Journal of Symbolic Computation 113 (2022) 1–28

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Characterizing positively invariant sets: Inductive and topological methods

Khalil Ghorbal[a], Andrew Sogokon[b]

[a] Inria, France
[b] SCC, Lancaster University, UK

ARTICLE INFO

Article history:
Available online 31 January 2022

Keywords:
Ordinary differential equations
Dynamical systems
Positively invariant sets
Polynomial vector fields
Decision procedures

ABSTRACT

We present two characterizations of positive invariance of sets under the flow of systems of ordinary differential equations. The first characterization uses *inward sets* which intuitively collect those points from which the flow evolves within the set for a short period of time, whereas the second characterization uses the notion of *exit sets*, which intuitively collect those points from which the flow immediately leaves the set. Our proofs emphasize the use of the *real induction* principle as a generic and unifying proof technique that captures the essence of the formal reasoning justifying our results and provides cleaner alternative proofs of known results. The two characterizations presented in this article, while essentially equivalent, lead to two rather different decision procedures (termed respectively **LZZ** and **ESE**) for checking whether a given semi-algebraic set is positively invariant under the flow of a system of polynomial ordinary differential equations. The procedure **LZZ** improves upon the original work by Liu, Zhan and Zhao (Liu et al., 2011). The procedure **ESE**, introduced in this article, works by splitting the problem, in a principled way, into simpler sub-problems that are easier to check, and is shown to exhibit substantially better performance compared to **LZZ** on problems featuring semi-algebraic sets described by formulas with non-trivial Boolean structure.

E-mail addresses: khalil.ghorbal@inria.fr (K. Ghorbal), a.sogokon@lancaster.ac.uk (A. Sogokon).

https://doi.org/10.1016/j.jsc.2022.01.004
0747-7171/© 2022 Elsevier Ltd. All rights reserved.

1. Introduction

Positive invariance is an important concept in the theory of dynamical systems and one which also has practical applications in areas of computer science, such as formal verification, as well as in control theory. Informally, a set is *positively invariant* if it is preserved under the evolution of the system according to the dynamics as time advances. A considerable amount of literature is dedicated to this subject (Blanchini, 1999), and great progress has been made in understanding positively invariant sets in continuous dynamical systems.

In computer science, the notion of an *inductive invariant* is analogous to that of a positively invariant set. It has relatively recently become the focus of considerable research interest, especially in the area of so-called *hybrid systems*, which studies systems that combine discrete and continuous dynamics. Significant progress has been made over the past decade in the methods for algorithmically checking inductive invariants of ODEs (i.e. deciding whether a given set is positively invariant); these methods provide powerful tools for reasoning about the temporal behaviour of ODEs without the need to explicitly solve them. For example, one may use an inductive invariant to *prove* that a system cannot evolve from a given set of initial conditions into a state which is deemed undesirable or unsafe (e.g. if the ODEs describe the motion of physical objects, one may wish to know that there can be no collisions between these objects in the future).

Contributions. This article presents a self-contained development of two characterizations of positively invariant sets of continuous systems (in Theorem 6 and Theorem 23). In the case of semi-algebraic sets and polynomial ODEs, the two characterizations lend themselves to two alternative decision procedures for checking set positive invariance, both of which are described in detail.

Section 3 is entirely devoted to the first characterization (Theorem 6), which relies on the concept of *inward sets* (see Zhan et al., 2017, Def. 9.4) and is very closely related to a theorem (Zhan et al., 2017, Thm. 9.1) which originally appeared in (Liu et al., 2011); we show how *real induction*, via equivalent, yet subtly different formulations, can be used to give clean proofs of this known result and of Theorem 6. The section then describes a robust implementation of the associated decision procedure (**LZZ**, after Liu, Zhan and Zhao), along with our improvements to the original method.

Section 4 presents the second characterization (Theorem 23), which is based on Conley's notion of *exit sets* (Conley, 1978). We give a direct proof for this new result while formally establishing the relationship between exit sets and inward sets. Section 4.3 presents a new algorithm (**ESE**, which stands for *Exit Set Emptiness*) that can more efficiently decide positive invariance of semi-algebraic sets described by formulas with non-trivial Boolean structure. The procedure works by splitting the problem into simpler sub-problems that are easier to check, reminiscent of divide-and-conquer algorithms.

Our implementations of the two decision procedures **LZZ** and **ESE** are empirically evaluated on a number of positive invariance checking problems where semi-algebraic sets are described by non-atomic formulas in Section 5, with **ESE** exhibiting substantially better performance.

2. Preliminaries

A system of autonomous ordinary differential equations (ODEs) has the form:

$$\left\{\begin{aligned} x_1' &= f_1(x_1, \ldots, x_n)\,, \\ &\vdots \\ x_n' &= f_n(x_1, \ldots, x_n)\,, \end{aligned}\right.$$

where x_i' stands for the time derivative $\frac{dx_i}{dt}$ and $f = (f_1, f_2, \ldots, f_n)$ is a vector-valued continuous function (which defines a *vector field* on $\mathbb{R}^n$); we will write such a system more concisely as $x' = f(x)$. We will denote by $\varphi(\cdot, x)$ the solution to the initial value problem $x' = f(x)$, with initial value $x \in \mathbb{R}^n$. We will only consider systems in which solutions to initial value problems always exist (at least locally) and are unique (e.g. local Lipschitz continuity of f is sufficient to guarantee this property).

When we quantify solutions over time t, we only consider t in the *maximal interval of existence* I_x, which in our case exists for any x and contains 0. In order to simplify our presentation, we will quantify over "all forward time" by writing $\forall\, t \geq 0$ with the understanding that $\varphi(\cdot, x)$ may only be defined for $t \in I_x$. We refer to the mapping φ as the (local) *flow* of the vector field f.

Definition 1 *(Positively invariant set).* Given a system of ODEs $x' = f(x)$, a set $S \subseteq \mathbb{R}^n$ is *positively invariant* if and only if no solution starting inside S can leave S in the future, i.e. just when the following holds:

$$\forall\, x \in S.\, \forall\, t \geq 0.\, \varphi(t, x) \in S\,.$$

One analogously arrives at a definition of *negatively invariant sets* in which no solution starting inside the set S is permitted to be outside the set in the *past*. Basic results in the theory of dynamical systems establish that a set S is positively invariant precisely when its complement S^c is negatively invariant (Bhatia and Szegő, 1970, Thm. 1.4), and that the closure of a positively invariant set is also positively invariant (Alongi and Nelson, 2007, Prop. 1.4.5); this property also holds for the set's interior (Bhatia and Szegő, 1970, Thm. 1.7).

Remark 2. Some authors (Blanchini and Miani, 2008) favour a definition of positively invariant sets in which the solutions $\varphi(t, x)$ are explicitly required to exist for all time $t \geq 0$, by imposing a global Lipschitz continuity requirement on the vector field f, whereas others (Redheffer, 1972) simply require that solutions emanating from the set S remain inside S for as long as they exist in the future (Definition 1 is stated in this spirit).

The first necessary and sufficient condition (i.e. characterization) for positive invariance of **closed** sets in systems of ODEs with unique solutions (but without requiring knowledge of the solutions φ) was given by Nagumo (1942),[1] and was later independently found by numerous other mathematicians (the interested reader is invited to consult (Blanchini, 1999), (Blanchini and Miani, 2008, Ch. 4, §4.2), and (Walter, 1998, Ch. III, §10, XV, XVI) for more details about Nagumo's theorem and its multiple rediscoveries). Informally, Nagumo's theorem states that a *closed set* S is positively invariant if and only if at each point x on the *boundary* of S the vector $f(x)$ points into the interior of the set or is tangent to it. The theorem may be easily applied in cases where the set S is a *sub-level set* of a differentiable real-valued function g, i.e. a set defined as $\{x \in \mathbb{R}^n \mid g(x) \leq 0\}$, provided that the gradient vector $\nabla g(x)$ is non-vanishing (i.e. non-zero) whenever $g(x) = 0$ (intuitively this ensures that the boundary of S is smooth): in this special case Nagumo's theorem says that S is positively invariant if and only if $g'(x) \leq 0$ for all x such that $g(x) = 0$, where g' denotes the (first) Lie derivative of g with respect to the vector field f, which is defined by[2]:

$$g' \overset{\text{def}}{=} \nabla g \cdot f = \sum_{i=1}^{n} \frac{\partial g}{\partial x_n} f_i \;.$$

Remark 3. Applying Nagumo's theorem in practice becomes problematic when the boundary of S is not smooth, e.g. when the set $\{x \in \mathbb{R}^n \mid g(x) = 0\}$ contains *singularities* (points x where the gradient vanishes, i.e. $\nabla g(x) = 0$); these issues have been explored by Taly and Tiwari (2009). In order to apply the theorem more generally to sets that are intersections of sub-level sets, i.e. $\{x \in \mathbb{R}^n \mid g_i(x) \leq 0,\ i = 1, \ldots, k\}$, one likewise needs to be very careful. The concept of *practical sets* was introduced specifically to deal with these issues (see Blanchini and Miani, 2008, Ch. 4, Def. 4.9).

[1] Nagumo's result was in fact a little more general in that it did *not* require unique solutions and focused on so-called *weak positive invariance*, which is identical to positive invariance when solutions are unique.

[2] The Lie derivative of g is sometimes also denoted by $L_f(g)$ instead of g'.

In the following sections we will be concerned with characterizations of positive invariance that are of a very different nature to that of Nagumo's result (which provides a characterization only for closed sets obtained using the tools of real analysis and is without effective computational means of applying it). As we shall see, these alternative characterizations can be effectively applied using tools from commutative algebra and real algebraic geometry.

3. Characterizing positive invariance through inward sets

Let us consider the following construction of the so-called *inward set* for a given set $S \subseteq \mathbb{R}^n$ and a system of ODEs $x' = f(x)$ for which a unique (local) solution to the initial value problem exists for any $x \in \mathbb{R}^n$, following (Zhan et al., 2017, Def. 9.4):

$$\mathrm{In}_f(S) \overset{\text{def}}{=} \{x \in \mathbb{R}^n \mid \exists\, \varepsilon > 0.\ \forall\, t \in (0, \varepsilon).\ \varphi(t, x) \in S\}\,.$$

When time/flow is reversed, one can likewise construct the *inverse inward set*:

$$\mathrm{In}_{-f}(S) = \{x \in \mathbb{R}^n \mid \exists\, \varepsilon > 0.\ \forall\, t \in (0, \varepsilon).\ \varphi(-t, x) \in S\}\,.$$

It is useful to intuitively think of these as sets of states from which the system will evolve inside S for some non-trivial time interval "immediately in the future" and, respectively, has evolved inside S for some non-trivial time interval "immediately in the past".

We observe that, although according to the statement of $\mathrm{In}_f(S)$, x can be any point in $\mathbb{R}^n$, it is in fact restricted to the closure of S.

Lemma 4. *For $S \subseteq \mathbb{R}^n$, the set $\mathrm{In}_f(S)$ is a subset of the closure of S.*

Proof. We show by contradiction that $\mathrm{In}_f(S) \cap (S^c)^\circ$ is empty. Let x be an element of the intersection. Since $x \in (S^c)^\circ$, there exists an open neighbourhood $U \subset (S^c)^\circ$ of x and $\rho > 0$ such that $\varphi(t, x) \in U \subset S^c$ for all $t \in (0, \rho)$ (by continuity of $\varphi(\cdot, x)$). But if $x \in \mathrm{In}_f(S)$, then there exists $\varepsilon > 0$ such that $\varphi(t, x) \in S$ for all $t \in (0, \varepsilon)$. So $\varphi(t, x)$ is in both S^c and S for all $t \in (0, \min\{\rho, \varepsilon\})$, a contradiction. □

Remark 5. Notice that the *interior* of S is always contained inside $\mathrm{In}_f(S)$ (by definition) and the inclusion $S \subseteq \mathrm{In}_f(S)$ therefore holds trivially whenever S is an open set (for any f). A quick glance at the definitions

$$\mathrm{In}_f(S^c) = \{x \in \mathbb{R}^n \mid \exists\, \varepsilon > 0.\ \forall\, t \in (0, \varepsilon).\ \varphi(t, x) \notin S\}\,,$$
$$\mathrm{In}_f(S)^c = \{x \in \mathbb{R}^n \mid \forall\, \varepsilon > 0.\ \exists\, t \in (0, \varepsilon).\ \varphi(t, x) \notin S\}\,,$$

reveals the following inclusion $\mathrm{In}_f(S^c) \subseteq \mathrm{In}_f(S)^c$ for any set S. Whenever S is a closed set (S^c is open), we therefore have that $S^c \subseteq \mathrm{In}_f(S^c) \subseteq \mathrm{In}_f(S)^c$ or, if we prefer, $\mathrm{In}_f(S) \subseteq S$.

These constructions can be used to state the following characterization of positively invariant sets.

Theorem 6. *A set $S \subseteq \mathbb{R}^n$ is positively invariant under the flow of the system $x' = f(x)$ if and only if $S \subseteq \mathrm{In}_f(S)$ and $S^c \subseteq \mathrm{In}_{-f}(S^c)$.*

Theorem 6 can be understood and proved using *induction over the non-negative real numbers*. Though there are many different variations of induction over the reals (e.g. see Clark, 2019), this method of proof appears to be far less well known than standard mathematical induction over the natural numbers. We state below a version of real induction that is well suited to directly prove the theorem.

Lemma 7 *(Real induction). A predicate $P(t)$ holds for all $t \geq 0$ if and only if:*

1. $P(0)$,

2. $\forall\, t \geq 0.\ \Big(\neg P(t) \to \big(\exists\, \varepsilon > 0.\ \forall\, T \in (t-\varepsilon, t).\ \neg P(T)\big)\Big)$,
3. $\forall\, t \geq 0.\ \Big(P(t) \to \big(\exists\, \varepsilon > 0.\ \forall\, T \in (t, t+\varepsilon).\ P(T)\big)\Big)$.

Proof. Necessity is obvious. Sufficiency is easy to show by considering (for contradiction) that there exists $t \geq 0$ such that $\neg P(t)$ and defining the time $t_* = \inf\{t \geq 0 \mid \neg P(t)\}$ (which exists as the set is assumed to be non-empty, is bounded from below, and the reals are complete). By 1. and 3. we have that $t_* \neq 0$, so t_* must be positive, but in this case $P(t)$ holds for all $t \in [0, t_*)$ (by definition). If $P(t_*)$ holds, then t_* cannot be an infimum (by 3.), and if $\neg P(t_*)$ then (by 2.) we have that $\neg P(t)$ holds for all $t \in (t_* - \varepsilon, t_*)$ for some $\varepsilon > 0$; a contradiction. □

Using the above real induction principle, the proof of Theorem 6 is immediate if one takes "$\varphi(t, x) \in S$" to be the predicate $P(t)$ in Lemma 7. We remark that (unlike Nagumo's theorem), Theorem 6 makes no assumptions about the set S being closed, or open. As such, Theorem 6 is very general and applies to all sets and systems of ODEs with locally unique solutions.

Theorem 6 is closely related to (Zhan et al., 2017, Thm. 9.1) where the authors require $S^c \subseteq \mathrm{In}_{-f}(S)^c$ instead of $S^c \subseteq \mathrm{In}_{-f}(S^c)$.[3] Despite the fact that, in general, $\mathrm{In}_{-f}(S)^c \neq \mathrm{In}_{-f}(S^c)$ (cf. counterexample 19), the conditions in Theorem 6 and (Zhan et al., 2017, Thm. 9.1) are in fact equivalent. We show this equivalence by appealing again to real induction: we first state a slightly different real induction principle that is more suited to prove (Zhan et al., 2017, Thm. 9.1), providing thereby a new simpler proof for this known result, and then show that both principles are in fact equivalent.[4]

Lemma 8 *(Real induction (Jackson)). A predicate $P(t)$ holds for all $t \geq 0$ if and only if:*

1. $P(0)$,

2'. $\forall\, t > 0.\ \Big(\big(\exists\, \varepsilon \in (0, t].\ \forall\, T \in (t-\varepsilon, t).\ P(T)\big) \to P(t)\Big)$,

3. $\forall\, t \geq 0.\ \Big(P(t) \to \big(\exists\, \varepsilon > 0.\ \forall\, T \in (t, t+\varepsilon).\ P(T)\big)\Big)$.

Notice that condition 2'. could be equivalently replaced by its contrapositive form

2". $\forall\, t > 0.\ \Big(\neg P(t) \to \big(\forall\, \varepsilon \in (0, t].\ \exists\, T \in (t-\varepsilon, t).\ \neg P(T)\big)\Big)$.

Proof. Necessity is obvious. Sufficiency is easy to show by considering (for contradiction) the time $t_* = \inf\{t \geq 0 \mid \neg P(t)\}$. By 1. and 3. we have that $t_* \neq 0$, so t_* must be positive, but in this case $P(t)$ holds for all $t \in [0, t_*)$ (by definition) and by 2'. we have that $P(t_*)$ holds; a contradiction. □

Remark 9. For completeness, we include below a statement of Hathaway's *continuity induction* (Hathaway, 2011), which is very similar to the notion of real induction in (Clark, 2019). A predicate $P(t)$ holds for all $t \in [0, T]$, where $T > 0$, if and only if:

1. $P(0)$ holds,
2. $\forall\, \tau \in (0, T].\ \Big(\big(\forall\, \tau' \in [0, \tau).\ P(\tau')\big) \to P(\tau)\Big)$,
3. $\forall\, \tau \in [0, T).\ \Big(\big(\forall\, \tau' \in [0, \tau].\ P(\tau')\big) \to \big(\exists\, \epsilon > 0.\ \forall\, \tau'' \in (\tau, \tau+\epsilon).\ P(\tau'')\big)\Big)$.

The proof is essentially identical to that of Lemma 8.

[3] The set inclusions required in (Zhan et al., 2017, Thm. 9.1) can be alternatively phrased as $\mathrm{In}_{-f}(S) \subseteq S \subseteq \mathrm{In}_f(S)$.

[4] The idea of using real induction to prove (Zhan et al., 2017, Thm. 9.1) was first suggested by Paul B. Jackson and Kousha Etessami (School of Informatics, University of Edinburgh) in private communication with the second author.

The proof of (Zhan et al., 2017, Thm. 9.1) now becomes immediate using real induction as it is stated in Lemma 8. The following lemma establishes an equivalence between the two formulations of real induction.

Lemma 10. *Let $P(t)$ denote a predicate defined for all $t \geq 0$. If*

1. $P(0)$, *and*
3. $\forall\, t \geq 0.\ \Big(P(t) \to \big(\exists\, \varepsilon > 0.\ \forall\, T \in (t, t+\varepsilon).\ P(T)\big)\Big)$ *hold,*

then

2. $\forall\, t \geq 0.\ \Big(\neg P(t) \to \big(\exists\, \varepsilon > 0.\ \forall\, T \in (t-\varepsilon, t).\ \neg P(T)\big)\Big)$,

if and only if

2”. $\forall\, t > 0.\ \Big(\neg P(t) \to \big(\forall\, \varepsilon \in (0, t].\ \exists\, T \in (t-\varepsilon, t).\ \neg P(T)\big)\Big)$.

Proof. The implication from 2. to 2”. is obvious (in this sense, one may consider Lemma 7 *weaker* than Lemma 8). To prove the converse, suppose (for contradiction) that 2”. and ¬2. both hold. More explicitly:

$$\neg 2. \ \equiv\ \exists\, t \geq 0.\ \Big(\neg P(t) \wedge \big(\forall\, \varepsilon > 0.\ \exists\, T \in (t-\varepsilon, t).\ P(T)\big)\Big)\,.$$

Let $\tau > 0$ be the point at which $\neg P(\tau)$ holds in ¬2. (τ cannot be 0 by 1.) Then for all $\varepsilon_0 > 0$, there exists some $T_0 \in (\tau - \varepsilon_0, \tau)$ such that $P(T_0)$ holds. Consider the interval $I_0 = [T_0, \tau]$. At T_0, since $P(T_0)$ holds, we have (by 3.) that $P(t)$ holds for all t in the interval $I_1 = [T_0, T_0 + \varepsilon_1)$ for some $\varepsilon_1 > 0$. If $T_0 + \varepsilon_1 \geq \tau$, we obtain a contradiction (because $\neg P(\tau)$ is assumed to hold); otherwise we have $I_1 = [T_0, T_0 + \varepsilon_1) \subset [T_0, \tau]$. If at the endpoint of I_1 we have that $\neg P(T_0 + \varepsilon_1)$ holds, we obtain a contradiction (by 2”.), and if $P(T_0 + \varepsilon_1)$ holds we have (by 3.) that for some $\varepsilon_2 > 0$, $P(t)$ holds for all $t \in I_2 = [T_0, T_0 + \varepsilon_1 + \varepsilon_2)$. Repeating the argument, we obtain a sequence I_k of intervals of strictly increasing length where $P(t)$ holds. The right endpoints of the intervals in this sequence cannot converge within $(T_0, \tau]$ because this would yield a contradiction (by 2”.). The right endpoints thus go beyond τ, which again yields a contradiction. □

The equivalence stated in Lemma 10 is somewhat abstract and it may not be immediately clear how this equivalence is relevant with regard to inward sets. To make this more apparent, we prove below a lemma which can be used to establish the equivalence between Theorem 6 and (Zhan et al., 2017, Thm. 9.1) without appealing to real induction directly in the proof, although following a similar line of argument as that employed in the proof of Lemma 10.

Lemma 11. *Let $S \subseteq \mathbb{R}^n$. If $S \subseteq \mathrm{In}_f(S)$ then $\mathrm{In}_{-f}(S) = \mathrm{In}_{-f}(S^c)^c$.*

Proof. The inclusion $\mathrm{In}_{-f}(S) \subseteq \mathrm{In}_{-f}(S^c)^c$ holds in general by definition as already stated. Let $x \in \mathrm{In}_{-f}(S^c)^c$ and let $\varepsilon_0 > 0$. Then, by definition, there exists $t_0 \in (0, \varepsilon_0)$, such that $x_0 := \varphi(-t_0, x) \notin S^c$, or equivalently $x_0 \in S$. Since $S \subseteq \mathrm{In}_f(S)$, $x_0 \in \mathrm{In}_f(S)$ and there exists $\gamma_0 > 0$, such that for all $s_0 \in (0, \gamma_0)$, $\varphi(s_0, x_0) \in S$.

If $-t_0 + \gamma_0 < 0$, then the same arguments with $\varepsilon_1 := t_0 - \gamma_0$ lead to the existence of $t_1, \gamma_1 > 0$ such that for all $s_1 \in (0, \gamma_1)$, $\varphi(s_1, x_1) \in S$ where $x_1 := \varphi(-t_1, x)$. We can thus construct a (strictly) increasing sequence $-t_0 + \gamma_0, -t_1 + \gamma_1, \ldots$. Two cases may occur:

(i) If the sequence crosses zero after finitely many steps, that is there exists $n \geq 0$ such that $-t_n + \gamma_n \geq 0$, then this means that for all $t \in (0, t_n)$, $\varphi(-t, x) \in S$ thereby proving that $x \in \mathrm{In}_{-f}(S)$ since $-t_n < -t < 0 \leq -t_n + \gamma_n$.

(ii) If the sequence is upper bounded by 0, then it has a limit $-t_l + \gamma_l \leq 0$. The case $-t_l + \gamma_l < 0$ is impossible since we can perform one more step to get $-t_l + \gamma_l < -t_{l'} + \gamma_{l'} \leq 0$. Thus $-t_l + \gamma_l = 0$ and one gets $\varphi(-t, x) \in S$ for all $t \in (0, t_l)$ leading, as in case (i), to $x \in \mathrm{In}_{-f}(S)$. □

Remark 12. The statement of the characterization in Theorem 6 enjoys some rather nice properties when compared to that of (Zhan et al., 2017, Thm. 9.1). It is in particular symmetric in the sense that the set inclusions in the theorem are preserved when one simultaneously replaces S with its complement S^c and f with the reversed dynamics $-f$.

This allows for instance to immediately prove the well-known result in dynamical systems which states that a set is positively invariant if and only if its complement is negatively invariant (Bhatia and Szegő, 1970, Thm. 1.4). One sees that by syntactically replacing S with S^c and f with $-f$ in the conditions of Theorem 6, one obtains $S^c \subseteq \mathrm{In}_{-f}(S^c)$ and $S \subseteq \mathrm{In}_f(S)$, i.e. *equivalent* conditions, using only the set-theoretic fact that $(S^c)^c = S$. On the other hand, applying the same transformation to the conditions $S \subseteq \mathrm{In}_f(S)$ and $S^c \subseteq \mathrm{In}_{-f}(S)^c$ required in (Zhan et al., 2017, Thm. 9.1), one does *not* immediately obtain the same conditions; instead, one obtains $S^c \subseteq \mathrm{In}_{-f}(S^c)$ and $S \subseteq \mathrm{In}_f(S^c)^c$. In order to show that the original inclusions hold one needs to use the fact that $\mathrm{In}_{-f}(S^c) \subseteq \mathrm{In}_{-f}(S)^c$ for the first inclusion, and then use Lemma 11 for the second inclusion, which is somewhat more involved than using Theorem 6 to prove the same fact.

The main practical difficulty in applying Theorem 6 (or equivalently (Zhan et al., 2017, Thm. 9.1)) lies in the fact that inward sets $\mathrm{In}_f(S)$ and $\mathrm{In}_{-f}(S^c)$ are defined in terms of solutions to a system of differential equations; the theorem says nothing about our ability to construct these sets or reason about their inclusion. The following section will elucidate how this problem is addressed using tools from algebraic geometry in the important case where the set S is semi-algebraic and the right-hand side of the system $x' = f(x)$ is polynomial.

3.1. A decision procedure for checking positively invariant sets

In this section we describe a procedure for deciding whether a given set is positively invariant or not. For this we first require a few basic results. Let $g : \mathbb{R}^n \to \mathbb{R}$ denote a real-valued function. The zero-th Lie derivative of g is g itself, the first order Lie derivative $g' \overset{\text{def}}{=} \nabla g \cdot f$ corresponds to the total derivative of $t \mapsto g(\varphi(t, x))$ with respect to time t, and higher-order Lie derivatives are defined inductively, i.e. $g'' = (g')'$; the k-th order Lie derivative of g will be denoted by $g^{(k)}$. We will require the fact that unique solutions to real analytic systems of ODEs are also real analytic (Chicone, 2006, Thm 1.3). Whenever g is a real analytic function, its Taylor series expansion

$$g(\varphi(t, x)) = g(x) + g'(x)t + g''(x)\frac{t^2}{2!} + \cdots$$

converges in some time interval (ϵ_l, ϵ_u), where $\epsilon_l < 0 < \epsilon_u$. The set of states $\{x \in \mathbb{R}^n \mid g(x) = 0\}$, simply denoted by $g = 0$ in the sequel, remains invariant under the flow for some non-trivial forward time interval if and only if *all* Lie derivatives $g^{(k)}$, $k \geq 1$, vanish whenever $g(x) = 0$.

Remark 13. We will abuse notation slightly in this article by interchangeably using sets and formulas characterizing those sets. For example, we will use formulas in the arguments to In_f and In_{-f} (from Theorem 6). However, when describing sets we will use set-theoretic symbols $\cup$ and $\cap$ for set union and intersection, respectively, and will let S^c denote the complement of S; when we are working with formulas, we will instead employ the corresponding logical symbols $\vee$ and $\wedge$ for disjunction and conjunction, and $\neg$ for negation. The set $\mathbb{R}^n$ (resp. $\emptyset$) will be syntactically represented by the symbol $\mathbf{T}$ (resp. $\mathbf{F}$).

We thus have the inward set of $g = 0$ given by

$$\mathrm{In}_f(g = 0) \quad = \quad g = 0 \cap g' = 0 \cap g'' = 0 \cap g''' = 0 \cap \cdots \quad ,$$

which is characterized by the following infinite "formula"[5]

$$\text{“}\quad \mathrm{In}_f(g=0) \quad\equiv\quad g=0 \wedge g'=0 \wedge g''=0 \wedge g'''=0 \wedge \cdots \quad\text{”}.$$

For sets of states satisfying inequalities $\{x \in \mathbb{R}^n \mid g(x) < 0\}$, which we also concisely denote by the formula $g < 0$, the situation is similar with the following infinite construction:

$$\begin{aligned}\text{“}\quad \mathrm{In}_f(g<0) \quad\equiv\quad & g<0 \\ & \vee\ (g=0 \wedge g'<0) \\ & \vee\ (g=0 \wedge g'=0 \wedge g''<0) \\ & \vee\ (g=0 \wedge g'=0 \wedge g''=0 \wedge g'''<0) \\ & \vdots \\ & \qquad\quad \text{”}.\end{aligned}$$

Intuitively, the first non-zero Lie derivative of g needs to be negative at a point x satisfying $g(x) = 0$ in order for the flow $\varphi(t, x)$ to enter the set $g < 0$ from that point and remain within this set throughout some time interval $(0, \epsilon)$, for some positive ϵ.

Remark 14. One may draw physical analogies here, e.g. to the motion of a vehicle: if the velocity is 0, then it is the sign of the acceleration term that determines whether the vehicle will move forward in the next time instant; if both the velocity and the acceleration are 0, it is the sign of the derivative of the acceleration (i.e. the sign of the jerk term), and so forth.

The decision procedure developed by Liu et al. (2011) rests on the fact that for a polynomial function p and a polynomial system of ODEs $x' = f(x)$, the formulas characterizing $\mathrm{In}_f(p=0)$ and $\mathrm{In}_f(p<0)$ are indeed *finite*. To see why this is true, note that whenever p and $f_1, f_2, \ldots, f_n$ that make up f are polynomials, all the formal Lie derivatives $p', p'', \cdots$ are also guaranteed to be polynomials. Let us now recall the *ascending chain property* of ideals in the polynomial ring $\mathbb{R}[x_1, \ldots, x_n]$ – a consequence of Hilbert's basis theorem and the fact that the ring $\mathbb{R}$ is Noetherian (Cox et al., 2015, Ch. 2, Thm. 7).

Lemma 15. *Let $p \in \mathbb{R}[x_1, \ldots, x_n]$, then the ascending chain of ideals*

$$\langle p \rangle \subseteq \langle p, p' \rangle \subseteq \langle p, p', p'' \rangle \subseteq \cdots$$

is finite, i.e. there exists a $k \in \mathbb{N}$ such that $\langle p, p', \ldots, p^{(k)} \rangle = \langle p, p', \ldots, p^{(K)} \rangle$ for all $K \geq k$.

For a given p, we denote the smallest k in the above lemma by $\mathrm{ord}_f(p)$ and say that it defines the *order* of p with respect to the system of polynomial ODEs $x' = f(x)$. In practice, we can always compute $\mathrm{ord}_f(p)$ by simply computing successive formal Lie derivatives of p and successively checking whether

$$p^{(k+1)} \in \langle p, p', p'', \ldots, p^{(k)} \rangle$$

holds for $k = 1, 2, 3, \ldots$, until the membership check succeeds, which would imply that the ideal chain has stabilized (the fact that this process terminates is guaranteed by Lemma 15).[6] The ideal membership check can be easily performed by reducing the polynomial $p^{(k+1)}$ by the Gröbner basis

[5] Technically, a formula can only be finite, hence the quotes for such hypothetical objects.

[6] Using terminology from differential algebra (Ritt, 1950) one may say that the ideal $\langle p, p', \ldots, p^{(\mathrm{ord}_f(p))} \rangle$ defines a *differential ideal*.

of $\{p, p', \ldots, p^{(k)}\}$ for each successive k and checking whether the remainder is 0. An upper bound on the length of the ascending chain of ideals generated by successive Lie derivatives of p was obtained in (Novikov and Yakovenko, 1999, Thm. 4); this bound is doubly-exponential in the number of variables, however, in practice one typically observes the ideals stabilizing after only a few iterations.

As a direct consequence of Lemma 15, whenever $p, p', \ldots, p^{(\mathrm{ord}_f(p))}$ are all simultaneously 0, all higher derivatives must also evaluate to 0. More formally:

$$p = 0 \wedge p' = 0 \wedge p'' = 0 \wedge \cdots \wedge p^{(\mathrm{ord}_f(p))} = 0 \rightarrow \forall K > \mathrm{ord}_f(p).\ p^{(K)} = 0 .$$

Using this fact one can construct perfectly legitimate formulas that provide a finite characterization of $\mathrm{In}_f(p = 0)$ and $\mathrm{In}_f(p < 0)$, given as follows:

$$\begin{aligned}
\mathrm{In}_f(p = 0) \quad &\equiv \quad p = 0 \wedge p' = 0 \wedge p'' = 0 \wedge \cdots \wedge p^{(\mathrm{ord}_f(p))} = 0 \,, \\
\mathrm{In}_f(p < 0) \quad &\equiv \quad p < 0 \\
&\vee\ (p = 0 \wedge p' < 0) \\
&\vee\ (p = 0 \wedge p' = 0 \wedge p'' < 0) \\
&\ \vdots \\
&\vee\ (p = 0 \wedge p' = 0 \wedge p'' = 0 \wedge \cdots \wedge p^{(\mathrm{ord}_f(p))} < 0) \,.
\end{aligned}$$

Notice that in the construction of $\mathrm{In}_f(p < 0)$ the saturation of the chain of ideals guarantees that all further terms in the disjunction, i.e.

$$p = 0 \wedge p' = 0 \wedge p'' = 0 \wedge \cdots \wedge p^{(\mathrm{ord}_f(p))} = 0 \wedge \cdots \wedge p^{(K)} < 0$$

where $K > \mathrm{ord}_f(p)$, are False and therefore unnecessary.

3.2. *Improving the construction of* $\mathrm{In}_f(p = 0)$ *and* $\mathrm{In}_f(p < 0)$

One may work naïvely with ideals generated by the successive Lie derivatives $\langle p, p', p'', \ldots, p^{(k)}\rangle$ and construct $\mathrm{In}_f(p = 0)$ and $\mathrm{In}_f(p < 0)$ using these derivatives directly (as above), following Liu et al. (2011). However, this construction can be improved if one realizes that only the *remainders* of the Lie derivatives are needed for this construction, as will be shown in the following lemma. The practical advantage afforded by doing this is the degree of the remainder polynomials, which is typically lower than the degree of the Lie derivatives themselves.

Lemma 16. *Given a polynomial p and a system of polynomial ODEs $x' = f(x)$, let $\mathrm{rem}_0 = p$ and let rem_{i+1} be defined inductively as the* remainder *obtained from polynomial reduction (i.e. multivariate polynomial division) of the Lie derivative rem_i' by the polynomials $\{\mathrm{rem}_0, \mathrm{rem}_1 \ldots, \mathrm{rem}_i\}$. Then for all $i \geq 0$*

$$\mathrm{rem}_i = p^{(i)} - \sum_{j=0}^{i-1} \alpha_{ij} p^{(j)}$$

where α_{ij} are polynomials.

Proof. By induction. Base case: $\mathrm{rem}_0 = p = p^{(0)}$. For an inductive hypothesis, assume that $\mathrm{rem}_k = p^{(k)} - \sum_{j=0}^{k-1} \alpha_{kj} p^{(j)}$ holds for all $k \leq n$. Since rem_{n+1} is the remainder upon the reduction of rem_n' by $\{\mathrm{rem}_0, \ldots, \mathrm{rem}_n\}$, we have $\mathrm{rem}_{n+1} = \mathrm{rem}_n' - \sum_{i=0}^{n} \beta_i \mathrm{rem}_i$, where $\beta_0, \ldots, \beta_n$ are polynomials. From our inductive hypothesis and by applying the product rule for differentiation we have

$$\mathrm{rem}'_n = p^{(n+1)} - \left(\sum_{j=0}^{n-1} \alpha_{nj} p^{(j)}\right)' = p^{(n+1)} - \sum_{j=0}^{n} \gamma_j p^{(j)}\,, \tag{1}$$

where $\gamma_0, \dots, \gamma_n$ are polynomials, and

$$\begin{aligned}
\mathrm{rem}_{n+1} &= \mathrm{rem}'_n - \sum_{i=0}^{n} \beta_i \mathrm{rem}_i \qquad \text{[from the definition]} \\
&= \left(p^{(n+1)} - \sum_{j=0}^{n} \gamma_j p^{(j)}\right) - \sum_{i=0}^{n} \beta_i \mathrm{rem}_i \qquad \text{[from (1)]}\,, \\
&= \left(p^{(n+1)} - \sum_{j=0}^{n} \gamma_j p^{(j)}\right) - \sum_{i=0}^{n} \beta_i \left(p^{(i)} - \sum_{l=0}^{i-1} \alpha_{il} p^{(l)}\right) \quad \text{[by hypothesis]}\,,
\end{aligned}$$

from which it is apparent that rem_{n+1} has the required form:

$$\mathrm{rem}_{n+1} = p^{(n+1)} - \sum_{j=0}^{n} \alpha_{n+1j} p^{(j)}\,. \quad \square$$

Lemma 17. *Let* rem_i *be defined as in Lemma 16. Then the inward sets can be characterized as follows:*

$$\mathrm{In}_f(p=0) \quad \equiv \quad (\mathrm{rem}_0 = 0 \wedge \mathrm{rem}_1 = 0 \wedge \mathrm{rem}_2 = 0 \wedge \cdots \wedge \mathrm{rem}_{\mathrm{ord}_f(p)} = 0)$$

and

$$\begin{aligned}
\mathrm{In}_f(p<0) \quad \equiv \quad & \mathrm{rem}_0 < 0 \\
& \vee\ (\mathrm{rem}_0 = 0 \wedge \mathrm{rem}_1 < 0) \\
& \vee\ (\mathrm{rem}_0 = 0 \wedge \mathrm{rem}_1 = 0 \wedge \mathrm{rem}_2 < 0) \\
& \vdots \\
& \vee\ (\mathrm{rem}_0 = 0 \wedge \mathrm{rem}_1 = 0 \wedge \mathrm{rem}_2 = 0 \wedge \cdots \wedge \mathrm{rem}_{\mathrm{ord}_f(p)} < 0)\,.
\end{aligned}$$

Proof. For $\mathrm{In}_f(p=0)$, we show by induction that

$$\forall\, n \geq 0.\ \left(\bigcap_{i=0}^{n} \mathrm{rem}_i = 0\right) = \left(\bigcap_{i=0}^{n} p^{(i)} = 0\right).$$

Base case: $\mathrm{rem}_0 = p^{(0)} = p$ by definition. For the inductive hypothesis, let us assume that

$$\left(\bigcap_{i=0}^{k} \mathrm{rem}_i = 0\right) = \left(\bigcap_{i=0}^{k} p^{(i)} = 0\right)$$

holds for some $k \geq 0$. Then from the hypothesis we have that

$$\left(\bigcap_{i=0}^{k+1} \mathrm{rem}_i = 0\right) = \left(\bigcap_{i=0}^{k} p^{(i)} = 0 \ \cap \mathrm{rem}_{k+1} = 0\right).$$

By Lemma 16 we have $\mathrm{rem}_{k+1} = p^{(k+1)} - \sum_{j=0}^{k} \alpha_{k+1j} p^{(j)}$ and hence

$$\left(\bigcap_{i=0}^{k+1} \mathrm{rem}_i = 0\right) = \left(\bigcap_{i=0}^{k} p^{(i)} = 0 \cap p^{(k+1)} - \sum_{j=0}^{k} \alpha_{k+1j} p^{(j)} = 0\right)$$
$$= \left(\bigcap_{i=0}^{k} p^{(i)} = 0 \cap p^{(k+1)} = 0\right).$$

The proof for $\mathrm{In}_f(p < 0)$ follows a similar inductive argument. □

Remark 18. Using the remainders instead of the higher-order Lie derivatives of p for constructing $\mathrm{In}_f(p = 0)$ and $\mathrm{In}_f(p < 0)$ is pragmatically often a good choice. For a concrete example, consider the Van der Pol oscillator whose dynamics is given by $x' = y$ and $y' = -x - y(x^2 - 1)$, and let $p = x^2 + y^2 - 1$. The ascending chain of ideals

$$\langle \mathrm{rem}_0 \rangle \subseteq \langle \mathrm{rem}_0, \mathrm{rem}_1 \rangle \subseteq \langle \mathrm{rem}_0, \mathrm{rem}_1, \mathrm{rem}_2 \rangle \subseteq \cdots$$

stabilizes at $\langle \mathrm{rem}_0, \ldots, \mathrm{rem}_6 \rangle$, which is $\langle x^2 + y^2 - 1, 2y^4, -8xy^3, 24y^2, -48xy, 48 \rangle$. In contrast, if one uses the actual higher-order Lie derivatives, the 6 generators of the ideal $\langle p, p', \ldots, p^{(6)} \rangle$ are too large to all fit on this page, with $p^{(6)}$ having total degree 12. We should however note that in certain cases it may be more expensive to compute the ideal $\langle \mathrm{rem}_0, \mathrm{rem}_1, \ldots, \mathrm{rem}_{\mathrm{ord}_f(p)} \rangle$ than it is to compute $\langle p, p', \ldots, p^{(\mathrm{ord}_f(p))} \rangle$ because the potential gain in lowering the total degree of the ideal generators can be outweighed by the computational overhead arising from the size of the coefficients of the intermediate polynomials. This is a well-known phenomenon when computing Gröbner bases (Cox et al., 2015, Ch. 2, p. 116).

3.3. Distributive properties of In_f

Viewed as a set operator, In_f distributes over set intersections. For any sets $S_1, S_2 \subseteq \mathbb{R}^n$, one has:

$$\mathrm{In}_f(S_1 \cap S_2) = \mathrm{In}_f(S_1) \cap \mathrm{In}_f(S_2).$$

The operator In_f does not, however, distribute over set union; only the following set inclusion is guaranteed to hold in general:

$$\mathrm{In}_f(S_1 \cup S_2) \supseteq \mathrm{In}_f(S_1) \cup \mathrm{In}_f(S_2).$$

Counterexample 19. To see why the converse inclusion does not hold, consider the simple 1-dimensional system $x' = 1$ and the set

$$S = \left\{x \in \mathbb{R} \mid x \leq 0 \vee \left(x > 0 \wedge \sin\left(x^{-1}\right) = 0\right)\right\}.$$

The point $0 \in \mathbb{R}$ cannot be an element of $\mathrm{In}_f(S)$ because $\varphi(t, 0) = t$ and for any positive ϵ there exists a $t \in (0, \epsilon)$ such that $\sin\left(t^{-1}\right) \neq 0$ and therefore $\varphi(t, 0) \notin S$. In other words, 0 belongs to $\mathrm{In}_f(S)^c$. At the same time, 0 cannot be in $\mathrm{In}_f(S^c)$ either because the flow cannot move from the point at $x = 0$ without crossing one root of $\sin\left(t^{-1}\right) = 0$. Thus

$$\mathrm{In}_f(S \cup S^c) = \mathrm{In}_f(\mathbb{R}^n) = \mathbb{R}^n \neq \mathrm{In}_f(S) \cup \mathrm{In}_f(S^c).$$

The example also shows that in general $\mathrm{In}_f(S^c)$ is not equal to $\mathrm{In}_f(S)^c$ since $0 \in \mathrm{In}_f(S)^c$ while $0 \notin \mathrm{In}_f(S^c)$.[7]

[7] Recall from Remark 5 that $\mathrm{In}_f(S^c) \subseteq \mathrm{In}_f(S)^c$ holds for any set S. The above counterexample demonstrates that the converse inclusion does not hold generally.

For semi-analytic sets the In_f operator *does distribute* over set unions. In particular, for semi-algebraic sets (a special class of semi-analytic sets) given by

$$S = \bigcup_{i=1}^{l} \left(\bigcap_{j=1}^{m_i} p_{ij} < 0 \ \cap \bigcap_{j=m_i+1}^{M_i} p_{ij} = 0 \right) ,$$

where p_{ij} are polynomials, one has:

$$\mathrm{In}_f(S) = \bigcup_{i=1}^{l} \left(\bigcap_{j=1}^{m_i} \mathrm{In}_f(p_{ij} < 0) \ \cap \bigcap_{j=m_i+1}^{M_i} \mathrm{In}_f(p_{ij} = 0) \right) .$$

A proof of this property for semi-algebraic sets (Liu et al., 2011, Lemma 20) was generalized to semi-analytic sets in (Platzer and Tan, 2020, §6.1.2). These results in particular mean that, if one restricts attention to these classes of sets, the equality $\mathrm{In}_f(S)^c = \mathrm{In}_f(S^c)$ holds (making the equivalence of Theorem 6 and (Zhan et al., 2017, Thm. 9.1) immediate, contrary to the general setting where this equality does not hold and where Lemma 11 is required to prove the equivalence).

3.4. The **LZZ** decision procedure based on Theorem 6

Given a quantifier-free formula describing a semi-algebraic set

$$S \equiv \bigvee_{i=1}^{l} \left(\bigwedge_{j=1}^{m_i} p_{ij} < 0 \ \wedge \bigwedge_{j=m_i+1}^{M_i} p_{ij} = 0 \right) ,$$

and a polynomial system of ODEs $x' = f(x)$, in order to decide whether S is a positively invariant set, a basic decision procedure using the characterizations based on inward sets (Theorem 6 and (Liu et al., 2011, Thm. 19)), which we term **LZZ**, after the authors in Liu et al. (2011), can be implemented by performing the following steps:

1. Compute $\mathrm{In}_f(p_{ij} \bowtie_{ij} 0)$, where $\bowtie_{ij} \in \{=, <\}$ appearing in S (formulas $p < 0$ and $p = 0$, where p is a polynomial, will be referred to as *atomic formulas*), and from these construct
$$\mathrm{In}_f(S) \equiv \bigvee_{i=1}^{l} \left(\bigwedge_{j=1}^{m_i} \mathrm{In}_f(p_{ij} < 0) \ \wedge \bigwedge_{j=m_i+1}^{M_i} \mathrm{In}_f(p_{ij} = 0) \right) ,$$
following the distributive property of In_f for semi-algebraic sets S.
2. Construct $\mathrm{In}_{-f}(S^c)$ following the same process as in step 1, but using the complement S^c and the reversed system $x' = -f(x)$.
3. Check the semi-algebraic set inclusions $S \subseteq \mathrm{In}_f(S)$ and $S^c \subseteq \mathrm{In}_{-f}(S^c)$ from Theorem 6 using e.g. the CAD algorithm of Collins and Hong (1991).

Remark 20. One can alternatively construct $\mathrm{In}_{-f}(S)$ in step 2 and check the inclusions $S \subseteq \mathrm{In}_f(S)$ and $S^c \subseteq \mathrm{In}_{-f}(S)^c$ in step 3, following the original method of Liu et al. (2011), rather than the characterization in Theorem 6.

A basic implementation of the **LZZ** decision procedure thus requires an algorithm for computing Gröbner bases (to compute the inward sets in step 1 and step 2) and a decision procedure for the universally (or existentially) quantified fragment of real arithmetic (to check the semi-algebraic set inclusions in step 3).

In practice, the syntactic description of S may feature atomic formulas that are not of the form $p < 0$ or $p = 0$, e.g. S may feature the comparison operators $>, \geq, \leq$, and may have atomic formulas where the term on the right-hand side of the comparison operator is not 0 as assumed above. To implement step 1 and step 2 for this more general case (without tampering with the description of S) it is convenient to compute $\mathrm{In}_f(S)$ by syntactically replacing all atomic formulas $p_{\mathrm{lhs}} \bowtie p_{\mathrm{rhs}}$ (where p_{lhs} and p_{rhs} are polynomials and $\bowtie \in \{<, \leq, =, \neq, \geq, >\}$) appearing in the syntactic description of S, with $\mathrm{In}_f(p_{\mathrm{lhs}} \bowtie p_{\mathrm{rhs}})$, which can be defined for atoms in terms of the primitives $\mathrm{In}_f(p < 0)$ and $\mathrm{In}_f(p = 0)$ in the following way (we use ':=' to denote function definitions):

$$\begin{aligned}
&\mathrm{In}_f(\mathbf{T}) := \mathbf{T}\,,\\
&\mathrm{In}_f(\mathbf{F}) := \mathbf{F}\,,\\
&\mathrm{In}_f(p_{\mathrm{lhs}} = p_{\mathrm{rhs}}) := \mathrm{In}_f(p_{\mathrm{lhs}} - p_{\mathrm{rhs}} = 0)\,,\\
&\mathrm{In}_f(p_{\mathrm{lhs}} < p_{\mathrm{rhs}}) := \mathrm{In}_f(p_{\mathrm{lhs}} - p_{\mathrm{rhs}} < 0)\,,\\
&\mathrm{In}_f(p_{\mathrm{lhs}} > p_{\mathrm{rhs}}) := \mathrm{In}_f(p_{\mathrm{rhs}} - p_{\mathrm{lhs}} < 0)\,,
\end{aligned}$$

and, using the fact that $\mathrm{In}_f(S^c) = \mathrm{In}_f(S)^c$ for semi-algebraic sets S,

$$\begin{aligned}
&\mathrm{In}_f(p_{\mathrm{lhs}} \neq p_{\mathrm{rhs}}) := \neg\,\mathrm{In}_f(p_{\mathrm{lhs}} - p_{\mathrm{rhs}} = 0)\,,\\
&\mathrm{In}_f(p_{\mathrm{lhs}} \leq p_{\mathrm{rhs}}) := \neg\,\mathrm{In}_f(p_{\mathrm{rhs}} - p_{\mathrm{lhs}} < 0)\,,\\
&\mathrm{In}_f(p_{\mathrm{lhs}} \geq p_{\mathrm{rhs}}) := \neg\,\mathrm{In}_f(p_{\mathrm{lhs}} - p_{\mathrm{rhs}} < 0)\,.
\end{aligned}$$

The primitives $\mathrm{In}_f(p = 0)$ and $\mathrm{In}_f(p < 0)$ are defined following Lemma 17 as

$$\begin{aligned}
\mathrm{In}_f(p = 0) \quad &:= \quad (\mathrm{rem}_0 = 0 \wedge \mathrm{rem}_1 = 0 \wedge \mathrm{rem}_2 = 0 \wedge \cdots \wedge \mathrm{rem}_{\mathrm{ord}_f(p)} = 0)\,,\\
\mathrm{In}_f(p < 0) \quad &:= \quad \Big(\mathrm{rem}_0 < 0\\
&\quad \vee\ (\mathrm{rem}_0 = 0 \wedge \mathrm{rem}_1 < 0)\\
&\quad \vee\ (\mathrm{rem}_0 = 0 \wedge \mathrm{rem}_1 = 0 \wedge \mathrm{rem}_2 < 0)\\
&\quad \vdots\\
&\quad \vee\ (\mathrm{rem}_0 = 0 \wedge \mathrm{rem}_1 = 0 \wedge \mathrm{rem}_2 = 0 \wedge \cdots \wedge \mathrm{rem}_{\mathrm{ord}_f(p)} < 0)\Big)\,.
\end{aligned}$$

An implementation of the **LZZ** decision procedure in the Wolfram Language can be achieved with fewer than 35 lines of code following the above approach.[8]

4. Characterizing positive invariance through exit sets

In this section we develop an alternative characterization of positively invariant sets using the concept of *exit set* as formulated by Conley (1978).

Let $s \in I_x$ be a point in time within the maximal interval of existence of solution φ from initial value x, and let $I_{\varphi(s,x)} \overset{\mathrm{def}}{=} \{t \mid t+s \in I_x\}$, which is simply the time interval I_x offset by s (or, equivalently, the maximal interval of existence from the initial value $\varphi(s,x)$). The mapping φ defines a local flow on the topological space $\mathbb{R}^n$ since, for all $x \in \mathbb{R}^n$, $\varphi(0,x) = x$, and

$$\forall\, s \in I_x.\ \forall\, t \in I_{\varphi(s,x)}.\quad \varphi(t, \varphi(s,x)) = \varphi(s+t, x)\,.$$

Let S be a subset of $\mathbb{R}^n$. Recall that a point $x \in \mathbb{R}^n$ is a closure point of S if and only if every open set containing x intersects S in at least one point (not necessarily distinct from x itself if x happens to be in S). Let S° denote the interior of S. The boundary of S, denoted ∂S, is defined as $S \setminus S^\circ$. As before, we use $t > 0$ as a shorthand for $t \in I_x \cap (0, +\infty)$ and, similarly, by $t < 0$ we understand $t \in I_x \cap (-\infty, 0)$.

[8] Our implementation is available from (Ghorbal, 2020).

Definition 21 *(Exit Set (Conley, 1978)).* The *exit set* of $S \subseteq \mathbb{R}^n$ with respect to the local flow induced by $x' = f(x)$ is defined as follows:

$$\mathrm{Exit}_f(S) \overset{\text{def}}{=} \{x \in S \mid \forall\, t > 0.\ \exists\, s \in (0,t).\ \varphi(s,x) \notin S\}\,.$$

The exit set of S defines the set of points in S from which the flow cannot evolve forward in time without leaving the set S. As the name suggests, a flow starting at a point in $\mathrm{Exit}_f(S)$ "leaves the set S immediately" (regardless of where it was before). It is intuitive that such points can only lie on the boundary of S.

Lemma 22. *The set* $\mathrm{Exit}_f(S)$ *is a subset of* ∂S *(in addition to being a subset of* S*, by definition).*

Proof. Let $x \in \mathrm{Exit}_f(S) \cap S^\circ$, then there exists an open set $U \subset S^\circ$ containing x. By continuity of $\varphi(\cdot, x)$ with respect to time, there exists a neighbourhood I of 0 in I_x such that $\varphi(t,x) \in U$ for all $t \in I$. Let $t \in I \cap (0,+\infty)$. Since $x \in \mathrm{Exit}_f(S)$, there exists $s \in (0,t) \subset I$ such that $\varphi(s,x) \notin S$ and, a fortiori, $\varphi(s,x) \notin U$, which contradicts the existence of I and thus $\mathrm{Exit}_f(S) \cap S^\circ = \emptyset$. Since $\mathrm{Exit}_f(S) \subseteq S$ by definition, the exit set is a subset of ∂S. □

Positive invariance of a set S (as given in Definition 1) may be equivalently defined using the set of so-called *escape points* (also due to Conley, 1978)[9]:

$$\mathrm{Escape}_f(S) \overset{\text{def}}{=} \{x \in S \mid \exists\, t > 0.\ \varphi(t,x) \notin S\}\,. \tag{2}$$

Notice the difference between the exit and escape sets: starting at an exit point, the flow *immediately exits* the set S, whereas for an escape point the flow may first evolve within S before leaving S at some point in time in the future (i.e., it *must* eventually leave S). Thus, $\mathrm{Exit}_f(S) \subseteq \mathrm{Escape}_f(S)$. The set of escape points of S is empty precisely when S is a positively invariant set. Furthermore, this criterion can be stated entirely in terms of exit sets.

Theorem 23. *A set* $S \subseteq \mathbb{R}^n$ *is positively invariant if and only if both* $\mathrm{Exit}_f(S)$ *and* $\mathrm{Exit}_{-f}(S^c)$ *are empty.*

Proof. For necessity, it is easy to see that the set is not positively invariant whenever the exit sets are not both empty. Case (i): if $\mathrm{Exit}_f(S)$ is non-empty, then for some point $x \in S$ there exists a $t > 0$ such that $\varphi(t,x) \notin S$. Case (ii): if $\mathrm{Exit}_{-f}(S^c)$ is non-empty, then for some $y \notin S$ there exists a $\tau > 0$ such that $\varphi(-\tau, y) \in S$. Taking $z = \varphi(-\tau, y)$, it is clear that $z \in S$ and $\varphi(\tau, z) \notin S$.

For sufficiency we show that whenever S is not positively invariant, the sets $\mathrm{Exit}_f(S)$ and $\mathrm{Exit}_{-f}(S^c)$ cannot both be empty. Suppose (for contradiction) that both $\mathrm{Exit}_f(S)$ and $\mathrm{Exit}_{-f}(S^c)$ are empty and that S is not positively invariant. The set of escape points of S is therefore non-empty. Consider an escape point $x \in \mathrm{Escape}_f(S)$: by our hypothesis x cannot be in the empty set of exit points $\mathrm{Exit}_f(S)$. Therefore there exists a positive $t_0 \in I_x$ such that for all $s \in (0, t_0)$ one has $\varphi(s,x) \in S$, and there exists a $t_1 \in I_x$ such that $t_0 \le t_1$ and $\varphi(t_1, x) \notin S$ (i.e. $\varphi(t_1,x) \in S^c$). Let us define

$$T' = \{t \in I_x \cap (0,+\infty) \mid \forall s \in (0,t), \varphi(s,x) \in S\}\,.$$

Under our hypothesis, the set T' is non-empty and has a supremum t' such that $t_0 \le t' \le t_1$. Let us now define

$$T'' = \{t \in I_x \cap (0,+\infty) \mid \varphi(t,x) \notin S\}\,.$$

This set is likewise non-empty (as it contains t_1) and has an infimum t'' such that $t_0 \le t''$. Every element of T'' is an upper bound for T' (otherwise there would exist a time $t \in T''$ at which both

[9] The set of escape points is fundamental to the Ważewski principle. See Conley (1978) where it is denoted as W° for a set W.

$\varphi(t,x) \in S$ and $\varphi(t,x) \notin S$). Clearly, since t' is the least upper bound for T' it can act as a lower bound on T'' and we therefore have $t' \leq t''$, where t'' is the greatest lower bound for T''. Suppose the inequality is strict ($t' < t''$), then for all $r \in [t', t'')$ one has $\varphi(r,x) \in S$ (otherwise t'' is not the greatest lower bound for T''). But then t' cannot be the least upper bound for T' because $\varphi(s,x) \in S$ for $s \in (t', t'')$. Thus $t' = t''$ and we have two cases to consider: either (i) $\varphi(t',x) \in S$, in which case $\varphi(t',x) \in \mathrm{Exit}_f(S)$ and $\mathrm{Exit}_f(S)$ is therefore non-empty, or (ii) $\varphi(t',x) \notin S$, in which case $\varphi(t',x) \in \mathrm{Exit}_{-f}(S^c)$, so $\mathrm{Exit}_{-f}(S^c)$ is non-empty. Both cases give us a contradiction. □

Remark 24. The main technical difference between the proof of Theorem 23 and (Zhan et al., 2017, Thm. 9.1) is that the latter draws a contradiction from considering the supremum of the set T' (with respect to our notations in the proof of Theorem 23) whereas we draw a contradiction by considering in addition the set T''. This is to be expected as the statements of these theorems are slightly different: Theorem 23 complements S then applies the Exit_{-f} operator to S^c, whereas (Zhan et al., 2017, Thm. 9.1) applies the In_{-f} operator to S first then complements the result. This being said, the overall structure of both proofs is however very similar and this fact is better captured by appealing to the real induction principle as a generic proof technique as detailed in Section 3.

Remark 25. Readers with a background in dynamical systems may find it a little counterintuitive that one needs to consider the flow in the reversed system to characterize positive invariance. Indeed, for *closed sets* S it is well known that "local invariance" under the flow φ (viz. emptiness of $\mathrm{Exit}_f(S)$) is equivalent to positive invariance (e.g. see Cârjă et al., 2007, Ch. 4). It is important to remember that Theorem 23 makes no assumptions about the set S being open or closed. When S is open, local invariance holds trivially because the flow may always evolve within the set for some time from any $x \in S$.

Observe that the sets $\mathrm{Exit}_f(S)$ and $\mathrm{Exit}_{-f}(S)$ are not necessarily disjoint: for example, any isolated point which is not an equilibrium would lie in both sets. Neither are they required to cover the boundary ∂S: if S is an equilibrium point, then both $\mathrm{Exit}_f(S)$ and $\mathrm{Exit}_{-f}(S)$ are empty, whereas $\partial S = S$.

The operators Exit_f and In_f respectively capturing the main underlying concepts used in Theorem 6 and Theorem 23 are intimately related.

Lemma 26. *For any set* $S \subseteq \mathbb{R}^n$, $\mathrm{Exit}_f(S) = \mathrm{In}_f(S)^c \cap S$. *Equivalently, one has* $\mathrm{Exit}_f(S)^c \cap S = \mathrm{In}_f(S) \cap S$.

Proof. One has $x \in \mathrm{In}_f(S)^c \cap S$ if and only if $x \in S$, and, for any positive $t \in I_x$, there exists $s \in (0,t)$ such that $\varphi(s,x) \notin S$, otherwise $\varphi(s,x) \in S$ holds for all $s \in (0,t)$ which would mean that $x \in \mathrm{In}_f(S)$. The latter is exactly the definition of $\mathrm{Exit}_f(S)$. □

A symmetric equality holds (only) for closed sets.

Lemma 27. *For a* closed *set* $S \subseteq \mathbb{R}^n$, $\mathrm{In}_f(S) = \mathrm{Exit}_f(S)^c \cap S$.

Proof. If S is a closed set, then the inclusion $\mathrm{In}_f(S) \subseteq S$ holds trivially, from Lemma 26 we have $\mathrm{Exit}_f(S)^c \cap S = \mathrm{In}_f(S) \cap S$ and the result follows. □

Remark 28. According to the above lemmas, while $\mathrm{In}_f(S)$ is sufficient to fully recover $\mathrm{Exit}_f(S)$ by simple set operations. The converse is not true for general sets: the bare knowledge of $\mathrm{Exit}_f(S)$ is not enough to completely recover $\mathrm{In}_f(S)$ unless S is closed. This might seem as a conceptual defect favouring inward sets as more fundamental than exit sets. From a computational standpoint, however, this lack of symmetry between the two concepts turns out to be powerful: intuitively one does not need the full information encoded by inward sets to decide the positive invariance of S. Exit sets, despite carrying less information, are sufficient for this purpose.

Using Lemma 26, both characterizations of positively invariant sets in Theorem 6 and Theorem 23 can be recovered from one another using the following equivalences:

$$\emptyset = \underbrace{\mathrm{In}_f(S)^c \cap S}_{\mathrm{Exit}_f(S)} \iff S \subseteq \mathrm{In}_f(S)\,,$$

$$\emptyset = \underbrace{\mathrm{In}_{-f}(S^c)^c \cap S^c}_{\mathrm{Exit}_{-f}(S^c)} \iff S^c \subseteq \mathrm{In}_{-f}(S^c)\,.$$

The origins of exit sets in Theorem 23 lie in topology and it is the properties of exit sets that make this characterization computationally interesting. The astute reader may remark at this point that Theorem 23 admits a shorter proof using real induction via Lemma 26. This is indeed the case; however, such a proof would not rely on the concept of exit set nor would it expose the topological insights that we wish to call upon later. As we shall see, exit sets afford a very different way of looking at the problem of checking positive invariance and their properties can be exploited to give a substantially different algorithmic solution than that offered by **LZZ** in Section 3.4.

4.1. Properties of exit sets

Let $S_1, S_2 \subseteq \mathbb{R}^n$, we discuss below the distributive properties of Exit_f over set intersection and union.

Lemma 29. $\mathrm{Exit}_f(S_1 \cap S_2) = (\mathrm{Exit}_f(S_1) \cap S_2) \cup (S_1 \cap \mathrm{Exit}_f(S_2))$.

Proof. The inclusion $\mathrm{Exit}_f(S_1 \cap S_2) \supseteq (\mathrm{Exit}_f(S_1) \cap S_2) \cup (\mathrm{Exit}_f(S_2) \cap S_1)$ is immediate: if $x \in \mathrm{Exit}_f(S_1) \cap S_2$, then, for all positive t, there exists a positive $s < t$ such that $\varphi(s,x) \notin S_1$ and therefore $\varphi(s,x) \notin S_1 \cap S_2$. Likewise for $\mathrm{Exit}_f(S_1 \cap S_2) \supseteq \mathrm{Exit}_f(S_2) \cap S_1$. To prove the converse, let $x \in \mathrm{Exit}_f(S_1 \cap S_2)$, then $x \in S_1 \cap S_2$ and for all positive t, there exists a positive $s < t$ such that $\varphi(s,x) \notin S_1 \cap S_2$ which is equivalent to $\varphi(s,x) \notin S_1$ or $\varphi(s,x) \notin S_2$. □

Lemma 30. $\mathrm{Exit}_f(S_1 \cup S_2) \subseteq \big(\mathrm{Exit}_f(S_1) \cap \mathrm{In}_f(S_2)^c\big) \cup \big(\mathrm{In}_f(S_1)^c \cap \mathrm{Exit}_f(S_2)\big)$.

Proof. Let $x \in \mathrm{Exit}_f(S_1 \cup S_2)$, then by definition, for all $t > 0$, there exists $s \in (0,t)$ such that $\varphi(s,x) \notin S_1 \cup S_2$, which is equivalent to $\varphi(s,x) \notin S_1$ and $\varphi(s,x) \notin S_2$. By hypothesis, $x \in S_1 \cup S_2$. If $x \in S_1$ then it has to belong to $\mathrm{Exit}_f(S_1)$ as well as $\mathrm{In}_f(S_2)^c$, by definition of the latter. If $x \in S_2$, we get a symmetric formula by swapping S_1 and S_2, namely $x \in \mathrm{Exit}_f(S_2) \cap \mathrm{In}_f(S_1)^c$. The desired formula is the union of these two cases. □

Counterexample 31. The reverse inclusion of Lemma 30 does not hold in general. Consider the simple 1-dimensional system $x' = 1$ and the sets

$$S_1 = \{0\} \cup \left\{x \in \mathbb{R} \mid x > 0 \wedge \sin\left(x^{-1}\right) = 0\right\}\,,$$

$$S_2 = \{0\} \cup \left\{x \in \mathbb{R} \mid x > 0 \wedge \sin\left(x^{-1}\right) \neq 0\right\}\,.$$

The point 0 belongs to both $\mathrm{Exit}_f(S_1)$ and $\mathrm{Exit}_f(S_2)$. In addition, it does not belong to either $\mathrm{In}_f(S_1)$ or $\mathrm{In}_f(S_2)$. However, 0 is not in $\mathrm{Exit}_f(S_1 \cup S_2)$ as the union ($x \geq 0$) is clearly a positively invariant set for the considered flow.

This simple example highlights the main reason why the inclusion in Lemma 30 cannot in general be replaced with set equality. If $x \in \mathrm{Exit}_f(S_1) \cap \mathrm{In}_f(S_2)^c$, one can only conclude that for any positive ϵ_1, ϵ_2, there exist $t_1 \in (0, \epsilon_1)$ and $t_2 \in (0, \epsilon_2)$ such that $\varphi(t_1, x) \notin S_1$ and $\varphi(t_2, x) \notin S_2$; there is nothing to suggest that t_1 should be equal to t_2, which is required for x to belong to $\mathrm{Exit}_f(S_1 \cup S_2)$. However, if one restricts attention to semi-analytic sets S (which includes semi-algebraic sets) then $\mathrm{In}_f(S^c) =$

$\mathrm{In}_f(S)^c$ (as observed in the previous section), and the inclusion of Lemma 30 becomes an equality. (Notice that semi-analyticity is only sufficient to ensure that $\mathrm{In}_f(S^c) = \mathrm{In}_f(S)^c$. We currently lack a full characterization of the most general topological settings that respect this equality.)

Lemma 32. *Let S_1, S_2 be semi-analytic sets. Then*

$$\mathrm{Exit}_f(S_1 \cup S_2) = \left(\mathrm{Exit}_f(S_1) \cap \mathrm{In}_f(S_2)^c\right) \cup \left(\mathrm{In}_f(S_1)^c \cap \mathrm{Exit}_f(S_2)\right).$$

Proof.

$$\begin{aligned}\mathrm{Exit}_f(S_1 \cup S_2) &= \mathrm{In}_f(S_1 \cup S_2)^c \cap (S_1 \cup S_2)\\ &= (\mathrm{In}_f(S_1)^c \cap \mathrm{In}_f(S_2)^c \cap S_1) \cup (\mathrm{In}_f(S_1)^c \cap \mathrm{In}_f(S_2)^c \cap S_2)\\ &= \left(\mathrm{Exit}_f(S_1) \cap \mathrm{In}_f(S_2)^c\right) \cup \left(\mathrm{Exit}_f(S_2) \cap \mathrm{In}_f(S_1)^c\right). \quad \square\end{aligned}$$

4.2. The **ESE** decision procedure based on Theorem 23

Given a quantifier-free formula describing a semi-algebraic set S and a polynomial system of ODEs $x' = f(x)$, Theorem 23 can be used to algorithmically decide whether S is positively invariant or not with respect to f.

A naïve approach would be to first compute $E = \mathrm{Exit}_f(S) \cup \mathrm{Exit}_{-f}(S^c)$ recursively on the Boolean structures of S and S^c using Lemmas 30 and 32, then check whether E is empty or not. Such an approach would be very similar to the **LZZ** procedure described in section 3.4 and would therefore suffer from the same problem, namely the impossibility of the current state-of-the-art quantifier elimination algorithms to check the emptiness of E in reasonable time, even for seemingly simple planar systems (cf. section 5). Indeed, one experimentally observes that, for many interesting examples, the construction of the set E is not computationally expensive despite requiring several ideal membership tests as, often, the order (with respect to f) of the polynomials involved remains low. An overwhelming share of the running time for a typical problem is spent on proving emptiness of E (as is the case for checking the inclusions $S \subseteq \mathrm{In}_f(S)$ and $S^c \subseteq \mathrm{In}_{-f}(S^c)$ using **LZZ**).

We will see in this section how the concept of exit sets, and more precisely Theorem 23, can be used to overcome this bottleneck in a principled way. The main idea is to "chop the set E into smaller pieces" (chunks) on which the emptiness test can be performed in a divide-and-conquer fashion, instead of constructing a formula characterizing E first and only then checking for its emptiness. What is perhaps more interesting is that Theorem 23 suggests a natural way of splitting E into chunks in such a way that each chunk involves precisely *one* exit set of an atomic formula. This, in turn, allows one to exploit topological properties of atomic formulas, such as openness, in order to check for set emptiness *syntactically*, obviating the need for expensive computations such as real quantifier elimination.

As in the previous sections, we use the same notation for semi-algebraic sets and their formal representations as quantifier-free formulas of real arithmetic. Without loss of generality, we also restrict our attention to the atomic formulas, $p < 0$ and $p = 0$, where p is a polynomial. The formulas $p \leq 0$ and $p \neq 0$, are syntactic sugar for $(p < 0 \vee p = 0)$ and $(-p < 0 \vee p < 0)$ respectively. Similarly, $p > 0$, $p \geq 0$ can be encoded as $-p < 0$, $-p \leq 0$ respectively.

The exit sets of **F**, **T**, and $p < 0$ are all empty (by Lemma 22) as the sets defined by these formulas are open. According to the same lemma, the exit set of $p = 0$ necessarily lies on its boundary, which is also given by $p = 0$. When the first Lie derivative of p does not vanish on $p = 0$, the flow necessarily leaves the set for some positive time. The same reasoning applies for higher-order Lie derivatives. As with the construction of In_f in Section 3.4, the construction of the exit set of $p = 0$ is fully captured by a (finite) formula:

$$\begin{aligned}\mathrm{Exit}_f(p = 0) \equiv \big(\, & p = 0 \wedge p' \neq 0\\ \vee\, & p = 0 \wedge p' = 0 \wedge p'' \neq 0\end{aligned}$$

$$\begin{aligned}&\vdots\\ &\vee\, p=0 \wedge p'=0 \wedge p''=0 \wedge \cdots \wedge p^{(\mathrm{ord}_f(p))} \neq 0\big)\,.\end{aligned}$$

Note that Lemma 16 also applies to $\mathrm{Exit}_f(p=0)$ and the remainders rem_i (as defined in the lemma) can be used instead of the Lie derivatives $p^{(i)}$. In summary, the exit set of atomic formulas can be constructed using a procedure Exit_f which is defined as follows:

$$\begin{aligned}
\mathrm{Exit}_f(\mathbf{F}) &:= \mathbf{F}\,,\\
\mathrm{Exit}_f(\mathbf{T}) &:= \mathbf{F}\,,\\
\mathrm{Exit}_f(p<0) &:= \mathbf{F}\,,\\
\mathrm{Exit}_f(p=0) &:= \big(\,\mathrm{rem}_0 = 0 \wedge \mathrm{rem}_1 \neq 0\\
&\qquad\quad \vee\, \mathrm{rem}_0 = 0 \wedge \mathrm{rem}_1 = 0 \wedge \mathrm{rem}_2 \neq 0\\
&\qquad\quad \vdots\\
&\qquad\quad \vee\, \mathrm{rem}_0 = 0 \wedge \mathrm{rem}_1 = 0 \wedge \cdots \wedge \mathrm{rem}_{\mathrm{ord}_f(p)} \neq 0\big)\,.
\end{aligned}$$

Thus, the only non-trivial exit set for atomic formulas is the exit set of an equality as it is the only (atomic) closed set.

We next define a recursive procedure called $\mathrm{NonEmpty}_f$, parametrized by the vector field f, and which takes as its arguments two quantifier-free real arithmetic formulas describing semi-algebraic sets S and R. It is defined as follows (A denotes an atomic formula):

$$\begin{aligned}
\mathrm{NonEmpty}_f(A,\ R) &:= \mathrm{Reduce}\left(\exists x_1.\ldots.\exists x_n.\ \mathrm{Exit}_f(A) \wedge R\right)\,,\\
\mathrm{NonEmpty}_f(S_1 \wedge S_2,\ R) &:= \mathrm{NonEmpty}_f(S_1,\ S_2 \wedge R)\\
&\quad\ \vee \mathrm{NonEmpty}_f(S_2,\ S_1 \wedge R)\,,\\
\mathrm{NonEmpty}_f(S_1 \vee S_2,\ R) &:= \mathrm{NonEmpty}_f(S_1, \neg\mathrm{In}_f(S_2) \wedge R)\\
&\quad\ \vee \mathrm{NonEmpty}_f(S_2,\ \neg\mathrm{In}_f(S_1) \wedge R)\,,\\
\mathrm{NonEmpty}_f(\neg S,\ R) &:= \mathrm{NonEmpty}_f(\mathrm{Neg}(S),\ R)\,.
\end{aligned}$$

In addition to Exit_f, $\mathrm{NonEmpty}_f$ relies on three other procedures: In_f (already defined in Section 3.4), Neg, and Reduce. The procedure Neg applies negation $\neg$ to the formula it receives as its argument (but does *not* recursively apply negation to the sub-formulas). For atomic formulas, Neg simply negates the formula, expressing the result in terms of only the basic forms of atomic formulas ($\mathbf{T}$, $\mathbf{F}$, $p<0$, and $p=0$):

$$\begin{aligned}
\mathrm{Neg}(\mathbf{F}) &:= \mathbf{T}\,,\\
\mathrm{Neg}(\mathbf{T}) &:= \mathbf{F}\,,\\
\mathrm{Neg}(p<0) &:= (-p<0) \vee (-p=0)\,,\\
\mathrm{Neg}(p=0) &:= (-p<0) \vee (p<0)\,.
\end{aligned}$$

For non-atomic formulas Neg simply applies De Morgan's laws and eliminates double negation:

$$\begin{aligned}
\mathrm{Neg}(S_1 \wedge S_2) &:= (\neg S_1) \vee (\neg S_2)\,,\\
\mathrm{Neg}(S_1 \vee S_2) &:= (\neg S_1) \wedge (\neg S_2)\,,\\
\mathrm{Neg}(\neg S) &:= S\,.
\end{aligned}$$

The procedure Reduce checks for emptiness of the semi-algebraic set by performing real quantifier elimination (this functionality is offered e.g. by implementations of CAD (Collins and Hong, 1991); however, there exist alternatives which are not based on CAD, e.g. RAGLib (Safey El Din, 2017)).

In a nutshell, the main purpose of $\mathrm{NonEmpty}_f$ is to *recursively* check for emptiness of exit sets, as stated more formally in the following lemma.

Lemma 33. *Let S and R be two formulas describing semi-algebraic sets. Then* $\mathrm{NonEmpty}_f(S, R)$ *returns False if and only if* $\mathrm{Exit}_f(S) \cap R$ *is empty.*

Proof. The proof is by induction on the depth of formula S. Base case: if $S \in \{\mathbf{F}, \mathbf{T}, p < 0, p = 0\}$, then $\mathrm{NonEmpty}_f(S, R)$ is

$$\mathrm{Reduce}\left(\exists x_1. \dots \exists x_n.\ \mathrm{Exit}_f(S) \wedge R\right) ,$$

which is False if and only if $\mathrm{Exit}_f(S) \cap R$ is empty (we freely interchange $\wedge$ and $\cap$ as well as the empty set and False as mentioned in Remark 13).

For the inductive hypothesis, suppose the property holds for all formulas of depth less than or equal to k and let S_1, S_2, and S' be such formulas.

If $S = S_1 \wedge S_2$, then by definition $\mathrm{NonEmpty}_f(S_1 \wedge S_2, R)$ is False if and only if both $\mathrm{NonEmpty}_f(S_1, S_2 \wedge R)$ and $\mathrm{NonEmpty}_f(S_2,\ S_1 \wedge R)$ are False. By the induction hypothesis, this means that both $\mathrm{Exit}_f(S_1) \wedge (S_2 \wedge R)$ and $\mathrm{Exit}_f(S_2) \wedge (S_1 \wedge R)$ are empty, and therefore their union is also empty. One gets the desired result by factoring out R then using Lemma 29:

$$\begin{aligned} \emptyset &= \left(\mathrm{Exit}_f(S_1) \cap (S_2 \cap R)\right) \cup \left(\mathrm{Exit}_f(S_2) \cap (S_1 \cap R)\right) \\ &= \left((\mathrm{Exit}_f(S_1) \cap S_2) \cup (\mathrm{Exit}_f(S_2) \cap S_1)\right) \cap R \\ &= \mathrm{Exit}_f(S_1 \cap S_2) \cap R\,. \end{aligned}$$

The disjunctive case can be proved similarly using Lemma 32.

Finally, if $S = \neg S'$, $\mathrm{NonEmpty}_f(S, R) = \mathrm{NonEmpty}_f(\mathrm{Neg}(S'), R)$ and one may eliminate all negations from $\mathrm{Neg}(S')$ by applying De Morgan's laws and double negation elimination and finally applying Neg to any remaining negated atoms. Since the property holds for atomic formulas, conjunctions and disjunctions, it holds for S as well. □

The procedure $\mathrm{NonEmpty}_f$ can thus be used to check positive invariance as an immediate corollary of Theorem 23 and Lemma 33 by setting R to $\mathbf{T}$.

Theorem 34. *A semi-algebraic set S is positively invariant for a system of ODEs* $x' = f(x)$ *if and only if* $\neg\left(\mathrm{NonEmpty}_f(S, \mathbf{T})\ \vee\ \mathrm{NonEmpty}_{-f}(\neg S, \mathbf{T})\right)$.

Accordingly, we define the *Exit Set Emptiness* (**ESE**) decision procedure that checks for positive invariance of S with respect to f as

$$\mathbf{ESE}(S, f) := \neg\left(\mathrm{NonEmpty}_f(S, \mathbf{T})\ \vee\ \mathrm{NonEmpty}_{-f}(\neg S, \mathbf{T})\right) .$$

4.3. Complexity analysis

For given formulas S and R, in order to check the emptiness of $\mathrm{Exit}_f(S) \cap R$, the procedure $\mathrm{NonEmpty}_f(S, R)$ performs several calls to Reduce in order to eliminate existential quantifiers. The number of such calls depends only on the Boolean structure of S, in particular, the second argument R plays no role in the way the procedure operates. In this section, we first give upper and lower bounds of the number of such calls as a measure of the impact of the encoding of S. We then discuss further decompositions of $\mathrm{Exit}_f(S)$ as a union of *basic* semi-algebraic sets. Recall that a basic semi-algebraic set is a set described by a conjunction of atomic formulas $\bigwedge_i (p_i \bowtie_i 0)$, where $\bowtie_i \in \{<, =\}$ and p_i are polynomials.

Proposition 35. *Suppose the set S is characterized by a formula in disjunctive normal form (DNF) $\bigvee_{i=1}^{k} \bigwedge_{j=1}^{m_i} A_{ij}$, where A_{ij} are atomic formulas. Let $m = \max_i m_i$. Then the recursion depth of* $\text{NonEmpty}_f(S, \mathbf{T})$ *is bounded by $k + m$ and the number of calls to* Reduce *is $\sum_{i=1}^{k} m_i \leq km$, each of which has the form* $\text{Reduce}\,\exists x_1 \ldots \exists x_n.\text{Exit}_f(A_{rs}) \wedge R_{rs}$*, where*

$$R_{rs} \equiv \bigwedge_{j=1, j\neq s}^{m_r} A_{rj} \wedge \neg\text{In}_f \left(\bigvee_{i=1, i\neq r}^{k} \bigwedge_{j=1}^{m_i} A_{ij} \right) .$$

Proof. The form of the real quantifier elimination (QE) problems is immediate from the definition of NonEmpty_f. The equivalence of R_{rs} is obtained by using the distributive properties (over disjunctions and conjunctions) of the In_f operator. □

For instance, suppose $S \equiv (A_{11} \wedge A_{12}) \vee A_{21} \vee A_{31}$ ($k = 3$, $m = m_1 = 2$, $m_2 = m_3 = 1$). Then, in the worst case, the procedure $\text{NonEmpty}_f(S, \mathbf{T})$ has to call Reduce 4 times:

$$\text{Reduce}\,\exists x_1 \ldots \exists x_n.\, \text{Exit}_f(A_{11}) \wedge A_{12} \wedge \neg\text{In}_f(A_{21} \vee A_{31}) \,,$$
$$\text{Reduce}\,\exists x_1 \ldots \exists x_n.\, \text{Exit}_f(A_{12}) \wedge A_{11} \wedge \neg\text{In}_f(A_{21} \vee A_{31}) \,,$$
$$\text{Reduce}\,\exists x_1 \ldots \exists x_n.\, \text{Exit}_f(A_{21}) \wedge \neg\text{In}_f((A_{11} \wedge A_{12}) \vee A_{31}) \,,$$
$$\text{Reduce}\,\exists x_1 \ldots \exists x_n.\, \text{Exit}_f(A_{31}) \wedge \neg\text{In}_f((A_{11} \wedge A_{12}) \vee A_{21}) \,.$$

Proposition 36. *Suppose the set S is characterized by a formula in conjunctive normal form (CNF) $\bigwedge_{i=1}^{k} \bigvee_{j=1}^{m_i} A_{ij}$ where A_{ij} are atomic formulas, and let $m = \max_i m_i$. Then the recursion depth of* $\text{NonEmpty}_f(S, \mathbf{T})$ *is bounded by $k + m$ and the number of calls to* Reduce *is $\sum_{i=1}^{k} m_i \leq km$, each of which has the form* $\text{Reduce}\,\exists x_1 \ldots \exists x_n.\text{Exit}_f(A_{rs}) \wedge R_{rs}$*, where*

$$R_{rs} \equiv \neg\text{In}_f \left(\bigwedge_{j=1, j\neq s}^{m_r} A_{rj} \right) \wedge \bigwedge_{i=1, i\neq r}^{k} \bigvee_{j=1}^{m_i} A_{ij} \,.$$

For instance, suppose $S \equiv (A_{11} \vee A_{12}) \wedge A_{21} \wedge A_{31}$, ($k = 3$, $m = m_1 = 2$, $m_2 = m_3 = 1$). Then, in the worst case, the procedure $\text{NonEmpty}_f(S, \mathbf{T})$ has to call Reduce 4 times:

$$\text{Reduce}\,\exists x_1 \ldots \exists x_n.\, \text{Exit}_f(A_{11}) \wedge \neg\text{In}_f(A_{12}) \wedge (A_{21} \wedge A_{31}) \,,$$
$$\text{Reduce}\,\exists x_1 \ldots \exists x_n.\, \text{Exit}_f(A_{12}) \wedge \neg\text{In}_f(A_{11}) \wedge (A_{21} \wedge A_{31}) \,,$$
$$\text{Reduce}\,\exists x_1 \ldots \exists x_n.\, \text{Exit}_f(A_{21}) \wedge ((A_{11} \wedge A_{12}) \vee A_{31}) \,,$$
$$\text{Reduce}\,\exists x_1 \ldots \exists x_n.\, \text{Exit}_f(A_{31}) \wedge ((A_{11} \wedge A_{12}) \vee A_{21}) \,.$$

Remark 37. Suppose $S \equiv \bigvee_{i=1}^{k} \bigwedge_{j=1}^{m_i} A_{ij}$ and let S' denote the same formal expression as S except that $\vee$ and $\wedge$ are swapped. Then the QE problems that $\text{NonEmpty}_f(S', \mathbf{T})$ has to solve could be obtained syntactically from those of $\text{NonEmpty}_f(S, \mathbf{T})$ by swapping A_{ij} and $\neg\text{In}_f(A_{ij})$ (and leaving $\text{Exit}_f(A_{ij})$ untouched).

The encoding of the set S to be checked may have a significant impact on the number of calls to Reduce in $\text{NonEmpty}_f(S, \mathbf{T})$. For instance, suppose S is encoded as $S_1 \equiv (A_1 \vee (A_2 \wedge A_3)) \wedge (A_4 \vee (A_2 \wedge A_3))$ where the A_i are atomic formulas. Then $\text{NonEmpty}_f(S_1, \mathbf{T})$ calls Reduce 6 times. In this case, none of the upper bounds of Propositions 35 nor 36 apply because S_1 is neither in DNF nor in CNF. If one uses the equivalent (DNF) encoding $S_2 \equiv (A_1 \wedge A_4) \vee (A_2 \wedge A_3)$ for S, then $\text{NonEmpty}_f(S_2, \mathbf{T})$ calls Reduce only 4 times at most.

Lemma 38. *The number of calls to* Reduce *is bounded below by the number of distinct atomic formulas in S (regardless of the encoding of S).*

Proof. The procedure $\mathrm{NonEmpty}_f$ requires one call to Reduce for each problem of the form $\mathrm{Exit}_f(A) \wedge R$ (where A is an atomic formula), and R any arbitrary formula. Depending on the encoding of S, $\mathrm{NonEmpty}_f$ might call Reduce once for $\mathrm{Exit}_f(A) \wedge (R_1 \vee R_2)$, or twice for $\mathrm{Exit}_f(A) \wedge R_1$ and $\mathrm{Exit}_f(A) \wedge R_2$ separately. In the best case, the encoding of S is such that each call to Reduce features a distinct $\mathrm{Exit}_f(A)$ (otherwise, the several calls with the same $\mathrm{Exit}_f(A)$ can be factored out), and the result follows. □

An interesting open question is whether there exists a systematic way of finding an encoding of S which always results in the minimal number of calls to Reduce that is possible. We leave this question open while observing that one can build simple examples for which neither the DNF nor the CNF encoding of S are adequate in this regard (it suffices to consider encodings with redundant atomic formulas).

The QE problems to solve in Proposition 35 can be split further (by distributivity) into $\prod_{i=1, i\neq r}^{k} m_i \leq m^{k-1}$ "smaller" problems of the form

$$\text{Reduce } \exists x_1 \ldots \exists x_n.\ \mathrm{Exit}_f(A_{rs}) \wedge \bigwedge_{j=1, j\neq s}^{m_r} A_{rj} \wedge \bigwedge_{i=1, i\neq r}^{k} \neg \mathrm{In}_f(A_{i\ell_i}) .$$

Likewise, the QE problems to solve in Proposition 36 can be split further into $\prod_{i=1, i\neq r}^{k} m_i \leq m^{k-1}$ problems of the form

$$\text{Reduce } \exists x_1 \ldots \exists x_n.\ \mathrm{Exit}_f(A_{rs}) \wedge \bigwedge_{j=1, j\neq s}^{m_r} \neg \mathrm{In}_f(A_{rj}) \wedge \bigwedge_{i=1, i\neq r}^{k} A_{i\ell_i} .$$

We could further evaluate Exit_f and In_f for atomic formulas. To do so, one has to account for the system of ODEs $x' = f(x)$ as well as the order of the involved polynomials with respect to f. Let $\deg(p)$ denote the (total) degree of a polynomial p, and $\deg(f)$ the maximum degree of the polynomials appearing in the right-hand side of $x' = f(x)$. Recall that the degree of p', the first (Lie) derivative of p with respect to f, has a total degree which is at most $\deg(p) + (\deg(f) - 1)$, and the degree of $p^{(s)}$ is at most $\deg(p) + s(\deg(f) - 1)$. Recall that $\mathrm{ord}_f(p)$ denotes the order of p with respect to f.

The set $\mathrm{Exit}_f(p \bowtie 0)$ is the union of $\mathrm{ord}_f(p)$ basic semi-algebraic sets, whereas $\mathrm{In}_f(p \bowtie 0)$ is the union of $\mathrm{ord}_f(p) + 1$ basic semi-algebraic sets.

Lemma 39. *Let p_i, $1 \leq i \leq m$, and q_j, $1 \leq j \leq k$, denote some polynomials and let ρ denote the maximum of their respective order with respect to f. The expression*

$$\mathrm{Exit}_f(p_1 \bowtie_1 0) \wedge \bigwedge_{i=2}^{m} (p_i \bowtie_i 0) \wedge \bigwedge_{j=1}^{k} \mathrm{In}_f\big(q_j \bowtie_j 0\big)$$

is the union of at most $\rho(\rho+1)^k$ basic semi-algebraic sets. Each basic semi-algebraic set is a conjunction of at most $m - 1 + (k+1)(\rho+1)$ expressions of the form $p \bowtie 0$.

Proof. The expression is a union of at most $\mathrm{ord}_f(p_1) \prod_{j=1}^{k} (\mathrm{ord}_f(q_j) + 1)$ basic semi-algebraic sets. From which one immediately deduces the $\rho(\rho+1)^k$ upper bound. Each basic semi-algebraic set is a conjunction of at most $(\mathrm{ord}_f(p_1) + 1) + (m-1) + \sum_{j=1}^{k} (\mathrm{ord}_f(q_j) + 1) \leq m + k + (k+1)\rho$ literals. □

For instance, $\mathrm{Exit}_f(p_1 = 0) \wedge (p_2 < 0) \wedge \mathrm{In}_f(q < 0)$ where $\mathrm{ord}_f(p_1) = \mathrm{ord}_f(q) = 2$, (thus $m = 2$, $k = 1$, and $\rho = 2$) is the following union

$$\begin{aligned}
& p_1 = 0 \wedge p_1' \neq 0 \wedge p_2 < 0 \wedge q < 0 \\
\vee\ & p_1 = 0 \wedge p_1' \neq 0 \wedge p_2 < 0 \wedge q = 0 \wedge q' < 0 \\
\vee\ & p_1 = 0 \wedge p_1' \neq 0 \wedge p_2 < 0 \wedge q = 0 \wedge q' = 0 \wedge q'' < 0 \\
\vee\ & p_1 = 0 \wedge p_1' = 0 \wedge p_1'' \neq 0 \wedge p_2 < 0 \wedge q < 0 \\
\vee\ & p_1 = 0 \wedge p_1' = 0 \wedge p_1'' \neq 0 \wedge p_2 < 0 \wedge q = 0 \wedge q' < 0 \\
\vee\ & p_1 = 0 \wedge p_1' = 0 \wedge p_1'' \neq 0 \wedge p_2 < 0 \wedge q = 0 \wedge q' = 0 \wedge q'' < 0 \,.
\end{aligned}$$

Theorem 40. *Let S be a semi-algebraic set encoded either as $\bigwedge_{i=1}^{k} \bigvee_{j=1}^{m_i} (p_{ij} \bowtie_{ij} 0)$ (DNF) or as $\bigvee_{i=1}^{k} \bigwedge_{j=1}^{m_i} (p_{ij} \bowtie_{ij} 0)$ (CNF) for some polynomials p_{ij}. Let $m = \max_i m_i$, $d = \max_{i,j} \deg(p_{ij})$, and $\rho = \max_{i,j} \operatorname{ord}_f(p_{ij})$. Then $\operatorname{Exit}_f(S) \vee \operatorname{Exit}_{-f}(\neg S)$ is a union of at most $km^k \rho(\rho+1)^{k-1}$ basic semi-algebraic sets*

$$q_1 \bowtie_1 0 \wedge \ldots \wedge q_s \bowtie_s 0 \,,$$

where $s \leq m - 1 + k(\rho+1)$ and $\deg(q_j) \leq d + \rho(\deg(f) - 1)$.

Proof. Suppose $S \equiv \bigvee_{i=1}^{k} \bigwedge_{j=1}^{m_i} (p_{ij} \bowtie_{ij} 0)$ (the same reasoning applies when S is in CNF). Thus $\neg S \equiv \bigwedge_{i=1}^{k} \bigvee_{j=1}^{m_i} \neg(p_{ij} \bowtie_{ij} 0)$. According to Propositions 35 and 36, $\operatorname{Exit}_f(S)$ is a union of at most km^k basic semi-algebraic sets, each involving $\operatorname{Exit}_f(p_{ij} \bowtie_{ij} 0)$, whereas $\operatorname{Exit}_{-f}(\neg S)$ is the union of at most km^k basic semi-algebraic sets, each involving $\operatorname{Exit}_{-f} \neg(p_{ij} \bowtie_{ij} 0)$. If $p_{ij} \bowtie_{ij} 0$ encodes a closed set, then its negation encodes an open set (and vice versa). Thus at least one of the expressions

$$\operatorname{Exit}_f(p_{rs} \bowtie_{rs} 0) \wedge \bigwedge_{j=1, j\neq s}^{m_r} (p_{rj} \bowtie_{rj} 0) \wedge \bigwedge_{i=1, i\neq r}^{k} \neg \operatorname{In}_f(p_{i\ell_i} \bowtie_{i\ell_i} 0)$$

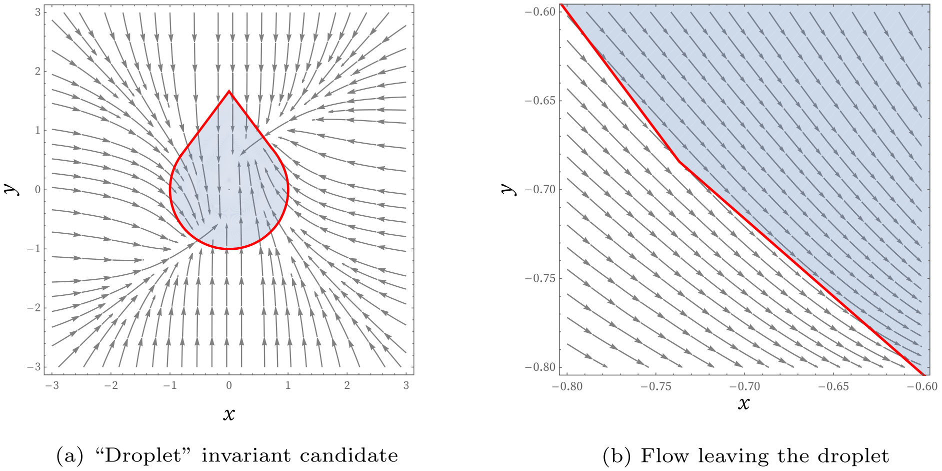
or

$$\operatorname{Exit}_{-f} \neg(p_{rs} \bowtie_{rs} 0) \wedge \bigwedge_{j=1, j\neq s}^{m_r} \operatorname{In}_{-f}(p_{rj} \bowtie_{rj} 0) \wedge \bigwedge_{i=1, i\neq r}^{k} \neg(p_{i\ell_i} \bowtie_{i\ell_i} 0)$$

reduces to False syntactically, and the total number of basic semi-algebraic sets is therefore km^k. Now, according to Lemma 39, each of the above expressions is the union of at most $\rho(\rho+1)^{k-1}$ basic semi-algebraic sets (after evaluating In_f and Exit_f for atomic formulas). Thus $\operatorname{Exit}_f(S) \vee \operatorname{Exit}_{-f}(\neg S)$ is the union of at most $km^k \rho(\rho+1)^{k-1}$ basic semi-algebraic sets, as stated. The bounds on the total number of the involved polynomials as well as their degrees are direct consequences of Lemma 39 and of the bound on the total degree of high-order Lie derivatives, namely $d + \rho(\deg(f) - 1)$. □

The main conclusion from the analysis performed in this section is the following: instead of solving one large real quantifier elimination problem which results from a naïve application of Theorems 6 and 23 (coarse granularity), it is instead possible to solve exponentially many (precisely $km^k \rho(\rho+1)^{k-1}$) smaller real quantifier elimination problems as in Theorem 40; these smaller problems furthermore only involve basic semi-algebraic sets (fine granularity).

In theory, there exist decision procedures for deciding universally (or existentially) quantified sentences of real arithmetic that have singly exponential worst case complexity $(sd)^{O(n)}$, where s is the number of polynomials, d their maximum degree and n the number of variables (Grigor'ev, 1988). Each of the smaller QE problems features fewer polynomials with a lower maximum degree than the original QE problem. The potential gain in complexity is however mitigated by the number of these small problems, which is exponential as stated in Theorem 40.



(a) “Droplet” invariant candidate

(b) Flow leaving the droplet

Fig. 1. Checking positive invariance.

The procedure **ESE**, as defined in Section 4.2, seeks a trade-off between the fine and coarse granularities which translates into a trade-off between the computational cost of QE problems versus the number of QE problems to solve. Combined with the syntactic reductions to False of $\text{Exit}_f(A)$ whenever A is an atomic formula encoding an open set, the concept of exit sets provides a powerful tool from a computational standpoint – in addition to its ability to characterize positively invariant sets in full generality as stated in Theorem 23.

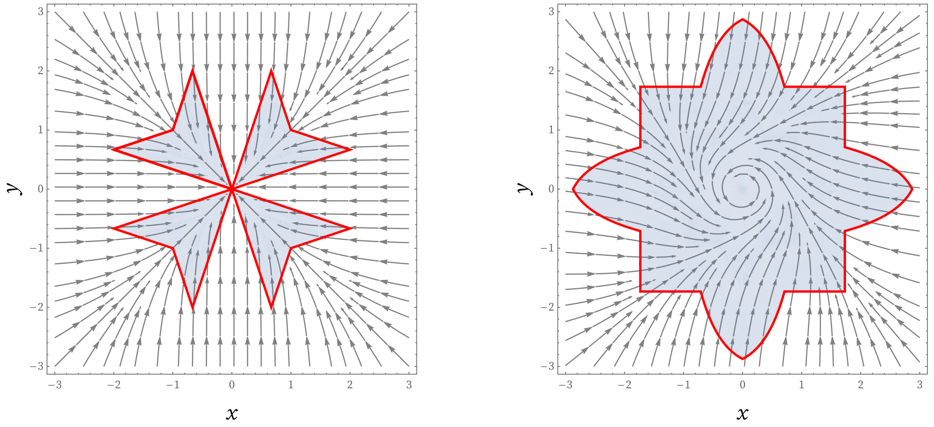
The next section provides some examples that are out of reach for **LZZ** (see Section 3.4) and where **ESE** (see Section 4.2) succeeds in deciding set positive invariance. Notice that, although one can divide the QE problem in **LZZ** into basic semi-algebraic sets, such an approach will not benefit from the syntactic reductions to False offered by Exit_f (without paying an extra computational overhead to detect such cases).

5. Experiments

For checking positive invariance of sets described by a single atomic formula (e.g. $p < 0$), there is no discernible difference in performance between the **LZZ** and **ESE** procedures. However, there is a very palpable difference between the two procedures when checking positive invariance of sets described by more interesting formulas with non-trivial Boolean structure. The examples below serve to illustrate this difference.

Example 41. Consider the non-linear system $x' = -x^3$, $y' = -y^3 + x$. To construct a semi-algebraic set with non-trivial Boolean structure, let us consider the sequence of points obtained from a *rational parametrization* of the unit circle $x^2 + y^2 = 1$, e.g. a sequence of points $(x_t, y_t) = (\frac{2t}{t^2+1}, -\frac{1-t^2}{t^2+1}) \in \mathbb{Q}^2$. From the arithmetic sequence of rational numbers $t_0 = -2$, $t_{n+1} = t_n + \frac{1}{8}$ with t in the range $[-2, 2]$, we can construct a sequence of half-planes that include the unit disc centred at the origin and are tangent to the unit circle at the points (x_t, y_t). The intersection of these half-planes results in a droplet-like shape shown in Fig. 1a and is characterized by a formula S which is a conjunction of 36 linear inequalities.

By inspecting the phase portrait of the system in Fig. 1a, the set defined by this formula appears to be positively invariant, which is something we should be able to check using the procedures described in the previous sections. Checking positive invariance of S using our implementation of **ESE** returns



(a) Semi-linear invariant

(b) Semi-algebraic invariant

Fig. 2. Positive invariants.

False within 0.3 seconds.[10] Indeed, while it is difficult to see from inspecting Fig. 1a, a closer examination (Fig. 1b) reveals that the set characterized by S is not positively invariant because the flow does in fact leave the droplet region. On the other hand, no answer to this positive invariance question could be obtained using **LZZ** within reasonable time (> 4 hours).

Example 42. Now let us consider the system $x' = -x^3,\ \ y' = -y^3$ and the set corresponding to the tilted Maltese cross in Fig. 2a, which, unlike the previous example, is *not* described by a purely conjunctive formula, but is instead given by a disjunction of 4 formulas describing the arms of the cross (each arm is described by a formula of the form $p_1 \leq 0 \wedge p_2 \leq 0 \wedge (p_3 \leq 0 \vee p_4 \leq 0)$, where each $p_{i=1,2,3,4}$ is linear). For this example, one can verify that the set is indeed a positive invariant using **ESE**, which returns True within 164 seconds. Once more, no answer could be obtained using **LZZ** within reasonable time (> 4 hours).

The set shown in Fig. 2a is *semi-linear* because its formal description only features polynomials of maximum degree 1. Fig. 2b illustrates a semi-algebraic set which is not semi-linear, featuring quadratic polynomials in its formal description; the vector field shown in Fig. 2b corresponds to $x' = -x^3 - y,\ \ y' = -y^3 + x$. Using **ESE** we are able to check (within 7 seconds) that the set is indeed positively invariant under the flow of the system, whereas **LZZ** produces the same answer in over 30 minutes.

6. Positive invariants under constraints

In addition to the standard notion of set positive invariance (as given in Definition 1), more general notions have been considered. For example *continuous invariance*, as it is known in the formal verification literature (see e.g. Platzer and Clarke, 2008; Liu et al., 2011), extends positive invariance to accommodate cases in which there is a *constraint* (given by some $Q \subseteq \mathbb{R}^n$) imposed on the evolution of the system.

Definition 43 *(Continuous invariant).* A set $S \subseteq \mathbb{R}^n$ is a *continuous invariant* under evolution constraint $Q \subseteq \mathbb{R}^n$ if and only if the following holds:

$$\forall\, x \in S.\, \forall\, t \geq 0.\big((\forall\, \tau \in [0,t].\ \varphi(\tau, x) \in Q) \to \varphi(t, x) \in S\big)\,.$$

[10] Using Mathematica 12.0, running on a machine with an Intel Core i5-7300U CPU clocked at 2.6 GHz with 16 GB of RAM.

Essentially, in a *continuous invariant* positive invariance is predicated on the constraint Q being maintained. Thus, positive invariance may be regarded as a special case of *continuous invariance* as defined above, i.e. the special case where the constraint Q is all of $\mathbb{R}^n$.

Remark 44. Readers familiar with temporal logics such as LTL may think of continuous invariance as (very loosely speaking) being in a certain sense analogous to temporal modal operators such as Weak Until (**W**), i.e. one may think of a continuous invariant described by formula S subject to evolution constraint described by Q as satisfying the temporal logic formula $S \mathbf{W} \neg Q$. Of course, the semantics of such a formula needs to be defined over the trajectories of the continuous system rather than discrete traces, e.g. as is done in Signal Temporal Logic (STL, see Maler and Nickovic, 2004).

The work of Liu et al. (2011) was developed in this slightly more general setting of continuous invariance, rather than positive invariance. A semi-algebraic set S subject to a semi-algebraic evolution constraint Q is a continuous invariant of the system $x' = f(x)$ if and only if (Liu et al., 2011, Thm. 19): $S \cap Q \cap \mathrm{In}_f(Q) \subseteq \mathrm{In}_f(S)$ and $S^c \cap Q \cap \mathrm{In}_{-f}(Q) \subseteq \mathrm{In}_{-f}(S)^c$.

The **ESE** algorithm introduced in this article is likewise easily lifted to check continuous invariance.

Theorem 45. *A semi-algebraic set S is a continuous invariant for a system of ODEs $x' = f(x)$ subject to a semi-algebraic evolution constraint Q if and only if* $\neg\big(\mathrm{NonEmpty}_f(S, Q \setminus \mathrm{Exit}_f(Q)) \vee \mathrm{NonEmpty}_{-f}(\neg S, Q \setminus \mathrm{Exit}_{-f}(Q))\big)$.

The main difference with respect to Theorem 34, is that instead of considering the entire space $\mathbb{R}^n$ for both forward and backward flows, we focus on $Q \setminus \mathrm{Exit}_f(Q))$ (which is equivalent to $Q \cap \mathrm{In}_f(Q)$ by Lemma 26) for the forward flow and $Q \setminus \mathrm{Exit}_{-f}(Q)$ (or equivalently $Q \cap \mathrm{In}_{-f}(Q)$) for the backward flow. These formulations make explicit the fact that the states from which the flow exits Q (formally captured by $\mathrm{Exit}_f(Q)$) are not relevant for checking continuous invariance and are thus removed from Q. Said differently, by construction, the set $\mathrm{Exit}_f(Q)$ (resp. $\mathrm{Exit}_{-f}(Q)$) is considered a positive (resp. negative) invariant set relative to Q.

6.1. Discrete abstractions of continuous systems

Problems involving positive invariance checking under evolution constraints (i.e. continuous invariance in the sense of Definition 43) arise frequently in the area of formal verification. Invariants described using formulas with non-trivial Boolean structure are particularly important to verification methods based on *discrete abstractions* of continuous dynamical systems (Sogokon et al., 2016). Briefly, discrete abstraction involves partitioning the state space (e.g. $\mathbb{R}^n$) into disjoint sets that correspond to equivalence classes representing states in a discrete transition system. For example, such a partitioning can be obtained from an *algebraic decomposition* of $\mathbb{R}^n$ using a finite set of polynomials $\{p_1, \dots, p_k\}$. Each cell of this decomposition is described by a conjunction of sign conditions on these polynomials, e.g. the formula $S \equiv p_1 > 0 \wedge p_2 = 0 \wedge \cdots \wedge p_k < 0$ describes a cell (which is a basic semi-algebraic set corresponding to a single discrete state in the abstraction). Discrete abstractions of continuous systems are obtained by constructing a discrete transition relation between the discrete states. An abstraction is said to be *sound* if the absence of a discrete transition from the state described by S_i to another state described by S_j in the transition relation implies that the continuous system cannot evolve from any state within the set S_i to any state within S_j without leaving the union $S_i \cup S_j$; an abstraction is said to be *exact* if the presence of such a transition implies the existence of a trajectory which starts at a state within S_i and reaches some state in S_j without leaving the union $S_i \cup S_j$ in the process. In order to construct the transition relation for a sound and exact discrete abstraction one considers the union of neighbouring cells S_i and S_j in the algebraic decomposition and checks whether the set described by S_j is a continuous invariant subject to the constraint $S_i \vee S_j$. There can be no transition from cell S_i to S_j in the discrete transition relation if and only if S_j is continuous invariant under constraint $S_i \vee S_j$ in the sense of Definition 43. Naturally, the Boolean structure of the formulas involved make the construction of discrete abstractions a potentially fruitful area of application for the **ESE** algorithm.

7. Related work

The method of applying the ascending chain condition to ideals generated by successive Lie derivatives of polynomials in order to prove invariance of algebraic varieties in polynomial vector fields was employed by Novikov and Yakovenko (1999), Ghorbal and Platzer (2014), and more recently by Harms et al. (2017). Liu et al. (2011) were the first to address positive invariance of semi-algebraic sets using techniques described in Section 3 of this article. Dowek (2003) investigated the use of real induction to solve kinematic problems involving ODEs.

Platzer and Tan (2020) recently developed a system of formal axioms (one of which formalizes the real induction principle) for reasoning about continuous invariants in differential dynamic logic. This axiomatization is *complete* in the sense that a formal proof of continuous invariance of a *semi-analytic set* represented by a formula S can be derived in differential dynamic logic from the axioms whenever this invariance property holds, and a refutation can be derived whenever it does not.

Among characterizations of positive set invariance in a less general setting than that considered in this article, we note the work of Castelan and Hennet (1993), who reported necessary and sufficient conditions for positive invariance of convex polyhedra in linear vector fields.

8. Conclusion

This article describes two alternative characterizations of positively invariant sets for systems of ODEs with unique solutions.

The first characterization, along with its associated **LZZ** decision procedure for checking positive invariance of semi-algebraic sets in polynomial vector fields, is closely related to the work by Liu et al. (2011). While the relationship between the work of Liu et al. (2011) and the principle of *real induction* has been known informally to a number of researchers, this important link has not been adequately elaborated in existing literature. One of our aims in writing this article has been to make this relationship more widely appreciated and also to create an accessible account of the original **LZZ** decision procedure, along with our own improvements to this method (Section 3.2) and nuances in its practical implementation informed by our experience (Section 3.4).

The second part of the article contributes an alternative characterization of set positive invariance and is based on the notion of exit sets (Conley, 1978). The topological origins of this notion afford certain computational vistas that suggest a very different approach to developing a decision procedure for checking positive invariance than that of **LZZ**. The **ESE** procedure developed in Section 4.2 is, to the authors' knowledge, entirely novel. Its main advantage over **LZZ** lies in its efficient handling of formulas with non-trivial Boolean structure (a class of problems where the **LZZ** procedure generally performs poorly). The complexity analysis undertaken in Section 4.3 sheds some light on the computational advantages of using **ESE**, which is empirically confirmed in a number of examples in Section 5.

Important topics not touched upon in this article include *robustness* of positively invariant sets under small perturbations of the system dynamics; indeed, in practical applications, the system of ODEs is often only known approximately and invariants that are not robust are in a certain sense unphysical. In the future we hope to build upon the present work to address these considerations.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

The authors are indebted to Dr Paul B. Jackson and Dr Kousha Etessami at the University of Edinburgh for their insights into the real induction principle underpinning the work of Liu, Zhan and Zhao, and extend special thanks to Yong Kiam Tan at Carnegie Mellon University for suggesting improvements to the writing in an early draft of this work (and for bringing the authors' attention to the

article (Clark, 2019) of which they were previously unaware); his formal development of an invariant checking procedure in differential dynamic logic appeared in (Platzer and Tan, 2018) and (Platzer and Tan, 2020). The authors would also very much like to thank the anonymous reviewers for their careful reading and valuable suggestions for improving the article.

References

Alongi, J., Nelson, G., 2007. Recurrence and Topology. Graduate Studies in Mathematics, vol. 85. American Mathematical Society.

Bhatia, N.P., Szegő, G.P., 1970. Stability Theory of Dynamical Systems. Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete, vol. 161. Springer-Verlag.

Blanchini, F., 1999. Set invariance in control. Automatica 35, 1747–1767. https://doi.org/10.1016/S0005-1098(99)00113-2.

Blanchini, F., Miani, S., 2008. Set-Theoretic Methods in Control. Springer.

Cârjă, O., Necula, M., Vrabie Viability, I.I., 2007. Invariance and Applications. North-Holland Mathematics Studies, vol. 207. North-Holland.

Castelan, E.B., Hennet, J.-C., 1993. On invariant polyhedra of continuous-time linear systems. IEEE Trans. Autom. Control 38, 1680–1685. https://doi.org/10.1109/9.262058.

Chicone, C., 2006. Ordinary Differential Equations with Applications, second ed. Texts in Applied Mathematics, vol. 34. Springer.

Clark, P.L., 2019. The instructor's guide to real induction. Math. Mag. 92, 136–150. https://doi.org/10.1080/0025570X.2019.1549902.

Collins, G.E., Hong, H., 1991. Partial cylindrical algebraic decomposition for quantifier elimination. J. Symb. Comput. 12, 299–328. https://doi.org/10.1016/S0747-7171(08)80152-6.

Conley, C.C., 1978. Isolated Invariant Sets and the Morse Index. Regional Conference Series in Mathematics, vol. 38. American Mathematical Society.

Cox, D., Little, J., O'Shea, D., 2015. Ideals, Varieties, and Algorithms, fourth ed. Undergraduate Texts in Mathematics. Springer.

Dowek, G., 2003. Preliminary investigations on induction over real numbers. http://citeseerx.ist.psu.edu/viewdoc/versions?doi=10.1.1.123.9866.

Safey El Din, M., 2017. RAGlib: a library for real solving polynomial systems of equations and inequalities. https://www-polsys.lip6.fr/~safey/RAGLib/distrib.html.

Ghorbal, K., 2020. Implementation and examples (requires Wolfram Mathematica). https://github.com/kghorbal/LZZ-and-ES/tree/master/Mathematica.

Ghorbal, K., Platzer, A., 2014. Characterizing algebraic invariants by differential radical invariants. In: Ábrahám, E., Havelund, K. (Eds.), Tools and Algorithms for the Construction and Analysis of Systems - 20th International Conference, TACAS 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Proceedings. Grenoble, France, April 5–13, 2014. In: LNCS, vol. 8413. Springer, pp. 279–294.

Grigor'ev, D.Y., 1988. Complexity of deciding Tarski algebra. J. Symb. Comput. 5, 65–108. https://doi.org/10.1016/S0747-7171(88)80006-3.

Harms, M., Schilli, C., Zerz, E., 2017. Polynomial control systems: invariant sets given by algebraic equations/inequations. IFAC-PapersOnLine 50, 677–680. https://doi.org/10.1016/j.ifacol.2017.08.118.

Hathaway, D., 2011. Using continuity induction. Coll. Math. J. 42, 229–231. https://doi.org/10.4169/college.math.j.42.3.229.

Liu, J., Zhan, N., Zhao, H., 2011. Computing semi-algebraic invariants for polynomial dynamical systems. In: Chakraborty, S., Jerraya, A., Baruah, S.K., Fischmeister, S. (Eds.), Proceedings of the 11th International Conference on Embedded Software, EMSOFT 2011, Part of the Seventh Embedded Systems Week, ESWeek 2011. Taipei, Taiwan, October 9–14, 2011. ACM, pp. 97–106.

Maler, O., Nickovic, D., 2004. Monitoring temporal properties of continuous signals. In: Lakhnech, Y., Yovine, S. (Eds.), Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant Systems, Joint International Conferences on Formal Modelling and Analysis of Timed Systems, FORMATS 2004 and Formal Techniques in Real-Time and Fault-Tolerant Systems, FTRTFT 2004, Proceedings. Grenoble, France, September 22–24, 2004. In: LNCS, vol. 3253. Springer, pp. 152–166.

Nagumo, M., 1942. Über die Lage der Integralkurven gewöhnlicher Differentialgleichungen. Proc. Phys. Math. Soc. Jpn., 3rd Ser. 24, 551–559. https://doi.org/10.11429/ppmsj1919.24.0_551.

Novikov, D., Yakovenko, S., 1999. Trajectories of polynomial vector fields and ascending chains of polynomial ideals. Ann. Inst. Fourier 49, 563–609. https://doi.org/10.5802/aif.1683.

Platzer, A., Clarke, E.M., 2008. Computing differential invariants of hybrid systems as fixedpoints. In: Gupta, A., Malik, S. (Eds.), Computer Aided Verification, 20th International Conference, CAV 2008, Proceedings. Princeton, NJ, USA, July 7–14, 2008. In: LNCS, vol. 5123. Springer, pp. 176–189.

Platzer, A., Tan, Y.K., 2018. Differential equation axiomatization: the impressive power of differential ghosts. In: Dawar, A., Grädel, E. (Eds.), Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2018. Oxford, UK, July 09–12, 2018. ACM, pp. 819–828.

Platzer, A., Tan, Y.K., 2020. Differential equation invariance axiomatization. J. ACM 67, 6. https://doi.org/10.1145/3380825.

Redheffer, R., 1972. The theorems of Bony and Brezis on flow-invariant sets. Am. Math. Mon. 79, 740–747. https://doi.org/10.2307/2316263.

Ritt, J.F., 1950. Differential Algebra, vol. 33. American Mathematical Soc.

Sogokon, A., Ghorbal, K., Jackson, P.B., Platzer, A., 2016. A method for invariant generation for polynomial continuous systems. In: Jobstmann, B., Leino, K.R.M. (Eds.), Verification, Model Checking, and Abstract Interpretation - 17th International Conference, VMCAI 2016, Proceedings. St. Petersburg, FL, USA, January 17–19, 2016. In: LNCS, vol. 9583. Springer, pp. 268–288.

Taly, A., Tiwari, A., 2009. Deductive verification of continuous dynamical systems. In: Kannan, R., Kumar, K.N. (Eds.), IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2009. December 15–17, 2009, IIT Kanpur, India. In: LIPIcs, vol. 4, pp. 383–394.

Walter, W., 1998. Ordinary Differential Equations. Springer.

Zhan, N., Wang, S., Zhao, H. (Eds.), 2017. Formal Verification of Simulink/Stateflow Diagrams, A Deductive Approach. Springer.