach to equational differential in-
 1005 variants - (invited paper). In: ITP. Vol. 7406 of LNCS. Springer, pp. 28–48.
- 1006 Platzer, A., 2012b. The structure of differential invariants and differential cut elim-
 1007 ination. Logical Methods in Computer Science 8 (4), 1–38.
- 1008 Prajna, S., Jadbabaie, A., 2004. Safety verification of hybrid systems using barrier
 1009 certificates. In: In Hybrid Systems: Computation and Control. Springer, pp.
 1010 477–492.
- 1011 Prajna, S., Jadbabaie, A., Pappas, G., 2007. A framework for worst-case and
 1012 stochastic safety verification using barrier certificates. Automatic Control, IEEE
 1013 Transactions on 52 (8), 1415–1428.

- 1014 Richardson, D., 1968. Some undecidable problems involving elementary func-
1015 tions of a real variable. *Journal of Symbolic Logic* 33 (4), 514–520.
- 1016 Sankaranarayanan, S., Sipma, H. B., Manna, Z., 2008. Constructing invariants for
1017 hybrid systems. *Form. Methods Syst. Des.* 32 (1), 25–55.
- 1018 Taly, A., Tiwari, A., 2009. Deductive verification of continuous dynamical sys-
1019 tems. In: *FSTTCS*. Vol. 4 of *LIPIcs*. pp. 383–394.
- 1020 Tarski, A., 1951. A decision method for elementary algebra and geometry. *Bull.*
1021 *Amer. Math. Soc.* 59.
- 1022 Tiwari, A., 2008. Abstractions for hybrid systems. *Form. Methods Syst. Des.*
1023 32 (1), 57–83.
- 1024 Walter, W., 1998. *Ordinary Differential Equations*. Springer New York.
- 1025 Wu, Z., 2010. Tangent cone and contingent cone to the intersection of two closed
1026 sets. *Nonlinear Analysis: Theory, Methods & Applications* 73 (5), 1203 –
1027 1220.