Direct formal verification of liveness properties in continuous and hybrid dynamical systems

Direct formal verification of liveness properties in continuous and hybrid dynamical systems ⋆

Andrew Sogokon and Paul B. Jackson

LFCS, School of Informatics, University of Edinburgh, UK
a.sogokon@sms.ed.ac.uk, pbj@inf.ed.ac.uk

Abstract This paper is concerned with proof methods for the temporal property of eventuality (a type of liveness) in systems of polynomial ordinary differential equations (ODEs) evolving under constraints. This problem is of a more general interest to hybrid system verification, where reasoning about temporal properties in the continuous fragment is often a bottleneck. Much of the difficulty in handling continuous systems stems from the fact that closed-form solutions to non-linear ODEs are rarely available. We present a general method for proving eventuality properties that works with the differential equations directly, without the need to compute their solutions. Our method is intuitively simple, yet much less conservative than previously reported approaches, making it highly amenable to use as a rule of inference in a formal proof calculus for hybrid systems.

1 Introduction

In computer science, by *liveness* one informally understands the property of something "good" happening along the execution paths in a program. Thus, in stating that a program is *live* one asserts that some desirable property will hold true as the program runs. Liveness properties of discrete programs were studied by Lamport and Owicki in [16,23] and formally defined by Alpern and Schneider in [1]. In this paper we will be concerned with a particular type of liveness known as *eventuality*, which requires that some *target* set of states is eventually attained. Furthermore, instead of discrete computer programs, we will be working with continuous systems that are governed by ordinary differential equations and have an uncountably infinite number of states.

Continuous systems have generated significant interest among computer science and formal verification researchers over the past years as they form an important part of a broader class of dynamical systems known as *hybrid* (or *cyber-physical*) systems. Hybrid systems combine discrete and continuous behaviour; they are interesting because they provide the most general framework for modelling and verifying properties of dynamic phenomena. To give but a few examples, hybrid systems have found application in verifying safety of aircraft collision avoidance protocols [26], train control systems [25,17], simulating control systems for oil drills working with discontinuous friction [21] and many more.

⋆ This material is based upon work supported by the UK Engineering and Physical Sciences Research Council (EPSRC) under grant EP/I010335/1.

Formally verifying temporal properties of hybrid systems is no easy enterprise [11], in no small part due to their expressiveness, which makes most interesting questions about their behaviour inherently undecidable [13]. However, this does not mean that hybrid system verification is impossible and thus futile. On the contrary, formal verification tools have already been successfully applied in some impressive case studies, but it is also true that there is great scope for improvement in what verification tools are capable of. This is especially true of methods for verifying liveness properties, which are typically more difficult to prove than safety. In this paper we seek to partially remedy this by proposing a new deductive verification method for proving eventuality properties in continuous systems that can be implemented as a rule of inference in a theorem prover for hybrid systems.

The method we propose is able to work directly with initial states and target regions given by arbitrary semi-algebraic sets (that is, sets given by finite boolean combinations of polynomial equalities and inequalities) and generalizes previously reported approaches reported in [30,31,33,26]. Our approach is not restricted to bounded evolution domains (as e.g. [31]) and is able to prove eventuality properties for target regions described by formulas featuring equations (unlike [26,30]). Finally, the presence of system equilibria outside the target region presents an insurmountable obstacle for approaches reported in [30,31,26] and requires the user to manually remove them from the evolution domain [30]. We work with weaker conditions that only require a semi-algebraic over-approximation of the reachable set, which can be used to avoid equilibria without the need to manually alter the system. The conditions we give are much more general than in [33] and may be checked automatically using a decision procedure.

1.1 Contributions

In this paper we (**I**) describe a necessary condition for eventuality – the existence of what we call a *staging set* – and use it to (**II**) formulate conditions for proving eventuality properties in systems of polynomial ODEs without computing their solutions. (**III**) We illustrate the proof principle using some basic examples and (**IV**) describe how our approach can be used to construct formal proofs of certain liveness properties in a deductive verification tool for hybrid systems. Lastly, we (**V**) generalize total derivatives for formulas introduced in [26] by exploiting directional differentiability properties of the $\min \max$ function.

2 Preliminaries

In what follows, we will work with autonomous [1] systems of ordinary differential equations defined on $\mathbb{R}^n$ and evolving under constraints, i.e.

$$\begin{aligned} \dot{x}_i &= f_i(\boldsymbol{x}), \quad 1 \leq i \leq n, \\ \boldsymbol{x} &\in H \subseteq \mathbb{R}^n. \end{aligned}$$

[1] By this we mean that our ODEs have no *explicit* dependence on the time variable t. No generality is lost because any system with explicit time dependence can be turned into an autonomous system by adding a new 'clock' variable to model time evolution, e.g. if we let $\dot{x}_{n+1} = 1$ and replace every instance of t in the system with x_{n+1}.

We will write this more concisely as $\dot{\boldsymbol{x}} = f(\boldsymbol{x})$ & H. We will be interested in verifying properties of evolutions that lie within the constraints H, though in doing so we consider evolutions that might go outside of H. Furthermore, we will only work with polynomial systems, i.e. $f \in \mathbb{R}[\boldsymbol{x}]^n$, under evolution constraints H that are semi-algebraic sets.

Remark 1. To simplify our presentation we will interchangeably use the notation for sets and formulas characterizing those sets. Thus, H will denote both a semi-algebraic set $H \subseteq \mathbb{R}^n$ and a quantifier-free formula H of real arithmetic with free variables in $x_1, \ldots, x_n$ that characterizes the set H.

A *solution* to the initial value problem $(\dot{\boldsymbol{x}} = f(\boldsymbol{x}),\ \boldsymbol{x}_0)$ is a function $\varphi : (a, b) \to \mathbb{R}^n$ such that $\varphi(t)|_{t=0} = \boldsymbol{x}_0$ and $\frac{d}{dt}\varphi(t)|_{t=\tau} = f(\varphi(\tau))$ for all τ in some non-empty extended real interval (a, b) including 0. We will denote solutions to the initial value problem at time $t \in (a, b)$ by $\varphi_t(\boldsymbol{x}_0)$, where $\boldsymbol{x}_0$ is the initial value. The interval (a, b) is known as the *interval of existence* of a given solution; in what follows we will always consider the largest such interval, i.e. the *maximal* interval of existence.

In general, solutions to initial value problems need not be unique or even exist for all time $t \geq 0$, i.e. the maximal interval of existence need not be of the form (a, ∞). For instance, solutions to simple non-linear systems, such as $\dot{x} = x^2$, already exhibit *finite time blow-up*, i.e. diverge to infinity in finite time. In this paper we will work with differential equations whose solutions are unique and of sufficient duration to allow us to prove properties of interest. For simplicity we sometimes assume that solutions exist for all $t \geq 0$. In such cases, refinements of the arguments are needed if the solutions are of sufficient duration but do not exist for all $t \geq 0$. To remove this problem entirely, it is common (but not necessary) to require the system of ODEs to be Lipschitz continuous. Under these assumptions, we will refer to the solution φ as the *flow* of the system.

If the solution is available in *closed-form*, by which we informally understand a *finite* expression in terms of polynomials or elementary functions, then one can answer questions pertaining to the temporal behaviour of the system by working with the closed-form expression. In practice, however, closed-form solutions to non-linear ODEs are rarely available; even when they are, their form is often much more involved than the differential equations themselves. For instance, transcendental functions, such as $\sin$, $\cos$, $\exp$, $\log$, etc., frequently occur in solutions to very simple polynomial ODEs. This introduces a source of undecidability [32], which further undermines approaches to formal verification that rely on the knowledge of closed-form solutions.

Rather than working with the solution, it is sometimes possible to prove properties of interest by working with the differential equations *directly* [2]. This approach has been applied to formal safety verification (e.g. in [29,27,34]) and verification of progress and eventuality properties (e.g. see [33,30,26,31]). *Direct methods* for proving eventuality properties in ODEs have to date been rather conservative, i.e. they often fail even if the property is indeed true in a given system. Our interest in this paper is in exploring a direct verification approach that generalizes those previously reported and is at the same time less conservative.

[2] This idea is at the heart of the *qualitative theory* of differential equations and has its intellectual origins in the late nineteenth-century work of Henri Poincaré, published in [28].

In what follows, we will often write temporal properties as formulas of differential dynamic logic ($d\mathcal{L}$) [25], which provides a specification and verification language for hybrid systems, using hybrid programs [25] as operational models. The logic $d\mathcal{L}$ extends first-order logic with modalities $\langle\ \rangle$ and $[\ ]$ for hybrid programs. We will only be concerned with hybrid programs that define continuous systems; these are always of the form $\dot{\boldsymbol{x}} = f(\boldsymbol{x})\ \&\ H$. To a significant extent, our work will build upon results about invariant sets, which we discuss next.

2.1 Continuous Invariants

A fundamental property that provides the foundation for reasoning about safety in dynamical systems (be they discrete, continuous or hybrid) is that of set invariance. For continuous dynamical systems, by invariants we understand sets of states that remain invariant under the flow $\varphi_t(\cdot)$ for all $t \geq 0$. *Flow-invariant* (or *positively invariant*) sets are a very well-established concept in control and dynamical systems (see e.g. [4,3]) and can be used to prove safety properties for flows in a way analogous to program invariants in discrete programs. Platzer and Clarke in [27] generalized flow-invariant sets to *continuous invariants* for verifying safety of continuous systems under evolution constraints.

Definition 2. *A semi-algebraic set $I \subseteq \mathbb{R}^n$ is a continuous invariant for $\dot{\boldsymbol{x}} = f(\boldsymbol{x})\ \&\ H$ if and only if*

$$\forall\, \boldsymbol{x} \in I.\, \forall\, t \geq 0.\, (\forall\, \tau \in [0,t].\, \varphi_\tau(\boldsymbol{x}) \in H) \rightarrow (\forall\, \tau \in [0,t].\, \varphi_\tau(\boldsymbol{x}) \in I).$$

We may write a continuous invariance assertion as a formula in $d\mathcal{L}$ as follows:

$$I \rightarrow [\dot{\boldsymbol{x}} = f(\boldsymbol{x})\ \&\ H]\ I.$$

This formula asserts that if evolution starts anywhere inside I, then by following any solution *(box modality $[\ ]$) to the system $\dot{\boldsymbol{x}} = f(\boldsymbol{x})\ \&\ H$ for any length of time, the system* always *remains inside I.*

One useful way of thinking about continuous invariants (this will become apparent later) is as sets that "can only be left by entering $\neg H$ first".

Liu, Zhan and Zhao in [18] reported necessary and sufficient conditions for checking whether a given semi-algebraic set is a continuous invariant; their conditions are *direct*, i.e. do not require explicit knowledge of the solutions, and *decidable* if the system of ODEs is polynomial and H is semi-algebraic. This result leads to a *decision procedure* for semi-algebraic continuous invariant assertions, which can be expressed using $d\mathcal{L}$ formulas of the form $I \rightarrow [\dot{\boldsymbol{x}} = f(\boldsymbol{x})\ \&\ H]\ I$. The decision procedure described in [18] involves computing a finite number of higher-order *Lie derivatives* and exploits the ascending chain condition of Noetherian rings; see [18] for details and also [12] for related work on algebraic invariants. A Lie derivative of a real-valued differentiable function is the directional derivative of that function in the direction of the vector field induced by the system of ODEs. We denote the first-order Lie derivative

of a function $p : \mathbb{R}^n \to \mathbb{R}$ with respect to the vector field $f : \mathbb{R}^n \to \mathbb{R}^n$ as $\mathfrak{L}_f(p)$. Formally, the first Lie derivative is defined as

$$\mathfrak{L}_f(p) \equiv \sum_{i=1}^{n} \frac{\partial p}{\partial x_i} f_i \equiv \nabla p \cdot f.$$

Higher-order Lie derivatives are defined inductively, i.e. $\mathfrak{L}_f^k(p) = \mathfrak{L}_f(\mathfrak{L}_f^{k-1}p)$ for $k > 0$ and $\mathfrak{L}_f^0(p) = p$. Note also that in vector fields generated by ODEs, since $f_i = \dot{x}_i = \frac{dx_i}{dt}$, we have $\mathfrak{L}_f(p) = \sum_{i=1}^{n} \frac{\partial p}{\partial x_i}\frac{dx_i}{dt} = \frac{dp}{dt}$, i.e. the Lie derivative gives the *total derivative* of p with respect to time t. We will be using Lie derivatives in this capacity in the following sections.

3 Direct Method for Eventuality Verification

As a first attempt, one may define eventuality for continuous systems as follows:

$$\forall\, \boldsymbol{x}_0 \in X_0.\, \exists\, t \geq 0.\, \big(\varphi_t(\boldsymbol{x}_0) \in X_T\big),$$

where $X_0 \subseteq \mathbb{R}^n$ is the set of initial states and $X_T \subseteq \mathbb{R}^n$ is the target set. As with invariants, because continuous systems we consider may impose evolution domain constraints $H \subseteq \mathbb{R}^n$, the formal definition of eventuality needs an additional clause stipulating that continuous evolutions remain within the constraint until the target set is attained. Below we give a general definition of eventuality for continuous systems.

Definition 3. *Given a system $\dot{\boldsymbol{x}} = f(\boldsymbol{x})$ & H, where $H \subseteq \mathbb{R}^n$ is the evolution constraint, $X_0 \subseteq H$ is the set of initial states from which solutions are unique and of sufficient duration and $X_T \subseteq \mathbb{R}^n$ is the target set of states that we wish the system to attain by starting anywhere inside X_0, then the eventuality property holds if and only if*

$$\forall\, \boldsymbol{x}_0 \in X_0.\, \exists\, t \geq 0.\, \big(\, (\forall \tau \in [0,t].\, \varphi_\tau(\boldsymbol{x}_0) \in H) \;\wedge\; \varphi_t(\boldsymbol{x}_0) \in X_T\big),$$

By solutions of sufficient duration we understand solutions that may blow up in finite positive time, but only after reaching X_T (finite time blow up in negative time is innocuous for showing eventuality).

We may phrase the eventuality property using a $d\mathcal{L}$ formula as follows:

$$X_0 \to \langle \dot{\boldsymbol{x}} = f(\boldsymbol{x}) \;\&\; H \rangle\, X_T.$$

The above formula asserts that if we start anywhere inside X_0, then by following the *solution* to the system $\dot{\boldsymbol{x}} = f(\boldsymbol{x})$ & H, we *eventually* (diamond modality $\langle\ \rangle$) reach a state which lies inside X_T. In using the above formula, we assume that each of the sets H, X_0 and X_T is semi-algebraic and is thus characterized by a quantifier-free formula in the theory of real arithmetic.

3.1 Staging Sets

We now introduce *staging sets*, which are a particular kind of continuous invariants that we use to give an over-approximation of the continuous behaviour in a system with a view to proving eventuality properties without computing solutions to ODEs.

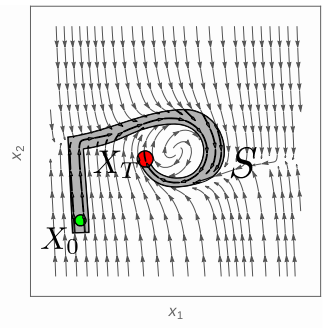

Figure 1: Staging set (intuitively). Initial set of states X_0 is shown in green, the target set X_T in red and possible choice for a staging set S in grey; H is taken to be $\mathbb{R}^2$.

Definition 4. *Given a system $\dot{\boldsymbol{x}} = f(\boldsymbol{x})$ & H, a set of initial states $X_0 \subseteq H$ and a target set of states $X_T \subseteq \mathbb{R}^n$, we say that a set $S \subseteq \mathbb{R}^n$ is a **staging set** if we have $S \subseteq H$, $X_0 \setminus X_T \subseteq S$ and*

$$\forall\, \boldsymbol{x}_0 \in S.\, \forall\, t \geq 0.\, (\forall \tau \in [0,t].\, \varphi_\tau(\boldsymbol{x}_0) \notin X_T \cap H) \;\rightarrow\; (\forall \tau \in [0,t].\, \varphi_\tau(\boldsymbol{x}_0) \in S).$$

One could write this formally using $d\mathcal{L}$ as

$$\big(X_0 \wedge \neg X_T \rightarrow S\big) \wedge \big(S \rightarrow [\dot{\boldsymbol{x}} = f(\boldsymbol{x})\ \&\ \neg(X_T \wedge H)]\ S\big) \wedge \big(X_0 \vee S \rightarrow H\big).$$

Intuitively, a staging set is any set within the evolution constraint H that includes the non-trivial initial states $X_0 \setminus X_T$ and that "can only be left by entering the target region X_T within the constraint H", or provides a "continuous exit window into X_T within H". Fig. 1 illustrates this intuition. Let us remark that staging sets are very natural because their existence is a necessary pre-requisite for the eventuality property to hold.

Proposition 5. *If the eventuality property holds for $\dot{\boldsymbol{x}} = f(\boldsymbol{x})$ & H with initial and target sets $X_0 \subseteq H, X_T \subseteq \mathbb{R}^n$ as before, then there exists a staging set for the system.*

Proof. Assuming the eventuality property holds true in the system, we have $X_0 \subseteq H$ and for each $\boldsymbol{x}_0 \in X_0 \setminus X_T$ there exists some $t > 0$ such that $\varphi_t(\boldsymbol{x}_0) \in X_T$ and $\forall\, \tau \in [0,t].\, \varphi_\tau(\boldsymbol{x}_0) \in H$. Now define $\gamma(\boldsymbol{x}_0) \equiv \{\varphi_{t'}(\boldsymbol{x}_0) \mid t' \in [0,t)\}$ to construct a staging set $S \equiv \bigcup_{\boldsymbol{x}_0 \in X_0} \gamma(\boldsymbol{x}_0)$. □

Remark 6. The construction in the proof above gives a staging set which may not possess a closed-form description. In practice, by restricting attention to semi-algebraic sets, one can *decide* whether a given candidate set constitutes a staging set for the system at hand. Also, note that if S is a staging set, then $S' \equiv S \setminus X_T$ is also a staging set.

Searching for a staging set is in principle no different to searching for a continuous invariant for safety verification. Methods for continuous invariant generation can therefore be applied to search for staging sets. Techniques for continuous invariant generation are still an active area of research, with *complete* [3] (albeit intractable) procedures available to search for semi-algebraic continuous invariants based on enumerating parametric semi-algebraic templates and using a decision procedure for continuous invariant checking described in [18] together with real quantifier elimination [35] (see [9] for a survey of more recent methods). In practice, certain incomplete invariant generation methods may offer more scalable alternatives. For instance, sum-of-squares techniques for computing polynomial sub-level set approximations of the finite-time reachable set due to Wang, Lall & West [36] are promising in this regard.

3.2 Progress Functions

The existence of a staging set only provides a *necessary condition* for eventuality. In this section we will give a *sufficient condition* that will allow us to soundly conclude the eventuality property. Because we already require the sets we work with to be semi-algebraic, we can invoke the following lemma.

Lemma 7. *If $H, I \subseteq \mathbb{R}^n$ are semi-algebraic and I is a continuous invariant for the system $\dot{\boldsymbol{x}} = f(\boldsymbol{x})$ & H then any solution that starts in $I \cap H$ and subsequently leaves I either **(i)** leaves H while still in I or **(ii)** has a non-empty segment immediately on leaving I that is wholly contained in $\mathbb{R}^n \setminus H$ (i.e. $\neg H$).*

Proof (sketch). Case (i) is obvious and follows from the definition of continuous invariants. For case (ii) we need to show that if I and H are left at the same time, then $\neg H$ is sustained for some non-empty time interval. If there is a time t' such that $\forall\, \tau \in [0, t').\ \varphi_\tau(\boldsymbol{x}_0) \in H \cap I$ and $\varphi_{t'}(\boldsymbol{x}_0) \notin H \cup I$, then $\neg H$ is sustained for $[t', t']$ immediately upon leaving I. If no such t' exists, consider a point $\boldsymbol{x}_1 \in I \cap H$ from which the system can no longer evolve inside I without violating the constraint H. It is necessarily the case that $\forall\, \epsilon > 0.\ \exists\, t \in (0, \epsilon).\varphi_t(\boldsymbol{x}_1) \notin H$ holds, i.e. no further motion of the system can sustain the constraint. We need to show the stronger property $\exists\, \epsilon > 0.\ \forall\, t \in (0, \epsilon).\varphi_t(\boldsymbol{x}_1) \notin H$. For any semi-algebraic set, let $P \subset \mathbb{R}[\boldsymbol{x}]$ be the collection of polynomials appearing in its description. At the point $\boldsymbol{x}_1$ for each $p_i \in P$ we have that $p_i(\boldsymbol{x}_1) \sim 0$, where $\sim \in \{<, =, >\}$. For those $p_i \in P$ such that $p_i(\boldsymbol{x}_1) > 0$ or $p_i(\boldsymbol{x}_1) < 0$, there is guaranteed to be an open neighbourhood U_i around $\boldsymbol{x}_1$ for which $p_i(U_i) > 0$ or $p_i(U_i) < 0$ holds (since polynomials are continuous functions). Therefore, there is some non-empty time neighbourhood $(0, \epsilon)$ for which the solution will sustain the strict sign conditions. When $p_i(\boldsymbol{x}_1) = 0$, one either has $\mathfrak{L}_f^k(p_i(\boldsymbol{x}_1)) = 0$ for infinitely many orders k, or there exists an $k \geq 1$ such that $\mathfrak{L}_f^k(p_i(\boldsymbol{x}_1)) \neq 0$. Since polynomials and solutions to polynomial ODEs are analytic functions, there is some open time neighbourhood $(0, \epsilon)$ where the sign condition on the polynomial p_i is sustained under the solution (see e.g. [18, Proposition 9]). Thus, if a semi-algebraic set cannot be sustained, then its semi-algebraic complement is sustained for some non-empty open time interval following the solution. □

[3] In the sense that an appropriate continuous invariant (if it exists) will always be found.

If one can show that any trajectory starting inside a staging set S eventually leaves S, one can use Lemma 7 to conclude the eventuality property. An obvious way of showing S is eventually left without computing the solution to the system of ODEs is to search for an appropriate function, whose derivative can be used as a measure of "progress in leaving S".

Proposition 8. *Given a staging set S for some polynomial system $\dot{\boldsymbol{x}} = f(\boldsymbol{x})$ & H with initial and target sets $X_0 \subseteq H$, $X_T \subseteq \mathbb{R}^n$ respectively and whose* solutions are of sufficient duration*, if there exists a continuously differentiable function $P : \mathbb{R}^n \to \mathbb{R}$ such that*

$$\exists\, \varepsilon > 0.\, \forall\, \boldsymbol{x} \in S. \quad \mathfrak{L}_f(P(\boldsymbol{x})) \leq -\varepsilon \;\wedge\; P(\boldsymbol{x}) \geq 0,$$

then, provided the sets are semi-algebraic, the eventuality property holds and P is known as a ***progress function*** *for S.*

Proof. Fix a start point $\boldsymbol{x}_0 \in X_0 \setminus X_T$ from which we want to argue there is a finite flow with end point in X_T and which is fully contained in H. First we show that there is a finite flow from $\boldsymbol{x}_0$ with end point outside of S. Assume that the solution with initial condition $\boldsymbol{x}_0$ is of sufficient duration such that either **(i)** the trajectory exits S at some point or **(ii)** the trajectory is inside S up to and including at least some time $\tau > P(\boldsymbol{x}_0)/\varepsilon$. In case **(ii)**, a simple application of the fundamental theorem of calculus yields

$$\begin{aligned} P(\varphi_\tau(\boldsymbol{x}_0)) - P(\varphi_0(\boldsymbol{x}_0)) \;=\; \int_0^\tau \frac{d}{dt} P(\varphi_t(\boldsymbol{x}_0))\, dt &= \int_0^\tau \mathfrak{L}_f(P(\varphi_t(\boldsymbol{x}_0)))\, dt \\ &\leq \int_0^\tau -\varepsilon\, dt \\ &= -\varepsilon\tau. \end{aligned}$$

Given $P(\varphi_0(\boldsymbol{x}_0)) = P(\boldsymbol{x}_0)$ we have that $P(\varphi_\tau(\boldsymbol{x}_0)) < 0$ which is impossible since $P(\boldsymbol{x}_0) \geq 0$ for all $\boldsymbol{x}_0 \in S$. Hence case **(i)** must hold. Using case **(i)**, we now apply Lemma 3 to the invariance property of the staging set S. We have that either the trajectory reaches $X_T \cap H$ within S and the eventuality property obviously holds, or, on exiting S we immediately have a non-empty segment of the trajectory contained in $X_T \cap H$ and the eventuality property holds too. □

Remark 9. Of course, given some set $\hat{S}$ such that $S \subseteq \hat{S}$, where S is a staging set, if one shows that $\hat{S}$ is left in finite time by following the solutions, then one can also conclude that X_T is eventually attained. This may seem like a complete waste of effort, but methods developed for *verified integration* of ODEs [2,22] can compute *enclosures* of finite-time reachable sets where the enclosure itself is *not* a staging set but is guaranteed to enclose one; in this case, the enclosure can act as $\hat{S}$. Formally verified implementations of enclosure construction algorithms have been reported by Immler [14,15].

Polynomial progress functions may be generated automatically using pre-defined polynomial *templates* of bounded degree with parametric coefficients. The templates can be enumerated (e.g. by successively increasing the polynomial degree) and checked using a real quantifier elimination procedure (such as e.g. CAD [6]), leaving the parameters

as free variables. The result is a semi-algebraic constraint on the coefficients that will yield a progress function. Of course, the computational complexity of real quantifier elimination [7] makes this approach infeasible and therefore practically uninteresting; however, theoretically, one has a *semi-decision procedure* for checking whether a polynomial progress function exists for a given semi-algebraic staging set and a polynomial ODE. Methods based on sum-of-squares techniques (e.g. [30]) may offer more practical (albeit incomplete) alternatives for finding progress functions.

4 Proof Rule for Eventuality in ODEs

We are now ready to formalize the proof method for eventuality properties using staging sets and progress functions, as described in the previous section, into a rule of inference.

Proposition 10. *The rule of inference given below (with four premises) is sound with the proviso that solutions are of sufficient duration.*

$$\vdash \exists\, \varepsilon > 0.\, \forall\, \boldsymbol{x}.\quad S \to \big(P \geq 0 \ \wedge\ \mathfrak{L}_f(P) \leq -\varepsilon\big)$$

$$\text{(SP)}\ \frac{X_0, \neg X_T \vdash S \qquad \vdash S \to [\dot{\boldsymbol{x}} = f(\boldsymbol{x})\ \&\ \neg(H \wedge X_T)]\, S \qquad X_0 \vee S \vdash H}{\vdash X_0 \to \langle \dot{\boldsymbol{x}} = f(\boldsymbol{x})\ \&\ H\rangle\, X_T}.$$

Proof. Corollary to Prop. 8. The sufficient duration proviso is soundness-critical (see [26, Counterexample 9] for an example of why this is important). A stronger requirement, e.g. Lipschitz continuity of f (if not globally, then within some compact subset of $\mathbb{R}^n$ containing X_T and S) may be used to give a formal criterion for ensuring the proviso holds, but this can be restrictive in practice. □

Example 11 (System with limit cycle and equilibrium). Consider the system of ODEs with an equilibrium and a limit cycle

$$\dot{x}_1 = x_2 - x_1\left(x_1^2 + x_2^2 - 1\right), \quad \dot{x}_2 = -x_1 - x_2\left(x_1^2 + x_2^2 - 1\right),$$

with $H \equiv x_1 \leq 2 \wedge x_1 \geq -2 \wedge x_2 \leq 2 \wedge x_2 \geq -2$ and let the initial set of states and the target region be as follows:

$$X_0 \equiv x_2 > 0 \wedge x_1 \geq -\frac{1}{4} \wedge x_1 \leq \frac{1}{4} \wedge (x_1^2 + x_2^2 - 1)^2 \leq \frac{1}{30},$$
$$X_T \equiv x_2 < 0 \wedge x_1 \geq -\frac{1}{4} \wedge x_1 \leq \frac{1}{4} \wedge (x_1^2 + x_2^2 - 1)^2 \leq \frac{1}{30}.$$

Consider also the following sets (depicted in Fig. 2):

$$S_1 \equiv \neg X_T \wedge x_1 \geq -\frac{1}{4} \wedge (x_1^2 + x_2^2 - 1)^2 \leq \frac{1}{30},$$
$$S_2 \equiv \neg X_0 \wedge x_1 \leq \frac{1}{4} \wedge (x_1^2 + x_2^2 - 1)^2 \leq \frac{1}{30}.$$

One may check using a decision procedure that S_1 is indeed a staging set for this system.

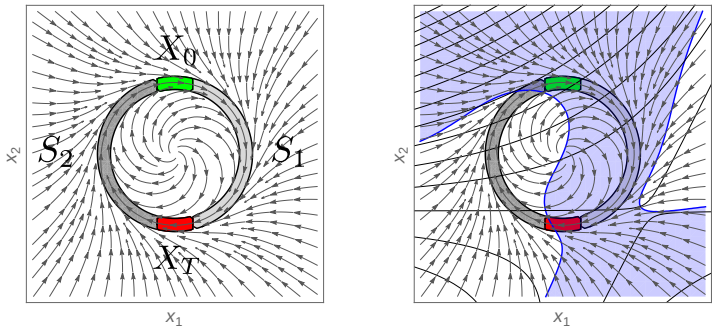

Figure 2: (**left**) Initial states X_0 (in green), target region X_T (in red) and staging sets S_1 (in grey and green, i.e. S_1 includes X_0) and S_2 (dark grey and red, i.e. S_2 includes X_T). (**right**) Level sets of the progress function P_1 for showing eventual exit out of S_1 and the region where $\exists\, \varepsilon > 0.\ \mathfrak{L}_f(P_1) \leq -\varepsilon$ holds (includes S_1; shaded in blue).

A possible progress function for S_1 is $P_1(\boldsymbol{x}) = -\left(x_1 - \frac{6}{5}\right)^2 + (x_1 - x_2 - 2)^2 + 10$. Computing the total derivative of P_1 (i.e. Lie derivative with respect to the vector field) we obtain $\mathfrak{L}_f(P_1(\boldsymbol{x})) =$

$$2\,(x_1 - x_2 - 2)\left(x_2^3 + x_1^2 x_2 - x_2 + x_1\right) + \frac{2}{5}\,(5x_2 + 4)\left(x_1^3 + \left(x_2^2 - 1\right)x_1 - x_2\right).$$

Using a decision procedure for real arithmetic to check that the sentence

$$\exists\, \varepsilon > 0.\, \forall\, \boldsymbol{x} \in S_1. \qquad \mathfrak{L}_f(P_1(\boldsymbol{x})) \leq -\varepsilon \ \wedge\ P_1(\boldsymbol{x}) \geq 0$$

is true is sufficient to conclude the eventuality property

$$X_0 \rightarrow \langle \dot{x}_1 = x_2 - x_1\left(x_1^2 + x_2^2 - 1\right), \dot{x}_2 = -x_1 - x_2\left(x_1^2 + x_2^2 - 1\right)\ \&\ H\rangle\ X_T$$

using the proof rule SP with S_1 as the staging set and P_1 acting as the progress function. Similarly, one may instead take X_T to be the initial set of states and X_0 to be the target region. By using S_2 as a staging set and taking the progress function

$$P_2(\boldsymbol{x}) = -\left(-x_1 - \frac{6}{5}\right)^2 + (-x_1 + x_2 - 2)^2 + 10$$

one may use the proof rule SP, instantiating S_2 and P_2 appropriately, to prove

$$X_T \rightarrow \langle \dot{x}_1 = x_2 - x_1\left(x_1^2 + x_2^2 - 1\right), \dot{x}_2 = -x_1 - x_2\left(x_1^2 + x_2^2 - 1\right)\ \&\ H\rangle\ X_0.$$

The proof rule SP can be used as part of a formal verification calculus for hybrid systems in which liveness properties of hybrid systems are reduced using rules of inference to proving liveness properties for discrete and continuous sub-components. When working in a proof calculus, the following proof rule, formalizing the transitivity of the eventuality relation between sets of states, is often convenient:

$$(\langle\rangle\ \text{Trans})\ \frac{\vdash X_0 \rightarrow \langle \dot{\boldsymbol{x}} = f(\boldsymbol{x})\ \&\ H\rangle\ T \qquad \vdash T \rightarrow \langle \dot{\boldsymbol{x}} = f(\boldsymbol{x})\ \&\ H\rangle\ X_T}{\vdash X_0 \rightarrow \langle \dot{\boldsymbol{x}} = f(\boldsymbol{x})\ \&\ H\rangle\ X_T}.$$

Let us note also that proving the property of *set reachability* reduces to proving the existence of a non-empty set of initial states $R \subseteq X_0$ from which the eventuality property holds. We may formalize this fact in the following proof rule:

$$(\text{Reach})\ \frac{\vdash R \wedge X_0 \not\equiv_{\mathbb{R}} \text{False} \quad \vdash R \rightarrow \langle \dot{\boldsymbol{x}} = f(\boldsymbol{x}) \,\&\, H \rangle\ X_T}{\vdash \exists\, \boldsymbol{x} \in X_0.\ \langle \dot{\boldsymbol{x}} = f(\boldsymbol{x}) \,\&\, H \rangle\ X_T}.$$

To show that a given set X_T is eventually attained from some initial set X_0 in a hybrid system, one can apply the rule SP to e.g. first show that some *guard set* within a mode is attained and then proceed to compute the sets reachable from the guard set by following the enabled discrete transitions, using these (or their semi-algebraic over-approximation) as the new initial sets in subsequent applications of SP.

The next section will discuss the relationship between SP and an existing proof method called *differential induction* using *differential variants* [26] that is part of the logic $d\mathcal{L}$ and has been applied to hybrid system liveness verification problems.

5 Non-differentiable Progress Functions

In this section we will use directional differentiability properties of the $\min \max$ functional with differentiable arguments [8,10] to broaden the class of progress functions at our disposal and discuss how this generalizes the definition of total derivative for *formulas* that was used for *differential variants* in [26]. We will also show how the proof rule SP serves to remove certain limitations inherent in differential variants.

5.1 Derivatives of Formulas and Differential Variants

Differential induction using differential variants (and differential invariants) is a direct proof method introduced by Platzer in [26] for proving eventuality (invariance) properties in ODEs, as part of a verification calculus for hybrid systems. The method allows one to work with arbitrary semi-algebraic sets represented by quantifier-free formulas. In order to work in this general setting, differential induction requires the notion of total derivative to be lifted to formulas, which is achieved through the use of the derivation operator D (see [26, Def. 13]); it is given as follows: $D(r) = 0$ for numbers, $D(x) = \dot{x}$ for variables, $D(a + b) = D(a) + D(b)$, where a, b stand for numbers or variables, $D(a \cdot b) = D(a) \cdot b + a \cdot D(b)$ (product rule), $D\left(\frac{a}{b}\right) = \frac{D(a)\cdot b - a \cdot D(b)}{b^2}$ (quotient rule),

$$\begin{aligned}
D(F \wedge G) &\equiv D(F) \wedge D(G), && \text{for quantifier-free formulas } F \text{ and } G,\\
D(F \vee G) &\equiv D(F) \wedge D(G), && \wedge \text{ needed for soundness in proving invariance [26]}\\
D(a \leq b) &\equiv D(a) \leq D(b), && \text{accordingly for } \geq, >, <, = .
\end{aligned}$$

The formula $(D(F) \geq \varepsilon)^{f(\boldsymbol{x})}_{\dot{\boldsymbol{x}}}$ is obtained by applying the derivation operator to formula F, performing a substitution where each $\dot{x}_i$ in $D(F)$ is replaced with the corresponding right-hand side in the differential equation and replacing all inequalities $a \geq b$ by $a \geq b + \varepsilon$ (accordingly for $<, \leq, >$; see [26, Section 4.6]).

$$(\text{DV})\frac{\vdash \exists\, \varepsilon > 0 (\neg X_T \wedge H \rightarrow (D(X_T) \geq \varepsilon)^{f(\boldsymbol{x})}_{\dot{\boldsymbol{x}}})}{[\dot{\boldsymbol{x}} = f(\boldsymbol{x}) \,\&\, \sim X_T] H \vdash \langle \dot{\boldsymbol{x}} = f(\boldsymbol{x}) \,\&\, H \rangle X_T}$$

The formula $\sim X_T$ is the *weak negation* of X_T [26, Section 4.6] defined by the negation of X_T in which every strict inequality is made non-strict. Formulas X_T provable using the rule DV [4] are called differential variants. Like our proof rule SP, the rule DV may be applied under the proviso that solutions are of sufficient duration (see [26, Section 4.7]).

In practice, DV is rather conservative because it is incapable of proving eventuality properties for target regions described by equations [26, Counterexample 7]. In Example 12 we demonstrate a simple proof of such a property using staging sets and progress functions.

Example 12 (Target region with equational description). Let the dynamics be given by the non-linear system $\dot{x}_1 = -1, \dot{x}_2 = (x_2 - x_1)^2$, $H = \mathbb{R}^2$ and consider a target region described an equation $X_T \equiv x_2 - x_1 = 0$ (see Fig. 3).

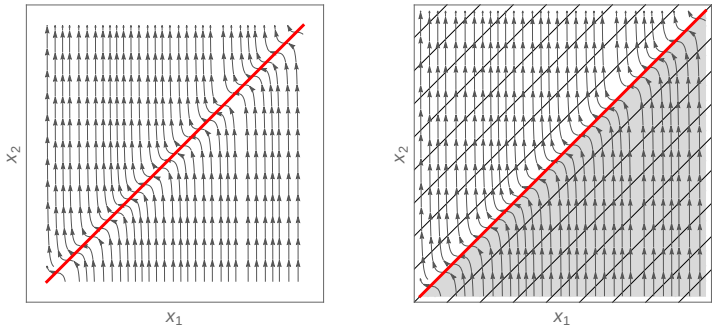

Figure 3: (**left**) Target region $X_T \equiv x_2 - x_1 = 0$ (in red) and any initial set such that $X_0 \to x_2 - x_1 < 0$ (anywhere below the red line, not shown). (**right**) Staging set $S \equiv x_2 - x_1 < 0$ (in grey) and level sets of the progress function $P(\boldsymbol{x}) = -(x_2 - x_1)$.

Suppose the initial set of states X_0 is any subset of $\{\boldsymbol{x} \in \mathbb{R}^2 \mid x_2 - x_1 < 0\}$. To show the eventuality property let us take $S \equiv x_2 - x_1 < 0$, which can be easily shown to be a staging set, and use $P(\boldsymbol{x}) = -(x_2 - x_1)$ as a progress function. The total derivative of P is given by $\mathfrak{L}_f(P(\boldsymbol{x})) = -(x_2 - x_1)^2 - 1$, which satisfies the ε-progress property inside the staging set S. An application of the rule SP proves the property $X_0 \to \langle \dot{x}_1 = -1, \dot{x}_2 = (x_2 - x_1)^2 \,\&\, H \rangle\, X_T$.

In general, finding an appropriate progress function P for use with the rule SP can be rather non-trivial; however, sometimes the description of the target region itself may suggest a progress function. Indeed, this is how the rule DV checks the ε-progress property towards the target region: by considering the total derivative of the formula giving the target region itself. This is not guaranteed to work even if the eventuality property is true, but one may think of DV as generating a "progress formula" from the description of the target region. Because DV relies on the derivation operator D for its notion of ε-progress for formulas, the resulting conditions are very strong. In what

[4] Note that X_T is required to define a closed set for the rule DV to be sound.

follows, we will seek to relax them, while still using the description of the target region to suggest a progress function that can be used with our proof method.

5.2 Non-differentiable Progress Functions

Given a quantifier-free formula X_T characterizing a semi-algebraic set, the weak negation of its negation, $\sim\neg X_T$ ($\sim$ defined as for DV), gives a formula characterizing a *closed* semi-algebraic set that over-approximates the closure of X_T. Note that any closed semi-algebraic set can always be put into the form

$$\bigvee_{i=1}^{n} \bigwedge_{j=1}^{m(i)} p_{ij} \leq 0,$$

where p_{ij} are polynomials. The set of states satisfying such a formula can equivalently be expressed as a sub-level set of a continuous function, i.e.

$$\min_{i\in[1,n]} \max_{j\in[1,m(i)]} p_{ij} \leq 0.$$

Although this function need not be differentiable, for ensuring the property of ε-progress, viz. $\mathfrak{L}_f(\cdot) \leq -\varepsilon$, we are merely interested in a certain condition on its *directional derivative* in the direction of the vector field. Directional differentiability properties of the $\min\max$ function have previously been investigated in non-smooth analysis [10,8] and it was shown that under certain mild assumptions (see [10]), the $\min\max$ function has a directional derivative that can also be expressed as a $\min\max$ function. Furthermore, these assumptions are guaranteed to hold if the ε-progress property is satisfied. The directional derivative of $\min\max$ (see [10]) in the direction of the vector field f, may be used to define

$$\mathfrak{L}_f\big(\min_{i\in[1,n]} \max_{j\in[1,m(i)]} p_{ij}\big) = \min_{i\in I_*} \max_{j\in J_*} \left(\mathfrak{L}_f(p_{ij})\right),$$

where p_{ij} are differentiable real-valued functions and

$$J_* = \{j_* \in [1, m(i)] \mid p_{ij_*} = \max_{j\in[1,m(i)]} (p_{ij})\},$$
$$I_* = \{i_* \in [1, n] \mid p_{i_*j} = \min_{i\in[1,n]} \max_{j\in[1,m(i)]} (p_{ij})\}.$$

The above definition may at first sight appear rather opaque; the following illustrative example is useful in exposing some of the intuition.

Example 13. Suppose that we have a formula $F \equiv p_1 \leq 0 \wedge p_2 \leq 0$. Then we have $F \equiv_{\mathbb{R}} \max(p_1, p_2) \leq 0$ and the directional derivative along f given by

$$\mathfrak{L}_f \max(p_1, p_2) = \begin{cases} \mathfrak{L}_f(p_1) & p_1 > p_2 \\ \mathfrak{L}_f(p_2) & p_2 > p_1 \\ \max(\mathfrak{L}_f(p_1), \mathfrak{L}_f(p_2)) & p_1 = p_2 \end{cases}$$

Intuitively, when there is only one differentiable "active component" (i.e. a function p_j which evaluates to the same value as the whole $\max$ function), the directional derivative is simply given by $\mathfrak{L}_f(p_j)$; however, when there are many, the index set J_* contains more than one element and the directional derivative is given by $\max_{j \in J_*} \mathfrak{L}_f(p_j)$ where all p_j are currently active. More generally, once the directional derivative of $\min \max p_{ij}$ is computed and an ε-progress condition is imposed, the resulting expression will feature conditionals involving $\min$, $\max$, ε and p_{ij}s and can thus be converted back into a formula giving precisely the conditions for the ε-progress of the $\min \max$ function. The resulting formulas will often be long and unwieldy, but for this simple example we can write the condition in full:

$$\begin{aligned}
\mathfrak{L}_f \max(p_1, p_2) \leq -\varepsilon \equiv\ & \big(p_1 > p_2 \rightarrow \mathfrak{L}_f(p_1) \leq -\varepsilon\big) \\
\wedge\ & \big(p_2 > p_1 \rightarrow \mathfrak{L}_f(p_2) \leq -\varepsilon\big) \\
\wedge\ & \big(p_1 = p_2 \rightarrow \\
& \quad (\mathfrak{L}_f(p_1) \geq \mathfrak{L}_f(p_2) \rightarrow \mathfrak{L}_f(p_1) \leq -\varepsilon) \wedge \\
& \quad (\mathfrak{L}_f(p_1) < \mathfrak{L}_f(p_2) \rightarrow \mathfrak{L}_f(p_2) \leq -\varepsilon)\ \big).
\end{aligned}$$

Similarly, if one wanted to impose the ε-progress property towards the formula $F \equiv p_1 \leq 0 \vee p_2 \leq 0$, encoded as $F \equiv_{\mathbb{R}} \min(p_1, p_2) \leq 0$, one would obtain

$$\begin{aligned}
\mathfrak{L}_f \min(p_1, p_2) \leq -\varepsilon \equiv\ & \big(p_1 < p_2 \rightarrow \mathfrak{L}_f(p_1) \leq -\varepsilon\big) \\
\wedge\ & \big(p_2 < p_1 \rightarrow \mathfrak{L}_f(p_2) \leq -\varepsilon\big) \\
\wedge\ & \big(p_1 = p_2 \rightarrow \\
& \quad (\mathfrak{L}_f(p_1) \leq \mathfrak{L}_f(p_2) \rightarrow \mathfrak{L}_f(p_1) \leq -\varepsilon) \wedge \\
& \quad (\mathfrak{L}_f(p_1) > \mathfrak{L}_f(p_2) \rightarrow \mathfrak{L}_f(p_2) \leq -\varepsilon)\ \big).
\end{aligned}$$

By nesting these definitions appropriately, using facts such as e.g. $\min(p_1, p_2, p_3) = \min(p_1, \min(p_2, p_3))$, one can arrive at ε-progress conditions for more complicated closed semi-algebraic sets.

Remark 14. Similar tools and ideas have been employed in sufficient conditions for positive invariance of certain sets with non-smooth boundaries (e.g. *practical sets* in [5] and closed semi-algebraic sets [34]). These approaches are based on Nagumo's theorem [20] and require computing/under-approximating the *contingent cone*, which can be defined in terms of limits of directional derivatives. The interested reader is invited to consult [10] for a more detailed exposition of the technical assumptions used in formulating the directional derivative of $\min \max$.

Example 15 (Non-differentiable progress function). Consider the continuous system $\dot{x}_1 = -x_1, \dot{x}_2 = -x_2, H = \mathbb{R}^2$ and let the target set of states correspond to a 2×2 box centred at the origin, i.e. $X_T \equiv x_1 \leq 1 \wedge x_1 \geq -1 \wedge x_2 \leq 1 \wedge x_2 \geq -1$. From the phase portrait in Fig. 4 (left) it is clear that the eventuality property is true, i.e. by starting the system outside the box, we are guaranteed to eventually enter the box by following the flow.

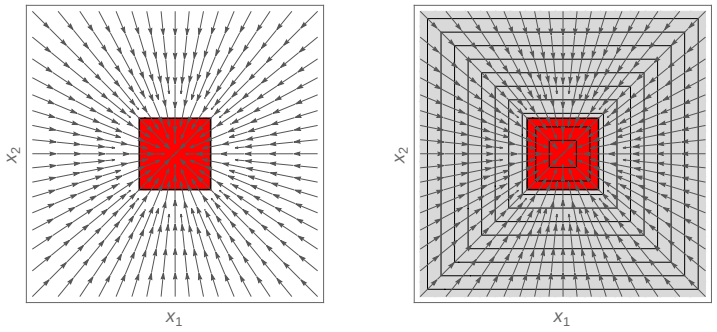

Figure 4: (**left**) Phase portrait, target set X_T (in red). (**right**) Level curves of a non-differentiable progress function (black) and a staging set $S \equiv \neg X_T$ (grey).

This property cannot be proved directly using the rule DV because the definition of the derivation operator for formulas requires one to show that *each* conjunct is a differential variant. In this case,

$$D(X_T) \geq \varepsilon \equiv \dot{x}_1 \leq \varepsilon \wedge \dot{x}_1 \geq \varepsilon \wedge \dot{x}_2 \leq \varepsilon \wedge \dot{x}_2 \geq \varepsilon.$$

Upon substituting the dynamics, this leads to unsatisfiable conditions (since $\varepsilon > 0$):

$$(D(X_T) \geq \varepsilon)^{f(\boldsymbol{x})}_{\dot{\boldsymbol{x}}} \equiv -x_1 \leq \varepsilon \wedge -x_1 \geq \varepsilon \wedge -x_2 \leq \varepsilon \wedge -x_2 \geq \varepsilon \equiv_{\mathbb{R}} \text{False}.$$

Instead, one may write down the formula for the box as a sub-level set, i.e.

$$X_T \equiv \max(x_1 - 1, -x_1 - 1, x_2 - 1, -x_2 - 1) \leq 0$$

and taking the complement of X_T to be the staging set, i.e. $S \equiv \neg X_T$, check that

$$\begin{aligned} \exists\, \varepsilon > 0.\, \forall \boldsymbol{x} \in S. \big(& \max(x_1 - 1, -x_1 - 1, x_2 - 1, -x_2 - 1) \geq 0 \\ & \wedge\ \mathfrak{L}_f \max(x_1 - 1, -x_1 - 1, x_2 - 1, -x_2 - 1) \leq -\varepsilon \big) \end{aligned}$$

is valid, which is sufficient to conclude the eventuality property for any $X_0 \subseteq S$.

6 Related Work

Prajna and Rantzer investigated automatic verification of eventuality properties for ODEs in [30]; their approach ensures that evolution occurs within the domain constraint by imposing extra constraints on the function used to demonstrate progress along the solutions. Furthermore, the ε-progress property is required to hold everywhere outside the target region. System equilibria lying outside the target region present a problem for this approach and need to be manually removed from the evolution domain. Ratschan and She introduced set-Lyapunov functions to study attraction to target regions in [31], considering only bounded domains and also imposing conditions for ensuring progress along the solutions everywhere outside the target region, which suffers from the same

problem. The proof method we have proposed works with a more general class of eventuality verification problems (as it makes fewer assumptions about the problem statement and the nature of the system) and can handle systems with equilibria outside the target region by appropriately over-approximating the reachable set using staging sets.

Our approach is fundamentally different from that used by Platzer in [26], e.g. allowing target regions with equational descriptions (among other things; see Section 5).

Ideas broadly similar to staging sets were explored by Stiver et al. in [33] using *common flow regions*. Informally, common flow regions are sets bounded by invariant manifolds and an "exit boundary". The conditions given in [33] require the target and the common flow regions to be given by a conjunction of sub-level sets of smooth functions and the defining polynomials (except the exit boundary) to be conserved quantities of the system. Conditions for staging sets are more general and less conservative.

Lastly, unlike previous approaches, we completely decouple the progress property (using progress functions) from conditions for over-approximating the reachable set of the system (using staging sets).

7 Conclusion

In this paper we have presented a very general proof principle for eventuality properties of continuous systems governed by polynomial ODEs under semi-algebraic evolution constraints that works without computing the solutions and can be shown to both extend and generalize previous approaches in [30,31,26,33]. We have presented a formalization of our method in a proof rule (SP) which is very well suited for use as part of a formal verification calculus for hybrid systems.

Our work addressed some important theoretical limitations inherent in available methods for eventuality verification; however, much future work remains before scalable formal verification tools can emerge and be applied in practice to large, industrially relevant verification problems. The two most important practical obstacles are manifested in the current dearth of scalable methods for continuous invariant (staging set) generation and limited tool support for searching for progress functions. As we have discussed, searching for staging sets is no different to generating continuous invariants, so improved invariant generation tools developed for safety verification of continuous systems can be applied to search for staging sets. Automatically generating progress functions is likewise a difficult problem and would greatly benefit from improved tools for non-linear optimization. We should note that these problems are pervasive in direct methods and are not limited to safety and liveness verification. In the control and dynamical systems community, direct methods for proving the property of *stability* [19] are considered standard, but do not provide the means of computing the stability-proving (Lyapunov) function; this task is delegated to the user and is the focus of much ongoing work to facilitate their automatic discovery (see e.g. [24]).

Acknowledgements The authors would like to thank Dr. Khalil Ghorbal at Carnegie Mellon University for his detailed technical scrutiny and suggestions for improving an early version of this work, Dr. André Platzer at the same institution for kindly responding to our query concerning the method of differential variants and extend special thanks to the anonymous reviewers for their diligent reading and valuable feedback.

References

1. Alpern, B., Schneider, F.B.: Defining liveness. Information processing letters 21(4), 181–185 (1985)
2. Berz, M., Makino, K.: Verified integration of ODEs and flows using differential algebraic methods on high-order Taylor models. Reliable Computing 4(4), 361–369 (1998)
3. Bhatia, N.P., Szegő, G.P.: Stability Theory of Dynamical Systems, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete, vol. 161. Springer-Verlag (1970)
4. Blanchini, F.: Set invariance in control. Automatica 35(11), 1747–1767 (1999)
5. Blanchini, F., Miani, S.: Set-Theoretic Methods in Control. Systems & Control : Foundations & Applications, Birkhäuser (2008)
6. Collins, G.E.: Hauptvortrag: Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In: Barkhage, H. (ed.) Automata Theory and Formal Languages. LNCS, vol. 33, pp. 134–183. Springer (1975)
7. Davenport, J.H., Heintz, J.: Real quantifier elimination is doubly exponential. J. Symb. Comput. 5(1/2), 29–35 (1988)
8. Demyanov, V.F.: The solution of minimaximin problems. USSR Computational Mathematics and Mathematical Physics 10(3), 44 – 55 (1970)
9. Dolzmann, A., Sturm, T., Weispfenning, V.: Real Quantifier Elimination in Practice. In: Algorithmic Algebra and Number Theory. pp. 221–247 (1998)
10. Ekici, E.: On the directional differentiability properties of the max-min function. Boletín de la Asociación Matemática Venezolana X(1), 35–42 (2003)
11. Fehnker, A., Krogh, B.H.: Hybrid system verification is not a sinecure. In: Automated Technology for Verification and Analysis, pp. 263–277. Springer (2004)
12. Ghorbal, K., Platzer, A.: Characterizing algebraic invariants by differential radical invariants. In: Ábrahám, E., Havelund, K. (eds.) TACAS. Lecture Notes in Computer Science, vol. 8413, pp. 279–294. Springer (2014)
13. Henzinger, T.A.: The theory of hybrid automata. In: Proceedings, 11th Annual IEEE Symposium on Logic in Computer Science. pp. 278–292 (1996)
14. Immler, F.: Formally verified computation of enclosures of solutions of ordinary differential equations. In: NASA Formal Methods - 6th International Symposium, NFM 2014, Houston, TX, USA, April 29 - May 1, 2014. Proceedings. pp. 113–127 (2014)
15. Immler, F.: Verified reachability analysis of continuous systems. In: Baier, C., Tinelli, C. (eds.) TACAS (to appear). LNCS, vol. 9035. Springer (2015)
16. Lamport, L.: Proving the correctness of multiprocess programs. IEEE Transactions on Software Engineering 3(2), 125–143 (March 1977)
17. Liu, J., Lv, J., Quan, Z., Zhan, N., Zhao, H., Zhou, C., Zou, L.: A calculus for hybrid CSP. In: Ueda, K. (ed.) Programming Languages and Systems, LNCS, vol. 6461, pp. 1–15. Springer (2010)
18. Liu, J., Zhan, N., Zhao, H.: Computing semi-algebraic invariants for polynomial dynamical systems. In: Chakraborty, S., Jerraya, A., Baruah, S.K., Fischmeister, S. (eds.) EMSOFT. pp. 97–106. ACM (2011)
19. Lyapunov, A.M.: The general problem of stability of motion. Kharkov Mathematical Society, Kharkov (1892)
20. Nagumo, M.: Über die Lage der Integralkurven gewöhnlicher Differentialgleichungen. In: Proceedings of the Physico-Mathematical Society of Japan. vol. 24, pp. 551–559 (May 1942)
21. Navarro-López, E.M., Carter, R.: Hybrid automata: an insight into the discrete abstraction of discontinuous systems. International Journal of Systems Science 42(11), 1883–1898 (2011)

22. Neher, M., Jackson, K.R., Nedialkov, N.S.: On Taylor model based integration of ODEs. SIAM Journal on Numerical Analysis 45(1), 236–262 (2007)
23. Owicki, S., Lamport, L.: Proving liveness properties of concurrent programs. ACM Transactions on Programming Languages and Systems (TOPLAS) 4(3), 455–495 (1982)
24. Parrilo, P.A.: Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization. Engineering and applied science, control and dynamical systems, California Institute of Technology (May 2000)
25. Platzer, A.: Differential dynamic logic for hybrid systems. J. Autom. Reasoning 41(2), 143–189 (2008)
26. Platzer, A.: Differential-algebraic dynamic logic for differential-algebraic programs. J. Log. Comput. 20(1), 309–352 (2010)
27. Platzer, A., Clarke, E.M.: Computing differential invariants of hybrid systems as fixedpoints. In: Gupta, A., Malik, S. (eds.) CAV. LNCS, vol. 5123, pp. 176–189. Springer (2008)
28. Poincaré, H.: Mémoire sur les courbes définies par une équation différentielle. Journal de mathématiques pures et appliquées 7, 3, 4, 375–422, 251–296, 167–224 (1881, 1882, 1885)
29. Prajna, S., Jadbabaie, A.: Safety verification of hybrid systems using barrier certificates. In: In Hybrid Systems: Computation and Control. pp. 477–492. Springer (2004)
30. Prajna, S., Rantzer, A.: Primal–dual tests for safety and reachability. In: Morari, M., Thiele, L. (eds.) Hybrid Systems: Computation and Control, Lecture Notes in Computer Science, vol. 3414, pp. 542–556. Springer Berlin Heidelberg (2005)
31. Ratschan, S., She, Z.: Providing a basin of attraction to a target region of polynomial systems by computation of Lyapunov-like functions. SIAM J. Control Optim. 48(7), 4377–4394 (Jul 2010)
32. Richardson, D.: Some undecidable problems involving elementary functions of a real variable. Journal of Symbolic Logic 33(4), 514–520 (12 1968)
33. Stiver, J.A., Koutsoukos, X.D., Antsaklis, P.J.: An invariant-based approach to the design of hybrid control systems. International Journal of Robust and Nonlinear Control 11(5), 453–478 (2001)
34. Taly, A., Tiwari, A.: Deductive verification of continuous dynamical systems. In: Kannan, R., Kumar, K.N. (eds.) FSTTCS. LIPIcs, vol. 4, pp. 383–394. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (2009)
35. Tarski, A.: A decision method for elementary algebra and geometry. Bulletin of the American Mathematical Society 59 (1951)
36. Wang, T.C., Lall, S., West, M.: Polynomial level-set method for polynomial system reachable set estimation. IEEE Transactions on Automatic Control 58(10), 2508–2521 (2013)