https://doi.org/10.1007/s00165-020-00525-0
The Author(s) 2021
Formal Aspects of Computing (2021) 33: 461–518

Formal Aspects of Computing

An axiomatic approach to existence and liveness for differential equations

Yong Kiam Tan and André Platzer

Computer Science Department, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, USA

Abstract. This article presents an axiomatic approach for deductive verification of existence and liveness for ordinary differential equations (ODEs) with differential dynamic logic (dL). The approach yields proofs that the solution of a given ODE exists long enough to reach a given target region without leaving a given evolution domain. Numerous subtleties complicate the generalization of discrete liveness verification techniques, such as loop variants, to the continuous setting. For example, ODE solutions may blow up in finite time or their progress towards the goal may converge to zero. These subtleties are handled in dL by successively refining ODE liveness properties using ODE invariance properties which have a complete axiomatization. This approach is widely applicable: several liveness arguments from the literature are surveyed and derived as special instances of axiomatic refinement in dL. These derivations also correct several soundness errors in the surveyed literature, which further highlights the subtlety of ODE liveness reasoning and the utility of an axiomatic approach. An important special case of this approach deduces (global) existence properties of ODEs, which are a fundamental part of every ODE liveness argument. Thus, all generalizations of existence properties and their proofs immediately lead to corresponding generalizations of ODE liveness arguments. Overall, the resulting library of common refinement steps enables both the sound development and justification of new ODE existence and of liveness proof rules from dL axioms. These insights are put into practice through an implementation of ODE liveness proofs in the KeYmaera X theorem prover for hybrid systems.

Keywords: Differential equations, Liveness, Global existence, Differential dynamic logic

1. Introduction

Hybrid systems are mathematical models describing discrete and continuous dynamics, and interactions thereof. This flexibility makes them natural models of cyber-physical systems (CPSs) which feature interactions between discrete computational control and continuous real world physics [Alu15, Pla18]. Formal verification of hybrid systems is of significant practical interest because the CPSs they model frequently operate in safety-critical settings. Verifying properties of the differential equations describing the continuous dynamics present in hybrid system models is a key aspect of any such endeavor.

Correspondence to: Yong Kiam Tan, e-mail: yongkiat@cs.cmu.edu

Table 1. Surveyed ODE liveness arguments with highlighting in blue for soundness-critical corrections identified in this article

Application	Without domain constraints		With domain constraints	
Hybrid systems verification [Pla10]	OK	(Cor. 12)	if open/closed, initially false	(Cor. 18)
Automated ODE verification [PR05, PR07]	[PR07, Remark 3.6]	is incorrect	if conditions checked globally	(Cor. 23)
Finding basin of attraction [RS10]	if compact	(Cor. 17)	if compact	(Cor. 20)
Staging set-based ODE liveness proofs [SJ15]	OK	(Cor. 15)	OK	(Cor. 21)
Switching logic synthesis [TT10]	if global solutions	(Cor. 13)	if global solutions	(Cor. 19)

The applications (and corrections, if any) for each surveyed argument is briefly described here. The referenced corollaries are corresponding derived proof rules with details of the corrections

This article focuses on deductive verification of *existence* and *liveness*[1] properties for ordinary differential equations (ODEs), i.e., the question whether an ODE solution exists for long enough to reach a given region without leaving its domain of evolution. Such questions can be phrased naturally in differential dynamic logic (dL) [Pla10, Pla12b, Pla17a, Pla18], a logic for *deductive verification* of hybrid systems whose relatively complete axiomatization [Pla12a, Pla17a] lifts ODE verification results to hybrid systems, and whose theorem prover, KeYmaera X [FMQ+15], enables an implementation.

For discrete systems, methods for proving liveness are well-known: loop variants show that discrete loops eventually reach a desired goal [Har79], while temporal logic is used to specify and study liveness properties in concurrent and infinitary settings [MP92, OL82]. However, the deduction of (continuous) ODE liveness properties is hampered by several difficulties: (i) solutions of ODEs may converge towards a goal without ever reaching it, (ii) solutions of nonlinear ODEs may blow up in finite time leaving insufficient time for the desired goal to be reached, and (iii) the goal may be reachable but only by (illegally) leaving the evolution domain constraint. In contrast, invariance properties for ODEs are better understood [Pla10, GP14, LZZ11] and have a complete dL axiomatization [PT20]. Motivated by the aforementioned difficulties, this article presents dL axioms enabling systematic, step-by-step refinement of ODE liveness properties, where each step is justified using an ODE invariance property. This refinement approach is a powerful framework for understanding ODE liveness arguments because it brings the full deductive power of dL's ODE invariance proof rules to bear on liveness proofs. Using invariance (or safety) properties to deduce liveness is a well-known proof technique for (discrete) concurrent systems [MP92, OL82]. This article shows that those ideas work just as well in the continuous setting—as long as the aforementioned difficulties are appropriately handled.

To demonstrate the applicability of the approach, this article surveys several arguments from the literature and derives them all as (corrected) dL proof rules, see Table 1. This logical presentation has two key benefits:

- The proof rules are *syntactically derived* from sound axioms of dL, which guarantees their correctness. Many of the surveyed arguments contain subtle soundness errors (Table 1, middle and right). These errors do not diminish the surveyed work. Rather, they emphasize the need for an axiomatic, uniform way of presenting and analyzing ODE liveness arguments instead of relying on ad hoc approaches.
- The approach identifies common refinement steps that form a basis for the surveyed liveness arguments drawn from various applications (Table 1, left). This library of building blocks enables sound development and justification of new ODE liveness proof rules, e.g., by generalizing individual refinement steps or by exploring different combinations of those steps. Corollaries 14, 16, and 22 are examples of new ODE liveness proof rules that can be derived and justified from the uniform approach that this article follows.

This article extends the authors' earlier conference version [TP19]. The key new insight is that all of the aforementioned liveness arguments (Table 1) are based on reducing liveness properties of ODEs to assumptions about sufficient existence duration for their solutions. In fact, many of those arguments become significantly simpler (and sound) when the ODEs of concern are assumed to have global solutions, i.e., they do not blow up in finite time. It is reasonable and commonplace to make such an assumption for the continuous dynamics in models of CPSs [Alu15, Section 6]. After all, mechanical systems do not simply cease

[1] The form of ODE liveness considered in this article is in the sense of Owicki and Lamport [OL82] for concurrent programs within their (linear) temporal logic. Liveness for ODEs has sometimes been called *eventuality* [PR07, SJ15] and *reachability* [TT10]. To minimize ambiguity, this article refers to the property as *liveness*, with a precise formal definition in Sect. 2. Other advanced notions of liveness for ODEs are discussed in Sect. 8.

to exist after a short time! An example from control theory is Lyapunov stability which guarantees global solutions near stable equilibria [Kha92, Definition 4.1][HC08, Theorem 3.1]. Control systems are designed to always operate near stable equilibria and so always have global solutions. Logically though, making an *a priori* assumption of global existence for ODEs means that the correctness of any subsequent verification results for the ODEs and hybrid system models are conditional on an unproved existence duration hypothesis. While global existence is known to hold for linear systems, even the simplest nonlinear ODEs (see Sect. 4) fail to meet the hypothesis without further assumptions. This article therefore adopts the view that (global) existence should be *proved* rather than *assumed* for the continuous dynamics in hybrid systems.

The new contributions of this article beyond the authors' earlier conference version [TP19] are:

- Section 4 presents deductive dL proofs of global existence for ODE solutions. Together with the liveness proofs of Sects. 5 and 6, this enables *unconditional* proofs of ODE liveness properties entirely within the uniform dL refinement framework without existence presuppositions.
- Section 7 shows how to apply the insights from Sects. 4–6 in practice. This includes: (i) the design of proof rules that are practically useful and well-suited for implementation (Sect. 7.1) and (ii) the design of proof support to aid users in existence and liveness proofs (Sect. 7.2).

The practical insights of Sect. 7 are drawn from an implementation of ODE liveness proof rules in the KeYmaera X theorem prover for hybrid systems [FMQ$^+$15]. The unconditional liveness proofs enabled by Sects. 4–6 fit particularly well with an implementation in KeYmaera X because axiomatic refinement closely mirrors KeYmaera X's design principles. KeYmaera X implements dL's uniform substitution calculus [Pla17a] and it is designed to minimize the soundness-critical code that has to be trusted in order to guarantee its verification results. On top of this soundness-critical core, KeYmaera X's non-soundness-critical tactics framework [FMBP17] adds support and automation for proofs. Liveness proofs are similarly based on a series of small refinement steps which are, in turn, implemented as (untrusted) tactics based on a small basis of derived refinement axioms. More complicated liveness arguments, such as those from Table 1 or from new user insights, are implemented by piecing those tactics together using tactic combinators [FMBP17]. The implementation required minor changes to ≈155 lines of soundness-critical code in KeYmaera X, while the remaining ≈1500 lines implement ODE existence and liveness proof rules as tactics. These additions suffice to prove all of the examples in this article and in ODE models elsewhere [SJ15, BTM$^+$19] (Sect. 7.2.3).

Throughout this article, core dL axioms underlying the refinement approach are presented as lemmas, which are summarized and proved in Appendix A. Existence and liveness proof rules that are derived syntactically from those axioms, e.g., Table 1, are listed as corollaries and their derivations are given in Appendix B. Counterexamples explaining the soundness errors in Table 1 are given in Appendix C.

2. Background: differential dynamic logic

This section reviews the syntax and semantics of dL, focusing on its continuous fragment which has a complete axiomatization for ODE invariants [PT20]. Full presentations of dL, including its discrete fragment, are available elsewhere [Pla12b, Pla17a, Pla18].

2.1. Syntax

The grammar of dL terms is as follows, where $x \in \mathbb{V}$ is a variable and $c \in \mathbb{Q}$ is a rational constant. These terms are polynomials over the set of variables $\mathbb{V}$:

$$p, q \ ::= \ x \mid c \mid p + q \mid p \cdot q$$

Notably, dL also supports term language extensions [PT20] that would enable, e.g., the use of exponentials and trigonometric functions. These extensions are compatible with the results presented in this article, but are omitted for simplicity as they are not the main focus of this article.

The grammar of dL formulas is as follows, where $\sim \in \{=, \neq, \geq, >, \leq, <\}$ is a comparison operator and α is a hybrid program:

$$\phi, \psi \ ::= \ \overbrace{p \sim q \mid \phi \wedge \psi \mid \phi \vee \psi \mid \neg \phi \mid \forall v \, \phi \mid \exists v \, \phi}^{\text{First-order formulas of real arithmetic } P,Q} \mid [\alpha]\phi \mid \langle \alpha \rangle \phi$$

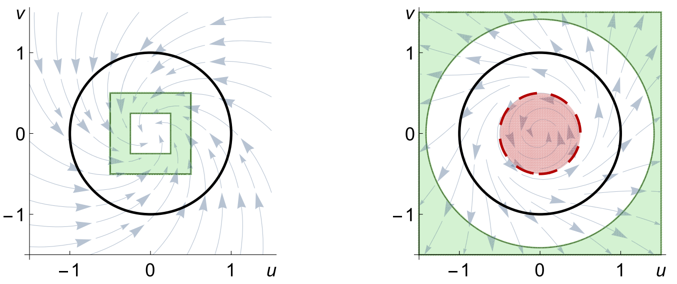


Fig. 1. Visualization of α_l (left) and α_n (right). Solutions of α_l globally spiral towards the origin. In contrast, solutions of α_n spiral inwards within the inner red disk (dashed boundary), but spiral outwards otherwise. For both ODEs, solutions starting on the black unit circle eventually enter their respective shaded green goal regions. The ODE α_n also exhibits finite-time blow up of solutions outside the red disk.

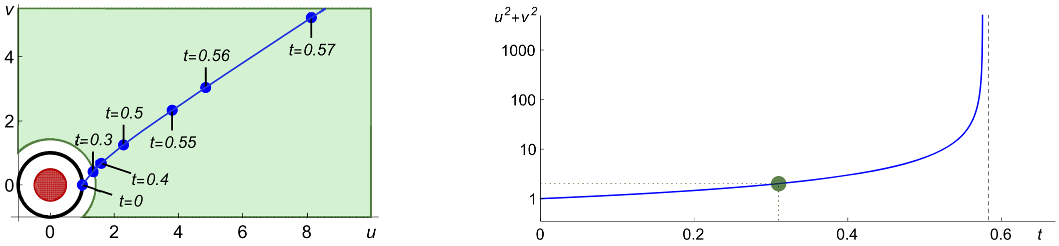


Fig. 2. Two views of the ODE α_n evolving from initial state $u = 1, v = 0$ over time t. The left plot shows its trajectory in the u, v plane (cf. Fig. 1) while the right plot shows the squared Euclidean norm $u^2 + v^2$ evolving over time t (with logarithmic scaling for the vertical axis). The solution blows up in finite time with norm approaching ∞ as t approaches 0.58 (rounded up, black dashed asymptote). Nevertheless, the solution reaches the green goal region $u^2 + v^2 \geq 2$ from Fig. 1 at $t \approx 0.31$ (rounded up, green dot) before blowing up.

The notation $p \succcurlyeq q$ (resp. $\preccurlyeq$) is used when the comparison operator can be either $\geq$ or $>$ (resp. $\leq$ or $<$). Other standard logical connectives, e.g., $\rightarrow, \leftrightarrow$, are definable as in classical logic. Formulas not containing the modalities $[\cdot], \langle\cdot\rangle$ are formulas of first-order real arithmetic and are written as P, Q. The box ($[\alpha]\phi$) and diamond ($\langle\alpha\rangle\phi$) modality formulas express dynamic properties of the hybrid program α. This article focuses on *continuous* programs, where α is given by a system of ODEs $x' = f(x) \,\&\, Q$. Here, $x' = f(x)$ is an n-dimensional system of differential equations, $x'_1 = f_1(x), \ldots, x'_n = f_n(x)$, over variables $x = (x_1, \ldots, x_n)$, where the LHS x'_i is the time derivative of x_i and the RHS $f_i(x)$ is a polynomial over variables x. The ODEs $x' = f(x)$ are *autonomous* as they do not depend explicitly on time on the RHS [Kha92]. A useful transformation is to add a clock variable t to the system with $x' = f(x, t), t' = 1$ if time dependency on the RHS is needed. The domain constraint Q specifies the set of states in which the ODE is allowed to evolve continuously. When there is no domain constraint, i.e., Q is the formula *true*, the ODE is also written as $x' = f(x)$. For n-dimensional vectors x, y, the dot product is $x \cdot y \overset{\text{def}}{=} \sum_{i=1}^{n} x_i y_i$ and $\|x\|^2 \overset{\text{def}}{=} \sum_{i=1}^{n} x_i^2$ denotes the squared Euclidean norm. Other norms are explicitly defined in this article when used.

The following two running example ODEs α_l and α_n are visualized in Fig. 1 with directional arrows corresponding to their RHS evaluated at points on the plane:

$$\alpha_l \equiv u' = -v - u, v' = u - v \tag{1}$$

$$\alpha_n \equiv u' = -v - u\left(\frac{1}{4} - u^2 - v^2\right), v' = u - v\left(\frac{1}{4} - u^2 - v^2\right) \tag{2}$$

The ODE α_l is *linear* because its RHS depends linearly on u and v while α_n is *nonlinear* because of the cubic terms in its RHS. The nonlinearity of α_n results in more complex behavior for its solutions, e.g., the difference in spiraling behavior inside or outside the red disk shown in Fig. 1. In fact, solutions of α_n blow up in finite time iff they start outside the disk characterized by $u^2 + v^2 \leq \frac{1}{4}$, whereas finite-time blow up is impossible for linear ODEs like α_l [Chi06, Wal98]. An illustration of finite-time blow up for α_n from an initial state outside the red disk is shown in Fig. 2. This phenomenon is precisely defined and investigated in Sect. 4, which enables formal proofs of the aforementioned (absence of) finite-time blow up.

When terms (or formulas) appear in contexts involving ODEs $x' = f(x)$, it is sometimes necessary to restrict the set of free variables they are allowed to mention. In this article, these restrictions are always stated explicitly and are also indicated as arguments to terms (or formulas), e.g., $p()$ means the term p does not mention any of $x_1, \dots, x_n$ as free variables, while $P(x)$ means the formula P may mention all of them. This understanding of variable dependencies is made precise using function and predicate symbols in dL's uniform substitution calculus [Pla17a].

2.2. Semantics

States $\omega : \mathbb{V} \to \mathbb{R}$ assign real values to each variable in $\mathbb{V}$; the set of all states is written $\mathbb{S}$. The semantics of polynomial term p in state $\omega \in \mathbb{S}$ is the real value $\omega[\![p]\!]$ of the corresponding polynomial function evaluated at ω. The semantics of dL formula ϕ is defined compositionally [Pla17a, Pla18] as the set of states $[\![\phi]\!] \subseteq \mathbb{S}$ in which that formula is true. The semantics of first-order logical connectives are defined as usual, e.g., $[\![\phi \land \psi]\!] = [\![\phi]\!] \cap [\![\psi]\!]$. For ODEs, the semantics of the modal operators is defined directly as follows. Let $\omega \in \mathbb{S}$ and $\boldsymbol{\varphi} : [0, T) \to \mathbb{S}$ (for some $0 < T \le \infty$), be the unique solution maximally extended to the right [Chi06, Wal98] for the ODE $x' = f(x)$ with initial value $\boldsymbol{\varphi}(0) = \omega$, then:

$$\omega \in [\![[x' = f(x) \,\&\, Q]\phi]\!] \text{ iff for all } 0 \le \tau < T \text{ where } \boldsymbol{\varphi}(\zeta) \in [\![Q]\!] \text{ for all } 0 \le \zeta \le \tau\text{: } \boldsymbol{\varphi}(\tau) \in [\![\phi]\!]$$
$$\omega \in [\![\langle x' = f(x) \,\&\, Q\rangle\phi]\!] \text{ iff there exists } 0 \le \tau < T \text{ such that } \boldsymbol{\varphi}(\zeta) \in [\![Q]\!] \text{ for all } 0 \le \zeta \le \tau \text{ and } \boldsymbol{\varphi}(\tau) \in [\![\phi]\!]$$

Informally, the *safety* property $[x' = f(x) \,\&\, Q]\phi$ is true in initial state ω if *all* states reached by following the ODE from ω while remaining in the domain constraint Q satisfy postcondition ϕ. Dually, the *liveness* property $\langle x' = f(x) \,\&\, Q\rangle\phi$ is true in initial state ω if *some* state which satisfies the postcondition ϕ is eventually reached in *finite* time by following the ODE from ω while staying in domain constraint Q at all times. Figure 1 suggests that formulas[2] $\langle\alpha_l\rangle(\frac{1}{4} \le \|(u,v)\|_\infty \le \frac{1}{2})$ and $\langle\alpha_n\rangle u^2 + v^2 \ge 2$ are true for initial states ω on the unit circle. These liveness properties are rigorously proved in Examples 4 and 5 respectively.

Variables $y \in \mathbb{V} \setminus \{x\}$ not occurring on the LHS of ODE $x' = f(x)$ remain constant along solutions $\boldsymbol{\varphi} : [0, T) \to \mathbb{S}$ of the ODE, with $\boldsymbol{\varphi}(\tau)(y) = \boldsymbol{\varphi}(0)(y)$ for all $\tau \in [0, T)$. Since only the values of $x = (x_1, \dots, x_n)$ change along the solution $\boldsymbol{\varphi}$, the solution may also be viewed geometrically as a trajectory in $\mathbb{R}^n$, dependent on the initial values of the constant *parameters* y. Similarly, the values of terms and formulas depend only on the values of their free variables [Pla17a]. Thus, terms (or formulas) whose free variables are all parameters for $x' = f(x)$ also have provably constant (truth) values along solutions of the ODE. For formulas ϕ that only mention free variables x, $[\![\phi]\!]$ can also be viewed geometrically as a subset of $\mathbb{R}^n$. Such a formula is said to *characterize* a (topologically) open (resp. closed, bounded, compact) set with respect to variables x iff the set $[\![\phi]\!] \subseteq \mathbb{R}^n$ is topologically open (resp. closed, bounded, compact) with respect to the Euclidean topology. These topological conditions are used as side conditions for some of the axioms and proof rules in this article. In Appendix A.3, a more general definition of these side conditions is given for formulas ϕ that mention parameters y. These side conditions are decidable [BCR98] when ϕ is a formula of first-order real arithmetic and there are simple syntactic criteria for checking if they hold (Appendix A.3).

Formula ϕ is valid iff $[\![\phi]\!] = \mathbb{S}$, i.e., ϕ is true in all states. If the formula $I \to [x' = f(x) \,\&\, Q]I$ is valid, the formula I is an *invariant* of the ODE $x' = f(x) \,\&\, Q$. Unfolding the semantics, this means that from any initial state ω satisfying I, all states reached by the solution of the ODE $x' = f(x)$ from ω while staying in the domain constraint Q satisfy I. Similarly, if the liveness formula $R \to \langle x' = f(x) \,\&\, Q\rangle P$ is valid then, for all initial states ω satisfying assumptions R, the target region P can be reached in finite time by following the ODE solution from ω while remaining in the domain constraint Q.

2.3. Proof calculus

All derivations are presented in a classical sequent calculus with the usual rules for manipulating logical connectives and sequents. The semantics of *sequent* $\Gamma \vdash \phi$ is equivalent to the formula $(\bigwedge_{\psi \in \Gamma} \psi) \to \phi$ and

[2] $\|\cdot\|_\infty$ denotes the supremum norm, with $\|x\|_\infty \equiv \max_{i=1}^n |x_i|$ for an n-dimensional vector x. The inequality $\|(u,v)\|_\infty \le \frac{1}{2}$ is expressible in first-order real arithmetic as $u^2 \le \frac{1}{4} \land v^2 \le \frac{1}{4}$. Similarly, $\frac{1}{4} \le \|(u,v)\|_\infty$ is expressible as $\frac{1}{16} \le u^2 \lor \frac{1}{16} \le v^2$.

a sequent is *valid* iff its corresponding formula is valid. Completed branches in a sequent proof are marked with $*$. First-order real arithmetic is decidable [BCR98] so proof steps are labeled with $\mathbb{R}$ whenever they follow from real arithmetic. An axiom (schema) is *sound* iff all its instances are valid. Proof rules are *sound* iff validity of all premises (above the rule bar) entails validity of the conclusion (below the rule bar). Axioms and proof rules are *derivable* if they can be deduced from sound dL axioms and proof rules. Soundness of the dL axiomatization ensures that derived axioms and proof rules are sound [Pla17a, Pla18].

The dL proof calculus (briefly recalled below) is *complete* for ODE invariants [PT20], i.e., any true ODE invariant expressible in first-order real arithmetic can be proved in the calculus. The proof rule $\mathrm{dI}_{\succcurlyeq}$ (below) uses the *Lie derivative* of polynomial p with respect to the ODE $x' = f(x)$, which is defined as the term $\mathcal{L}_{f(x)}(p) \overset{\text{def}}{=} \sum_{x_i \in x} \frac{\partial p}{\partial x_i} f_i(x)$. Higher Lie derivatives $\dot{p}^{(i)}$ are defined inductively: $\dot{p}^{(0)} \overset{\text{def}}{=} p, \dot{p}^{(i+1)} \overset{\text{def}}{=} \mathcal{L}_{f(x)}(\dot{p}^{(i)}), \dot{p} \overset{\text{def}}{=} \dot{p}^{(1)}$. Syntactically, Lie derivatives $\dot{p}^{(i)}$ are polynomials in the term language and they are provably definable in dL using differentials [Pla17a]. Semantically, the value of Lie derivative $\dot{p}$ is equal to the time derivative of the value of p along solution $\boldsymbol{\varphi}$ of the ODE $x' = f(x)$.

Lemma 1 (Axioms and proof rules of dL [Pla17a, Pla18, PT20])**.** *The following are sound axioms and proof rules of* dL*.*

$$\langle\cdot\rangle\quad \langle\alpha\rangle P \leftrightarrow \neg[\alpha]\neg P \qquad\qquad \mathrm{K}\quad [\alpha](R \rightarrow P) \rightarrow ([\alpha]R \rightarrow [\alpha]P)$$

$$\mathrm{dI}_{\succcurlyeq}\ \frac{Q \vdash \dot{p} \geq \dot{q}}{\Gamma, p \succcurlyeq q \vdash [x' = f(x)\,\&\,Q]p \succcurlyeq q} \qquad \text{(where } \succcurlyeq \text{ is either } \geq \text{ or } >\text{)}$$

$$\mathrm{dC}\ \frac{\Gamma \vdash [x' = f(x)\,\&\,Q]C \quad \Gamma \vdash [x' = f(x)\,\&\,Q \land C]P}{\Gamma \vdash [x' = f(x)\,\&\,Q]P} \qquad \mathrm{dW}\ \frac{Q \vdash P}{\Gamma \vdash [x' = f(x)\,\&\,Q]P}$$

$$\mathrm{M}[']\ \frac{Q, R \vdash P \quad \Gamma \vdash [x' = f(x)\,\&\,Q]R}{\Gamma \vdash [x' = f(x)\,\&\,Q]P} \qquad \mathrm{M}\langle'\rangle\ \frac{Q, R \vdash P \quad \Gamma \vdash \langle x' = f(x)\,\&\,Q\rangle R}{\Gamma \vdash \langle x' = f(x)\,\&\,Q\rangle P}$$

Proof in Appendix A.1.

Axiom $\langle\cdot\rangle$ expresses the duality between the box and diamond modalities. It is used to switch between the two in proofs and to dualize axioms between the box and diamond modalities. Axiom K is the modus ponens principle for the box modality. Differential invariants $\mathrm{dI}_{\succcurlyeq}$ say that if the Lie derivatives obey the inequality $\dot{p} \geq \dot{q}$, then $p \succcurlyeq q$ is an invariant of the ODE. Differential cuts dC say that if one can separately prove that formula C is always satisfied along the solution, then C may be assumed in the domain constraint when proving the same for formula P. In the box modality, solutions are restricted to stay in the domain constraint Q. Thus, differential weakening dW says that postcondition P is always satisfied along solutions if it is already implied by the domain constraint. Using dW, K, $\langle\cdot\rangle$, the final two monotonicity proof rules M['], M⟨'⟩ for differential equations are derivable. They strengthen the postcondition from P to R, assuming domain constraint Q, for the box and diamond modalities respectively.

Notice that the premises of several proof rules in Lemma 1, e.g., $\mathrm{dI}_{\succcurlyeq}$, dW, discard all assumptions Γ on initial states when moving from conclusion to premises. This is necessary for soundness because the premises of these rules internalize reasoning that happens *along* solutions of the ODE $x' = f(x)\,\&\,Q$ rather than in the initial state. On the other hand, the truth value of constant assumptions $P()$ do not change along solutions, so they can be soundly kept across rule applications [Pla18]. These additional constant contexts are useful when working with assumptions on symbolic parameters, e.g., $v() > 0$ to model a (constant) positive velocity.

Besides rules $\mathrm{dI}_{\succcurlyeq}$, dC, dW, the key to completeness for ODE invariance proofs in dL is the *differential ghosts* [Pla17a, PT20] axiom shown below. The $\exists$ quantifier in the axiom can be replaced with a $\forall$ quantifier.

$$\mathrm{DG}\quad [x' = f(x)\,\&\,Q(x)]P(x) \leftrightarrow \exists y\, [x' = f(x), y' = a(x)y + b(x)\,\&\,Q(x)]P(x)$$

Axiom DG says that, in order to prove safety postcondition $P(x)$ for the ODE $x' = f(x)$, it suffices to prove $P(x)$ for a larger system with an added ODE $y' = a(x)y + b(x)$ that is linear in the ghost variable y (because $a(x), b(x)$ do not mention y). Intuitively, this addition is sound because the ODE $x' = f(x)$ does not mention the added variables y, and so the evolution of $x' = f(x)$ should be unaffected by the addition of an ODE for y. However, this intuition only works if the additional ODEs do not unsoundly restrict the duration of the original solution by blowing up too early [Pla17a]. The linearity restriction prevents such a blow up. Using axiom DG in a proof appears counterintuitive because the axiom tries to prove a property for a seemingly easier (lower-dimensional) ODE by instead studying a more difficult (higher-dimensional) one! Yet, the DG axiom, is crucially used for completeness because it enables mathematical (or geometric) transformations to be carried out syntactically in the dL proof calculus [PT20]. This completeness result only requires a scalar version of DG that adds one ghost variable at time. More general vectorial versions of the axiom (where $a(x)$ is a matrix and $b(x)$ is a vector) have also been used elsewhere [PT20]. This article uses a new vectorial generalization that allows differential ghosts with provably bounded ODEs to be added.

Lemma 2 (Bounded differential ghosts)**.** *The following bounded differential ghosts axiom BDG is sound, where $y = (y_1, \ldots, y_m)$ is a m-dimensional vector of fresh variables (not appearing in x), $g(x, y)$ is a corresponding m-dimensional vector of terms, and $\|y\|^2$ is the squared Euclidean norm of y. Term $p(x)$ and formulas $P(x), Q(x)$ are dependent only on free variables x (and not y).*

$$\text{BDG}\quad \begin{array}{l}[x' = f(x), y' = g(x, y)\,\&\,Q(x)]\,\|y\|^2 \le p(x)\\ \rightarrow \big([x' = f(x)\,\&\,Q(x)]P(x) \leftrightarrow [x' = f(x), y' = g(x, y)\,\&\,Q(x)]P(x)\big)\end{array}$$

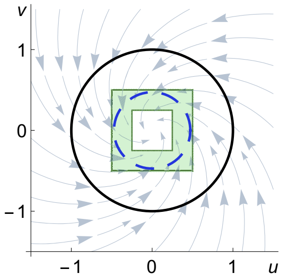
Proof in Appendix A.1.

Like DG, axiom BDG allows an arbitrary vector of ghost ODEs $y' = g(x, y)$ to be added syntactically to the ODEs. However, it places no syntactic restriction on the RHS of the ODE (such as linearity in axiom DG). For soundness, BDG instead adds a new precondition with a bound $\|y\|^2 \le p(x)$ in terms of x on the squared norm of y along solutions of the augmented ODE. This syntactic precondition ensures that y cannot blow up before x, so that solutions of $x' = f(x), y' = g(x, y)$ have existence intervals as long as those of the solutions of $x' = f(x)$. Section 4 shows how to prove these preconditions so that axiom BDG enables ODE existence proofs through the refinement approach of Sect. 3.

3. ODE liveness via box refinements

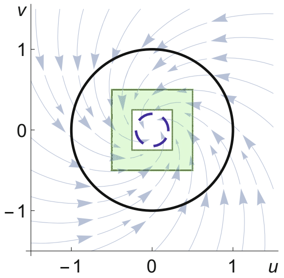
This section explains step-by-step refinement for proving ODE liveness properties in dL. Suppose that an initial liveness property $\langle x' = f(x)\,\&\,Q_0\rangle P_0$ is known for the ODE $x' = f(x)$. How could this be used to prove a desired liveness property $\langle x' = f(x)\,\&\,Q\rangle P$ for that ODE? Logically, this amounts to proving:

$$\langle x' = f(x)\,\&\,Q_0\rangle P_0 \rightarrow \langle x' = f(x)\,\&\,Q\rangle P \tag{3}$$



Proving implication (3) *refines* knowledge of the initial liveness property to the desired liveness property. As an example of such a refinement, consider the desired liveness property $\langle\alpha_l\rangle\big(\frac{1}{4} \le \|(u, v)\|_\infty \le \frac{1}{2}\big)$ for ODE α_l (1) starting from the initial circle $u^2 + v^2 = 1$ (cf. Fig. 1). Suppose the initial liveness property $\langle\alpha_l\rangle u^2 + v^2 = \frac{1}{4}$ is already proved, e.g., using the techniques of Sect. 5. As visualized on the right, ODE solutions starting from the black circle $u^2 + v^2 = 1$ eventually reach the dashed blue circle $u^2 + v^2 = \frac{1}{4}$. Since the blue circle is entirely contained in the green goal region, solutions that reach it must (trivially) also reach the goal region. Formally, the following instance of implication (3) is provable because formula $P_0 \rightarrow P$ is provable.

$$\langle\alpha_l\rangle \underbrace{\left(u^2 + v^2 = \frac{1}{4}\right)}_{P_0} \rightarrow \langle\alpha_l\rangle \underbrace{\left(\frac{1}{4} \le \|(u, v)\|_\infty \le \frac{1}{2}\right)}_{P} \tag{4}$$



Similarly, if the implication between domain constraints $Q_0 \rightarrow Q$ is provable, then implication (3) is proved by monotonicity, because any solution staying in the smaller domain Q_0 must also stay in the larger domain Q. However, neither of these monotonicity-based arguments are sufficiently powerful for liveness proofs because they do not account for the specific ODE $x' = f(x)$ under consideration at all. Returning to the ODE α_l, suppose instead that the initial (known) liveness property is $\langle\alpha_l\rangle u^2 + v^2 = \frac{1}{25}$. This is visualized on the right with a smaller dashed blue circle. The following instance of implication (3) is also valid for solutions starting from the black circle $u^2 + v^2 = 1$, but it does *not* follow from a straightforward monotonicity argument because the smaller dashed blue circle $u^2+v^2=\frac{1}{25}$ is not contained in the green goal region (formula $P_0 \rightarrow P$ is not valid).

$$\langle\alpha_l\rangle\underbrace{\left(u^2+v^2=\frac{1}{25}\right)}_{P_0}\rightarrow\langle\alpha_l\rangle\underbrace{\left(\frac{1}{4}\leq\|(u,v)\|_\infty\leq\frac{1}{2}\right)}_{P} \tag{5}$$

A proof of implication (5) requires additional information about solutions of the ODE α_l, namely, that they are continuous and the system α_l is planar. Informally, observe that it is impossible to draw a line (without lifting your pen off the page) that connects the black circle to the (smaller) dashed blue circle without crossing the green goal region. The continuous solutions of α_l are analogous to such lines and therefore must enter the green goal region before reaching the blue circle. To formalize such reasoning, this article's approach is built on refinement axioms that conclude instances of implication (3), like (4) and (5), from box modality formulas involving the ODE $x'=f(x)$. The following are four ODE refinement axioms of dL that are used for the approach. Crucially, these axioms are *derived* from the box modality axioms presented in Sect. 2.3 by exploiting the logical duality between the box and diamond modalities of dL. This makes it possible to build liveness arguments from a sound and parsimonious logical foundation.

Lemma 3 (Diamond ODE refinement axioms)**.** *The following $\langle\cdot\rangle$ ODE refinement axioms are derivable in* dL*. In axioms* BDG$\langle\cdot\rangle$, DDG$\langle\cdot\rangle$*, $y=(y_1,\ldots,y_m)$ is an m-dimensional vector of fresh variables (not appearing in x) and $g(x,y)$ is a corresponding m-dimensional vector of terms. Terms $p(x), L(x), M(x)$ and formulas $P(x), Q(x)$ are dependent only on free variables x (and not y).*

$$\mathrm{K}\langle\&\rangle \quad [x'=f(x)\,\&\,Q\wedge\neg P]\neg G\rightarrow\big(\langle x'=f(x)\,\&\,Q\rangle G\rightarrow\langle x'=f(x)\,\&\,Q\rangle P\big)$$

$$\mathrm{DR}\langle\cdot\rangle \quad [x'=f(x)\,\&\,R]Q\rightarrow\big(\langle x'=f(x)\,\&\,R\rangle P\rightarrow\langle x'=f(x)\,\&\,Q\rangle P\big)$$

$$\mathrm{BDG}\langle\cdot\rangle \quad \begin{array}{l}[x'=f(x),y'=g(x,y)\,\&\,Q(x)]\,\|y\|^2\leq p(x)\\ \rightarrow\big(\langle x'=f(x)\,\&\,Q(x)\rangle P(x)\rightarrow\langle x'=f(x),y'=g(x,y)\,\&\,Q(x)\rangle P(x)\big)\end{array}$$

$$\mathrm{DDG}\langle\cdot\rangle \quad \begin{array}{l}[x'=f(x),y'=g(x,y)\,\&\,Q(x)]\,2y\cdot g(x,y)\leq L(x)\|y\|^2+M(x)\\ \rightarrow\big(\langle x'=f(x)\,\&\,Q(x)\rangle P(x)\rightarrow\langle x'=f(x),y'=g(x,y)\,\&\,Q(x)\rangle P(x)\big)\end{array}$$

Proof in Appendix A.2.

Axiom K$\langle\&\rangle$ is best understood in the contrapositive. Formula $[x'=f(x)\,\&\,Q\wedge\neg P]\neg G$ says G never happens along the solution while $\neg P$ holds. Thus, the solution cannot get to G unless it gets to P first. Axiom K$\langle\&\rangle$ formalizes the informal reasoning used for implication (5) above in the contrapositive, with $G\equiv u^2+v^2=\frac{1}{25}$ and $P\equiv\big(\frac{1}{4}\leq\|(u,v)\|_\infty\leq\frac{1}{2}\big)$. In the (partial) derivation shown below, the left premise requires a proof that the dashed blue circle G cannot be reached while staying outside the green goal region P while the right premise requires a proof of the initial liveness property $\langle\alpha_l\rangle\big(u^2+v^2=\frac{1}{25}\big)$ for α_l. In a sequent calculus proof, refinement steps are naturally read from top-to-bottom (downwards), while deduction steps, i.e., axiom or rule applications, are read bottom-to-top (upwards).

Deduction

$$\Big\uparrow\quad \mathrm{K}\langle\&\rangle\ \dfrac{\dfrac{\vdots}{u^2+v^2=1\vdash[\alpha_l\,\&\,\neg(\frac{1}{4}\leq\|(u,v)\|_\infty\leq\frac{1}{2})]\neg(u^2+v^2=\frac{1}{25})}\qquad\dfrac{\vdots}{u^2+v^2=1\vdash\langle\alpha_l\rangle(u^2+v^2=\frac{1}{25})}}{u^2+v^2=1\vdash\langle\alpha_l\rangle(\frac{1}{4}\leq\|(u,v)\|_\infty\leq\frac{1}{2})}\quad\Big\downarrow$$

Refinement

In refinement axiom DR$\langle\cdot\rangle$, formula $[x'=f(x)\,\&\,R]Q$ says that the ODE solution never leaves Q while staying in R, so if the solution gets to P within R, then it also gets to P within Q. The latter two refinement axioms BDG$\langle\cdot\rangle$, DDG$\langle\cdot\rangle$ are both derived from BDG. The (nested) refinement in both axioms says that, if the ODE $x' = f(x)$ can reach $P(x)$, then the ODE $x' = f(x), y' = g(x, y)$, with the added variables y, can also reach $P(x)$. Axiom BDG$\langle\cdot\rangle$ is the derived diamond version of BDG, obtained by directly dualizing the inner equivalence of BDG with $\langle\cdot\rangle$ and propositional simplification. The intuition behind BDG$\langle\cdot\rangle$ is identical to BDG: if the added ghost ODEs y never blow up in norm, then they do not affect whether the solution of the original ODEs $x' = f(x)$ can reach $P(x)$.

Axiom DDG$\langle\cdot\rangle$ is a derived, differential version of BDG$\langle\cdot\rangle$. Instead of bounding the squared norm $\|y\|^2$ explicitly, DDG$\langle\cdot\rangle$ instead limits the rate of growth of the ghost ODEs by bounding the Lie derivative[3] $\mathcal{L}_{x'=f(x),y'=g(x,y)}(\|y\|^2) = 2y \cdot g(x, y)$ of the squared norm. This derivative bound in turn implicitly bounds the squared norm of the ghost ODEs by the solution of the linear differential equation $z' = L(x)z + M(x)$, with dependency on the value of x along solutions of the ODE $x' = f(x)$. This ensures that premature blow-up of y before x itself blows up is impossible. Any refinement step using axiom DDG$\langle\cdot\rangle$ can also use axiom BDG$\langle\cdot\rangle$ since the former is derived from the latter. The advantage of DDG$\langle\cdot\rangle$ is it builds in canonical differential reasoning steps once-and-for-all (see proof of Lemma 3 and Sect. 4) which simplifies the refinement proof.

Axioms K$\langle\&\rangle$, DR$\langle\cdot\rangle$, BDG$\langle\cdot\rangle$, DDG$\langle\cdot\rangle$ all prove implication (3) in just one refinement step. Logical implication is transitive though, so a sequence of such steps can be chained together to prove implication (3). This is shown in (6), with neighboring implications informally chained together for illustration:

$$\langle x' = f(x)\,\&\,Q_0\rangle P_0 \xrightarrow{\text{DR}\langle\cdot\rangle \text{ with } [x'=f(x)\,\&\,Q_0]Q_1} \langle x' = f(x)\,\&\,Q_1\rangle P_0 \xrightarrow{\text{K}\langle\&\rangle \text{ with } [x'=f(x)\,\&\,Q_1\wedge\neg P_1]\neg P_0} \langle x' = f(x)\,\&\,Q_1\rangle P_1 \longrightarrow \cdots \longrightarrow \langle x' = f(x)\,\&\,Q\rangle P \qquad (6)$$

With its side conditions, i.e., the box modality formulas, proven, the chain of refinements (6) proves the desired implication (3). However, a proof of the liveness property $\langle x' = f(x)\,\&\,Q\rangle P$ on the right still needs a proof of the hypothesis $\langle x' = f(x)\,\&\,Q_0\rangle P_0$ at the beginning of the chain. Typically, this hypothesis is a (simple) existence assumption for the differential equation. Formalizing and proving such existence properties is the focus of Sect. 4. Those proofs are also based on refinements and make use of axioms BDG$\langle\cdot\rangle$, DDG$\langle\cdot\rangle$.

Refinement with axiom DR$\langle\cdot\rangle$ requires proving the formula $[x' = f(x)\,\&\,R]Q$. Naïvely, one might expect that adding $\neg P$ to the domain constraint should also work, i.e., the solution only needs to be in Q while it has not yet gotten to P:

$$\text{DR}\langle\cdot\rangle\lightning \quad [x' = f(x)\,\&\,R \wedge \neg P]Q \rightarrow \big(\langle x' = f(x)\,\&\,R\rangle P \rightarrow \langle x' = f(x)\,\&\,Q\rangle P\big)$$

This conjectured axiom is unsound (indicated by $\lightning$) as the solution could sneak out of Q exactly when it crosses from $\neg P$ into P. In continuous settings, the language of topology makes precise what this means. The following topological refinement axioms soundly restrict what happens at the crossover point:

Lemma 4 (Topological ODE refinement axioms)**.** *The following topological $\langle\cdot\rangle$ ODE refinement axioms are sound. In axiom* COR*, P, Q either both characterize topologically open or both characterize topologically closed sets over variables x.*

$$\text{COR} \quad \neg P \wedge [x' = f(x)\,\&\,R \wedge \neg P]Q \rightarrow \big(\langle x' = f(x)\,\&\,R\rangle P \rightarrow \langle x' = f(x)\,\&\,Q\rangle P\big)$$

$$\text{SAR} \quad [x' = f(x)\,\&\,R \wedge \neg(P \wedge Q)]Q \rightarrow \big(\langle x' = f(x)\,\&\,R\rangle P \rightarrow \langle x' = f(x)\,\&\,Q\rangle P\big)$$

Proof in Appendix A.2.

Axiom COR is the more informative topological refinement axiom. Like the (unsound) axiom candidate DR$\langle\cdot\rangle\lightning$, it allows formula $\neg P$ to be assumed in the domain constraint when proving the box refinement. For soundness though, axiom COR has crucial topological side conditions on formulas P, Q so it can only be used when these conditions are met. Several variations of COR are possible (with similar soundness proofs), but they require alternative topological restrictions and additional topological notions. One useful variation involving the topological interior is given in Lemma 26. When these topological restrictions are enforced syntactically, axiom COR is derived from dL's real induction axiom [PT20]. For the sake of generality, this article gives semantic topological side conditions with associated semantic soundness proofs in Appendix A.2.

[3] In dL's uniform substitution calculus [Pla17a], this Lie derivative is written directly as the differential term $(\|y\|^2)'$ which can be soundly and syntactically rewritten using dL's differential axioms [Pla17a].

Axiom SAR applies more generally than COR but only assumes the less informative formula $\neg(P \wedge Q)$ in the domain constraint for the box modality. Its proof crucially relies on Q being a formula of real arithmetic so that the set it characterizes has tame topological behavior [BCR98], see the proof in Appendix A.2 for more details. By topological considerations, axiom SAR is also sound if formula P (or resp. Q) characterizes a topologically closed (resp. open) set over the ODE variables x. These additional cases are also proved in Appendix A.2 without relying on the fact that Q is a formula of real arithmetic.

4. Finite-time blow up and global existence

This section explains how global existence properties can be proved for a given ODE $x' = f(x)$, subject to assumptions Γ about the initial states for the ODE. The existence and uniqueness theorems for ODEs [Chi06, Wal98] guarantee that polynomial ODEs like $x' = f(x)$ always have a unique, right-maximal solution from any initial state, $\boldsymbol{\varphi} : [0, T) \to \mathbb{S}$ for some $0 < T \leq \infty$. However, these theorems give no guarantees about the precise duration T. In particular, ODEs can exhibit a technical phenomenon known as *finite-time blow up of solutions* [Chi06], where $\boldsymbol{\varphi}$ is only defined on a bounded time interval $[0, T)$ with $T < \infty$. Additionally, it is possible that such finite-time blow up phenomena only happens for *some* initial conditions (and corresponding solutions) of the ODE. Moreover, these initial conditions (with finite-time blow up) may not be relevant to the model of concern, especially when the dynamics of real world systems are controlled to stay away from the blow up. For example, α_n (2) exhibits finite blow up of solutions only outside the red disk as shown in Fig. 1 and the blow up occurs well after its solutions have reached the target region, see Fig. 2.

As an additional example for this section, consider the following nonlinear ODE:

$$\alpha_b \equiv v' = -v^2 \tag{7}$$

The solution to this ODE is $v(t) = \frac{v_0}{v_0+t}$, where $v_0 \neq 0$ is the initial value of v at time $t = 0$ (if $v_0 = 0$, then $v(t) = 0$ for all t). If $v_0 < 0$ initially, then this solution is only defined to the right for the finite time interval $[0, -v_0)$, because the denominator $v_0 + t$ is 0 at $t = -v_0$. On the other hand, for $v_0 \geq 0$, the existence interval to the right is $[0, \infty)$. Thus, α_b exhibits finite-time blow up of solutions, but only for $v_0 < 0$.

4.1. Global existence proofs

The discussion above uses the mathematical solution $v(t)$ of the ODE α_b (7) as a function of time. For deductive proofs, the (global) existence of solutions can be expressed in dL as a special form of an ODE liveness property. The first step is to add a fresh variable t with $t' = 1$ that tracks the progress of time[4], see Sect. 2.1. Then, using a fresh variable τ not in x, t, the following formula syntactically expresses that the ODE has a global solution because its solutions can reach time τ, for any arbitrary τ:

$$\forall \tau \, \langle x' = f(x), t' = 1 \rangle \, t > \tau \tag{8}$$

Proving formula (8) shows global existence of solutions for the ODE $x' = f(x)$. The simplest instance of (8) is for the ODE $t' = 1$ by itself without any ODE $x' = f(x)$. In this case, the formula (8) is valid because $t' = 1$ is an ODE with constant RHS and its solution exists for all time. The axiom TEx below expresses this fact and it is derived directly from the solution axiom of dL [Pla17a]:

Lemma 5 (Time existence). *The following axiom is derivable in* dL.

TEx $\forall \tau \, \langle t' = 1 \rangle t > \tau$

Proof in Appendix A.2.

Other instances of (8) can be proved using axioms BDG$\langle\cdot\rangle$, DDG$\langle\cdot\rangle$ with appropriate assumptions about the initial conditions for the additional ODEs $x' = f(x)$. This is exemplified for the ODE α_b next.

Example 1 (Velocity of particle with air resistance). The ODE α_b can be viewed as a model of the velocity of a particle that is slowing down due to air resistance. Of course, it does not make physical sense for the velocity of such a particle to "blow up". However, the solution of α_b only exists globally if the particle starts with positive initial velocity $v > 0$, otherwise, it only has short-lived solutions. The reason is that α_b only

[4] For consistency, the ODE $x' = f(x)$ is assumed to not mention t even if this is not always strictly necessary.

makes physical sense for positive velocities $v > 0$, so that the air resistance term $-v^2$ slows the particle down instead of speeding it up. Indeed, global existence (8) can be proved for α_b if its initial velocity is positive, i.e., the dL formula $v > 0 \rightarrow \forall\tau\, \langle v' = -v^2, t' = 1\rangle t > \tau$ is valid.

The derivation below starts with basic propositional steps (→R, ∀R), after which axiom DDG⟨·⟩ is used with $v' = -v^2$ as the differential ghost equation with the trivial choice of bounds $L = 0, M = 0$. This yields two premises, the right of which is proved by TEx. The resulting left premise requires proving the formula $2v \cdot (-v^2) \leq 0$ along the ODE. Mathematically, this says that the derivative of the squared norm v^2 is non-negative along α_b, so that v^2 is non-increasing and cannot blow up.[5] An M['] step strengthens the postcondition to $v > 0$ since $v > 0$ implies $2v \cdot (-v^2) \leq 0$ in real arithmetic. The resulting premise is an invariance property for $v > 0$ which is provable in dL (proof omitted [PT20]). The initial assumption $v > 0$ is crucially used in this step, as expected.

$$\text{→R, ∀R}\;\frac{\text{DDG}\langle\cdot\rangle\;\dfrac{\text{M}[']\;\dfrac{\dfrac{*}{v > 0 \vdash [v' = -v^2, t' = 1]\, v > 0}}{v > 0 \vdash [v' = -v^2, t' = 1]\, 2v \cdot (-v^2) \leq 0} \qquad \text{TEx}\;\dfrac{*}{\vdash \langle t' = 1\rangle t > \tau}}{v > 0 \vdash \langle v' = -v^2, t' = 1\rangle t > \tau}}{\vdash v > 0 \rightarrow \forall\tau\, \langle v' = -v^2, t' = 1\rangle t > \tau}$$

Section 3 offers another view of the derivation above as a single refinement step in the chain (6), recall that refinement steps are read from top-to-bottom. Here, an initial existence property for the ODE $t' = 1$ is refined to the desired existence property for the ODE $v' = -v^2, t' = 1$. The refinement step is justified using DDG⟨·⟩ with the box modality formula $[v' = -v^2, t' = 1]\, 2v \cdot (-v^2) \leq 0$.

$$\langle t' = 1\rangle t > \tau \xrightarrow{\text{DDG}\langle\cdot\rangle} \langle v' = -v^2, t' = 1\rangle t > \tau$$

This chain can be extended to prove global existence for more complicated ODEs $x' = f(x)$ in a stepwise fashion, and (possibly) alternating between uses of DDG⟨·⟩ or BDG⟨·⟩ for the refinement step. To do this, note that any ODE $x' = f(x)$ can be written in *dependency order*, where each group y_i is a vector of variables and each g_i corresponds to the respective vectorial RHS of the ODE for y_i for $i = 1, \ldots, k$. The RHS of each y_i' is only allowed to depend on the preceding vectors of variables (inclusive) $y_1, \ldots, y_i$.

$$\underbrace{y_1' = g_1(y_1), y_2' = g_2(y_1, y_2), y_3' = g_3(y_1, y_2, y_3), \ldots, y_k' = g_k(y_1, y_2, y_3, \ldots, y_k)}_{x'=f(x) \text{ written in dependency order}} \tag{9}$$

Corollary 6 (Dependency order existence)**.** *Let the ODE $x' = f(x)$ be in dependency order (9), and τ be a fresh variable not in x, t. The following rule with k stacked premises is derived from BDG⟨·⟩, DDG⟨·⟩ and TEx, where the postcondition of each premise P_i for $1 \leq i \leq k$ can be chosen to be either of the form:*

$\textcircled{B}$ $P_i \equiv \|y_i\|^2 \leq p_i(t, y_1, \ldots, y_{i-1})$ *for some term p_i with the indicated dependencies, or,*

$\textcircled{D}$ $P_i \equiv 2y_i \cdot g_i(y_1, \ldots, y_i) \leq L_i(t, y_1, \ldots, y_{i-1})\|y_i\|^2 + M_i(t, y_1, \ldots, y_{i-1})$ *for some terms L_i, M_i with the indicated dependencies.*

$$\text{DEx}\;\frac{\begin{array}{l}\Gamma \vdash [y_1' = g_1(y_1), t' = 1]P_1\\ \Gamma \vdash [y_1' = g_1(y_1), y_2' = g_2(y_1, y_2), t' = 1]P_2\\ \quad\vdots\\ \Gamma \vdash [y_1' = g_1(y_1), \ldots, y_k' = g_k(y_1, \ldots, y_k), t' = 1]P_k\end{array}}{\Gamma \vdash \forall\tau\, \langle x' = f(x), t' = 1\rangle t > \tau}$$

Proof Sketch (Proof in Appendix B.1). The derivation proceeds (backwards) by successive refinements using either BDG⟨·⟩ for premises corresponding to the form $\textcircled{B}$ or DDG⟨·⟩ for those corresponding to $\textcircled{D}$, with the ghost equations for g_i and the respective bounds p_i or L_i, M_i at each step for $i = k, \ldots, 1$. □

[5] The fact that v^2 is non-increasing can also be used in an alternative derivation with axiom BDG⟨·⟩ and the bound $p = v_0^2$, where v_0 syntactically stores the initial value of v.

Rule DEx corresponds to a refinement chain (6) of length k, with successive BDG$\langle\cdot\rangle$, DDG$\langle\cdot\rangle$ steps, e.g.:

$$\langle t' = 1\rangle t > \tau \xrightarrow{\text{BDG}\langle\cdot\rangle} \langle y_1'{=}g_1(y_1), t' = 1\rangle t > \tau \xrightarrow{\text{DDG}\langle\cdot\rangle} \cdots \longrightarrow \langle y_1'{=}g_1(y_1), \dots, y_k'{=}g_k(y_1, \dots, y_k), t' = 1\rangle t > \tau$$

In rule DEx any choice of the shape of premises (Ⓑ and Ⓓ) is sound as these correspond to an underlying choice of axiom BDG$\langle\cdot\rangle$, DDG$\langle\cdot\rangle$ to apply at each refinement step, respectively. Another source of flexibility arises when choosing the dependency ordering (9) for the ODE $x' = f(x)$, as long as the requisite dependency requirements are met. For example, one can always choose the coarsest dependency order $y_1 \equiv x, g_1 \equiv f(x)$ to directly prove global existence in one step using appropriate choice of bounds L_1, M_1. The advantage of using finer dependency orders in DEx is it allows the user to choose the bounds L_i, M_i in a step-by-step manner for $i = 1, \dots, k$. On the other hand, the flexibility of rule DEx can also be a drawback because it relies on manual effort from users to choose the partition and to prove the resulting premises. Section 4.2 explains useful recipes for using the flexibility behind rule DEx, e.g., Corollaries 8 and 10, while Sect. 7.2 further explains how proof support can help users in those proofs.

The discussion thus far proves global existence for ODEs with an explicit time variable t. This is not a restriction for the liveness proofs in later sections of this article because such a fresh time variable can always be added using the rule dGt below, which is derived from DG. The rule also adds the assumption $t = 0$ initially without loss of generality for ease of proof.

$$\text{dGt}\ \frac{\Gamma, t = 0 \vdash \langle x' = f(x), t' = 1 \,\&\, Q\rangle P}{\Gamma \vdash \langle x' = f(x) \,\&\, Q\rangle P}$$

4.2. Derived existence axioms

For certain classes of ODEs and initial conditions, there are well-known mathematical techniques to prove global existence of solutions. These techniques have purely syntactic renderings in dL as special cases of BDG$\langle\cdot\rangle$, DDG$\langle\cdot\rangle$, and DEx. In particular, this section shows how axioms GEx, BEx (shown below), which were proved semantically in the earlier conference version [TP19], can be derived syntactically. The refinement approach also yields natural generalizations of these axioms.

4.2.1. Globally Lipschitz ODEs

A function $f : \mathbb{R}^m \to \mathbb{R}^n$ is *globally Lipschitz continuous* if there is a (positive) Lipschitz constant $C \in \mathbb{R}$ such that the inequality $\|f(x) - f(y)\| \leq C\|x - y\|$ holds for all $x, y \in \mathbb{R}^m$, where $\|\cdot\|$ are appropriate norms. Since norms are equivalent on finite dimensional vector spaces [Wal98, §5.V], without loss of generality, the Euclidean norm is used for the following discussion. An ODE $x' = f(x)$ is *globally Lipschitz* if its RHS $f(x)$ is globally Lipschitz continuous and solutions of such ODEs always exist globally for all time [Wal98, §10.VII]. Global Lipschitz continuity is satisfied, e.g., by α_l (1), and more generally by linear (or even affine) ODEs of the form $x' = Ax$, where A is a matrix of (constant) parameters [Wal98] because of the following (mathematical) inequality with Lipschitz constant $\|A\|$, i.e., the (matrix-Euclidean) Frobenius norm of A:

$$\|Ax - Ay\| = \|A(x - y)\| \leq \|A\|\,\|x - y\|$$

This calculation uses the Euclidean norm $\|\cdot\|$, which is not a term in dL (Sect. 2.1) because it is not a polynomial. This syntactic exclusion is not an oversight: it is crucial to the soundness of dL that such non-differentiable terms are excluded from its syntax. For example, $\|x\|$ is not differentiable at $x = 0$. Thus, a subtle technical challenge in proofs is to appropriately rephrase mathematical inequalities, typically involving norms, into ones that can be reasoned about soundly also in the presence of differentiation. In this respect, the Euclidean norm is useful, because expanding the inequality $0 \leq (1 - \|x\|)^2$ and rearranging yields:

$$2\|x\| \leq 1 + \|x\|^2 \tag{10}$$

Notice that, unlike the Euclidean norm $\|x\|$, the RHS of the square inequality (10) can be represented syntactically. Indeed, the squared Euclidean norm is already used in axioms BDG, BDG$\langle\cdot\rangle$, DDG$\langle\cdot\rangle$. To support intuition, the proof sketches below continue to use mathematical inequalities involving Euclidean norms, while the proofs in the appendix use rephrasings with (10) instead. The following corollary shows how global existence for globally Lipschitz ODEs is derived using a norm inequality as a special case of rule DEx.

Corollary 7 (Global existence)**.** *The following global existence axiom is derived from* DDG$\langle\cdot\rangle$ *in* dL*, where* τ *is a fresh variable not in* x, t*, and* $x' = f(x)$ *is globally Lipschitz.*

GEx $\forall \tau \, \langle x' = f(x), t' = 1 \rangle t > \tau$

Proof Sketch (Proof in Appendix B.1). Let C be the Lipschitz constant for f. The proof uses DDG$\langle\cdot\rangle$ and two (mathematical) inequalities. The first inequality (11) bounds $\|f(x)\|$ linearly in $\|x\|$. The constant 0 is chosen here to simplify the resulting arithmetic.

$$\|f(x)\| = \|f(x) - f(0) + f(0)\| \leq \|f(x) - f(0)\| + \|f(0)\| \leq C\|x - 0\| + \|f(0)\| = C\|x\| + \|f(0)\| \tag{11}$$

The second inequality uses bound (11) on $\|f(x)\|$ to further bound $2x \cdot f(x)$ linearly in $\|x\|^2$ along the ODE with appropriate choices of L, M that only depend on the (positive) Lipschitz constant C and $\|f(0)\|$.

$$\begin{aligned} 2x \cdot f(x) &\leq 2\|x\|\|f(x)\| \overset{(11)}{\leq} 2\|x\|\big(C\|x\| + \|f(0)\|\big) = 2C\|x\|^2 + 2\|x\|\|f(0)\| \qquad (12) \\ &\overset{(10)}{\leq} 2C\|x\|^2 + (1 + \|x\|^2)\|f(0)\| = \underbrace{\big(2C + \|f(0)\|\big)}_{L}\|x\|^2 + \underbrace{\|f(0)\|}_{M} \qquad \square \end{aligned}$$

The derivation of axiom GEx uses DDG$\langle\cdot\rangle$, but global existence extends to more complicated ODEs with the aid of DEx as long as appropriate choices of L, M can be made. A useful example of such an extension is global existence for ODEs that have an *affine dependency order* (9), i.e., each $y_i' = g_i(y_1, \ldots, y_i)$ is affine in y_i with $y_i' = A_i(y_1, \ldots, y_{i-1})y_i + b_i(y_1, \ldots, y_{i-1})$ where A_i, b_i are respectively matrix and vector terms with appropriate dimensions and the indicated variable dependencies.

Corollary 8 (Affine dependency order global existence)**.** *Axiom* GEx *is derivable from* DDG$\langle\cdot\rangle$ *in* dL *for ODEs* $x' = f(x)$ *with affine dependency order.*

Proof Sketch (Proof in Appendix B.1). The proof is similar to Corollary 7 but uses DEx to prove global existence step-by-step for the dependency order. It uses the following (mathematical) inequality and corresponding choices of L_i, M_i (shown below) for $i = 1, \ldots, k$ at each step:

$$\begin{aligned} 2y_i \cdot (A_i y_i + b_i) &= 2(y_i \cdot (A_i y_i) + y_i \cdot b_i) \leq 2\|A_i\|\|y_i\|^2 + 2\|y_i\|\|b_i\| \\ &\leq 2\|A_i\|\|y_i\|^2 + (1 + \|y_i\|^2)\|b_i\| = \underbrace{(2\|A_i\| + \|b_i\|)}_{L_i}\|y_i\|^2 + \underbrace{\|b_i\|}_{M_i} \qquad (13) \end{aligned}$$

This inequality is very similar to the one used for Corollary 7, where $\|A_i\|$ corresponds to C, and $\|b_i\|$ corresponds to $\|f(0)\|$. The difference is that terms L_i, M_i are allowed to depend on the preceding variables $y_1, \ldots, y_{i-1}$. Importantly for soundness, both terms meet the appropriate variable dependency requirements of DDG$\langle\cdot\rangle$ because the terms A_i, b_i are not allowed to depend on y_i in the affine dependency order. □

With the extended refinement chain underlying DEx, Corollary 8 enables more general proofs of global existence for certain multi-affine ODEs that are not necessarily globally Lipschitz.

Example 2 (Multi-affine ODE). Consider the multi-affine ODE $u' = u, v' = uv$. The RHS of this ODE is given by the function $\begin{pmatrix} u \\ v \end{pmatrix} \mapsto \begin{pmatrix} u \\ uv \end{pmatrix}$ which is not globally Lipschitz.[6] Nevertheless, the ODE meets the dependency requirements of Corollary 8 and has provable global solutions.

The following derivation illustrates the proof of Corollary 8. In the first step, rule DEx is used with dependency order $y_1 \equiv u, y_2 \equiv v$ and Lipschitz constants $L_1(t) = 2, L_2(u, t) = 2u, M_1(t) = 0, M_2(u, t) = 0$. The dependency requirements of the Lipschitz constants, notably for L_2, are satisfied by these choices and the resulting premises are proved by dW, $\mathbb{R}$ because the postconditions are valid real arithmetic formulas.

[6] For the function to be globally Lipschitz, there must exist a constant $C \in \mathbb{R}$ such that for all $\begin{pmatrix} u_1 \\ v_1 \end{pmatrix}, \begin{pmatrix} u_2 \\ v_2 \end{pmatrix} \in \mathbb{R}^2$, the norm inequality $\| \begin{pmatrix} u_1 - u_2 \\ u_1 v_1 - u_2 v_2 \end{pmatrix} \| \leq C \| \begin{pmatrix} u_1 - u_2 \\ v_1 - v_2 \end{pmatrix} \|$ is satisfied. No such C exists because the $u_1 v_1 - u_2 v_2$ component on the LHS grows quadratically while the corresponding component $v_1 - v_2$ on the RHS grows linearly (consider setting $u_i = v_i$ for $i = 1, 2$).

$$\mathrm{DEx}\ \dfrac{\mathrm{dW}\ \dfrac{\mathbb{R}\ \dfrac{*}{\vdash 2(u)(u) \le (2)u^2}}{\vdash [u' = u, t' = 1]2(u)(u) \le (2)u^2} \qquad \mathrm{dW}\ \dfrac{\mathbb{R}\ \dfrac{*}{\vdash 2(v)(uv) \le (2u)v^2}}{\vdash [u' = u, v' = uv, t' = 1]2(v)(uv) \le (2u)v^2}}{\vdash \forall \tau \, \langle u' = u, v' = uv, t' = 1 \rangle t > \tau}$$

Observe that the premises of DEx remove the ODEs for u, v in a step-by-step fashion. This is the key for generalizing global existence for globally Lipschitz ODEs [Wal98, §10.VII] to more general classes of ODEs.

4.2.2. Bounded existence

Returning to the example ODEs α_n (2) and α_b (7), observe that axiom GEx applies to neither of those ODEs because they do not have affine dependency order. As observed earlier in Fig. 1 and Example 1 respectively, neither α_n nor α_b have global solutions from all initial states. Although Example 1 shows how global existence for α_b can be proved from assumptions motivated by physics, it is also useful to have general axioms (similar to GEx) corresponding to well-known mathematical techniques for proving global existence of solutions for nonlinear ODEs under particular assumptions. One such mathematical technique is briefly recalled next.

Suppose that the solution of ODE $x' = f(x)$ is trapped within a bounded set (whose compact closure is contained in the domain of the ODE), then, the ODE solution exists globally [HC08, Corollary 2.5][Kha92, Theorem 3.3]. In control theory, this principle is used to show the global existence of solutions near stable equilibria [HC08, Kha92]. It also applies in case the model of interest has state variables that are *a priori* known to range within a bounded set [Alu15, Section 6].

This discussion suggests that the following formula is valid for any ODE $x' = f(x)$, where $B(x)$ characterizes a bounded set over the variables x so the assumption $[x' = f(x)]B(x)$ says that the ODE solution is always trapped within the bounded set characterized by $B(x)$.

$$[x' = f(x)]B(x) \rightarrow \forall \tau \, \langle x' = f(x), t' = 1 \rangle t > \tau \tag{14}$$

Formula (14) is (equivalently) rewritten succinctly in the following corollary by negating the box modality.

Corollary 9 (Bounded existence)**.** *The following bounded existence axiom is derived from* BDG⟨·⟩ *in* dL*, where* τ *is a fresh variable not in* x, t*, and formula* $B(x)$ *characterizes a bounded set over variables* x*.*

BEx $\forall \tau \, \langle x' = f(x), t' = 1 \rangle (t > \tau \lor \neg B(x))$

Proof Sketch (Proof in Appendix B.1). The squared norm $\|x\|^2$ function is continuous in x so it is bounded above by a constant D on the compact closure of the set characterized by $B(x)$. The proof uses axiom BDG⟨·⟩ with $p(x) = D$ and rephrases formula (14) with axiom ⟨·⟩. □

Example 3 (Trapped solutions). Axiom BEx proves global existence for α_n (2) within the compact disk $u^2 + v^2 \le \frac{1}{4}$ by showing that solutions starting in the disk are trapped in it. After the first ∀R step, a K⟨&⟩ step adds a disjunction to the postcondition. On the resulting right premise, axiom BEx finishes the proof. The left premise is an invariance property of the ODE (see Fig. 1), whose elided proof is easy [PT20].

$$\forall\mathrm{R}\ \dfrac{\mathrm{K}\langle\&\rangle\ \dfrac{\dfrac{*}{u^2 + v^2 \le \frac{1}{4} \vdash [\alpha_n, t' = 1 \,\&\, \neg(t > \tau)](u^2 + v^2 \le \frac{1}{4})} \qquad \mathrm{BEx}\ \dfrac{*}{\vdash \langle \alpha_n, t' = 1 \rangle (t > \tau \lor \neg(u^2 + v^2 \le \frac{1}{4}))}}{u^2 + v^2 \le \frac{1}{4} \vdash \langle \alpha_n, t' = 1 \rangle t > \tau}}{u^2 + v^2 \le \frac{1}{4} \vdash \forall \tau \, \langle \alpha_n, t' = 1 \rangle t > \tau}$$

Axiom BEx removes the global Lipschitz (or affine dependency) requirement of GEx but weakens the postcondition to say that solutions must either exist for sufficient duration or blow up and leave the bounded set characterized by formula $B(x)$. Like axiom GEx, axiom BEx is derived by refinement using axiom BDG⟨·⟩. This commonality yields a more general version of BEx, which also incorporates ideas from GEx.

Corollary 10 (Dependency order bounded existence)**.** *Consider the ODE* $x' = f(x)$ *in dependency order* (9)*, and where* τ *is a fresh variable not in* x, t*. The following axiom is derived from* BDG⟨·⟩, DDG⟨·⟩ *in* dL*, where the indices* $i = 1 \ldots, k$ *are partitioned into two disjoint index sets* L, N *such that:*

- *For each* $i \in L$*,* $y_i' = g_i(y_1, \ldots, y_i)$ *is affine in* y_i*.*

- *For each $i \in N$, $B_i(y_i)$ characterizes a bounded set over the variables y_i.*

  GBEx $\forall \tau \, \langle x' = f(x), t' = 1 \rangle \big(t > \tau \lor \bigvee_{i \in N} \neg B_i(y_i)\big)$

Proof Sketch (Proof in Appendix B.1). The derivation is similar to rule DEx, with an internal DDG⟨·⟩ step (similar to GEx) for $i \in L$ and an internal BDG⟨·⟩ step (similar to BEx) for $i \in N$. □

The index set L in Corollary 10 indicates those variables of $x' = f(x)$ whose solutions are guaranteed to exist globally (with respect to the other variables). On the other hand, the index set N indicates the variables that may cause finite-time blow up of solutions. The postcondition of axiom GBEx says that solutions either exist for sufficient duration or they blow up and leave one of the bounded sets indexed by N. An immediate modeling application of Corollary 10 is to identify which of the state variables in a model must be proved (or assumed) to take on bounded values [Alu15, Section 6]. This idea underlies the automated existence proof support discussed in Sect. 7.2.

4.3. Completeness for global existence

The derivation of the existence axioms GEx, BEx, GBEx and rule DEx illustrate the use of liveness refinement for proving existence properties. Moreover, BDG⟨·⟩ is the sole ODE diamond refinement axiom underlying these derivations (recall DDG⟨·⟩ is derived from BDG⟨·⟩). This yields a natural question: are there ODEs whose solutions exist globally, but whose global existence *cannot* be proved syntactically using BDG⟨·⟩? The next completeness result gives a conditional completeness answer: *all* global existence properties can be proved using BDG⟨·⟩, if the corresponding ODE solutions are *syntactically representable*.

Proposition 11 (Global existence completeness)**.** *If the ODE $x' = f(x)$ has a global solution representable in the* dL *term language, then the global existence formula* (8) *is derivable for $x' = f(x)$ from axiom* BDG⟨·⟩*.*

Proof Sketch (Proof in Appendix B.1). Suppose that ODE $x' = f(x)$ has a global solution syntactically represented in dL as term $X(t)$ dependent only on the free variable t, the (symbolic) initial values x_0 of variables x, and the (constant) parameters for the ODE. The equality $x = X(t)$ is provable along the ODE $x' = f(x), t' = 1$ because solutions are equational invariants [Pla17a, PT20]. The proof uses BDG⟨·⟩ with the bounding term $p = \|X(t)\|^2$, so that the required hypothesis of BDG⟨·⟩, i.e., $[x' = f(x), t' = 1]\|x\|^2 \leq \|X(t)\|^2$ proves trivially using the equality $x = X(t)$. □

The following remark illustrates the usage and limitations of Proposition 11.

Remark 1 (Syntactically representable solutions). Consider the example ODE $u' = u, v' = uv$ proved to have global solutions in Example 2. Mathematically, its solution is given by the following functions (defined for all $t \in \mathbb{R}$), where u_0, v_0 are the initial values of u, v at time $t = 0$ and exp is the real exponential function.

$$u(t) = u_0 \exp(t), v(t) = \frac{v_0}{\exp(u_0)} \exp(u_0 \exp(t)) \tag{15}$$

Since the solution (15) is defined globally, Proposition 11 seemingly provides an alternative way to prove global existence for the ODE. The caveat is that Proposition 11 only applies when the solution is *syntactically representable* in the term language. The term language of this article (Sect. 2.1) only accepts polynomial solutions. However, dL's term language extensions [PT20] considerably extends the class of syntactically representable solutions to include[7], e.g., towers of exponentials, like those found in (15). Thus, the usefulness of Proposition 11 is limited by which solutions are syntactically representable.

Notably though, the proof in Proposition 11 actually only requires a provable upper bound $X(t)$ with $\|x\|^2 \leq \|X(t)\|^2$, rather than an equality. Such an upper bound, if syntactically representable in dL, also suffices for proving global existence. The complicated closed form solution (15) also highlights the advantage of axioms BDG⟨·⟩, DDG⟨·⟩ and their use in the derived axioms of Corollaries 7–10 because they implicitly deduce global existence *without* needing an explicitly representable solution for the ODEs.

[7] Nevertheless, even such a syntactic extension is insufficient because Turing machines can be simulated by solutions of polynomial differential equations [GCB08, Theorem 2]. It is possible to construct polynomial ODEs whose solutions do not blow up, but grow like the (Turing-computable) Ackermann function, i.e., faster than any tower of exponentials.

5. Liveness without domain constraints

This section presents proof rules for liveness properties of ODEs $x' = f(x)$ without domain constraints, i.e., where Q is the formula *true*. Errors and omissions in the surveyed techniques are highlighted in blue.

5.1. Differential variants

The fundamental technique for verifying liveness of discrete loops are loop variants, i.e., well-founded quantities that increase (or decrease) across each loop iteration. *Differential variants* [Pla10] are their continuous analog, where the value of a given term p is shown to increase along ODE solutions by showing that its rate of change is bounded below by a positive constant $\varepsilon() > 0$ along those solutions. Recall this article's syntactic convention (Sect. 2.1) that term $\varepsilon()$ is not allowed to depend on any of the free variables $x_1, \dots, x_n$ appearing in the ODE and must therefore remain constant along the ODE solution.

Corollary 12 (Atomic differential variants [Pla10]). *The following proof rules (where $\succcurlyeq$ is either $\geq$ or $>$) are derivable in* dL. *Terms $\varepsilon(), p_0()$ are constant for ODE $x' = f(x), t' = 1$. In rule $\text{dV}_{\succcurlyeq}$, the ODE $x' = f(x)$ has provable global solutions.*

$$\text{dV}^{\Gamma}_{\succcurlyeq}\ \frac{\neg(p \succcurlyeq 0) \vdash \dot{p} \geq \varepsilon()}{\Gamma, p = p_0(), t = 0, \langle x' = f(x), t' = 1\rangle\big(p_0() + \varepsilon()t > 0\big) \vdash \langle x' = f(x), t' = 1\rangle p \succcurlyeq 0}$$

$$\text{dV}_{\succcurlyeq}\ \frac{\neg(p \succcurlyeq 0) \vdash \dot{p} \geq \varepsilon()}{\Gamma, \varepsilon() > 0 \vdash \langle x' = f(x)\rangle p \succcurlyeq 0}$$

Proof Sketch (Proof in Appendix B.2). Rule $\text{dV}^{\Gamma}_{\succcurlyeq}$ is derived from axiom $\text{K}\langle\&\rangle$ with $G \equiv \big(p_0() + \varepsilon()t > 0\big)$:

$$\text{K}\langle\&\rangle\ \frac{\Gamma, p = p_0(), t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg(p \succcurlyeq 0)]\big(p_0() + \varepsilon()t \leq 0\big)}{\Gamma, p = p_0(), t = 0, \langle x' = f(x), t' = 1\rangle\big(p_0() + \varepsilon()t > 0\big) \vdash \langle x' = f(x), t' = 1\rangle p \succcurlyeq 0}$$

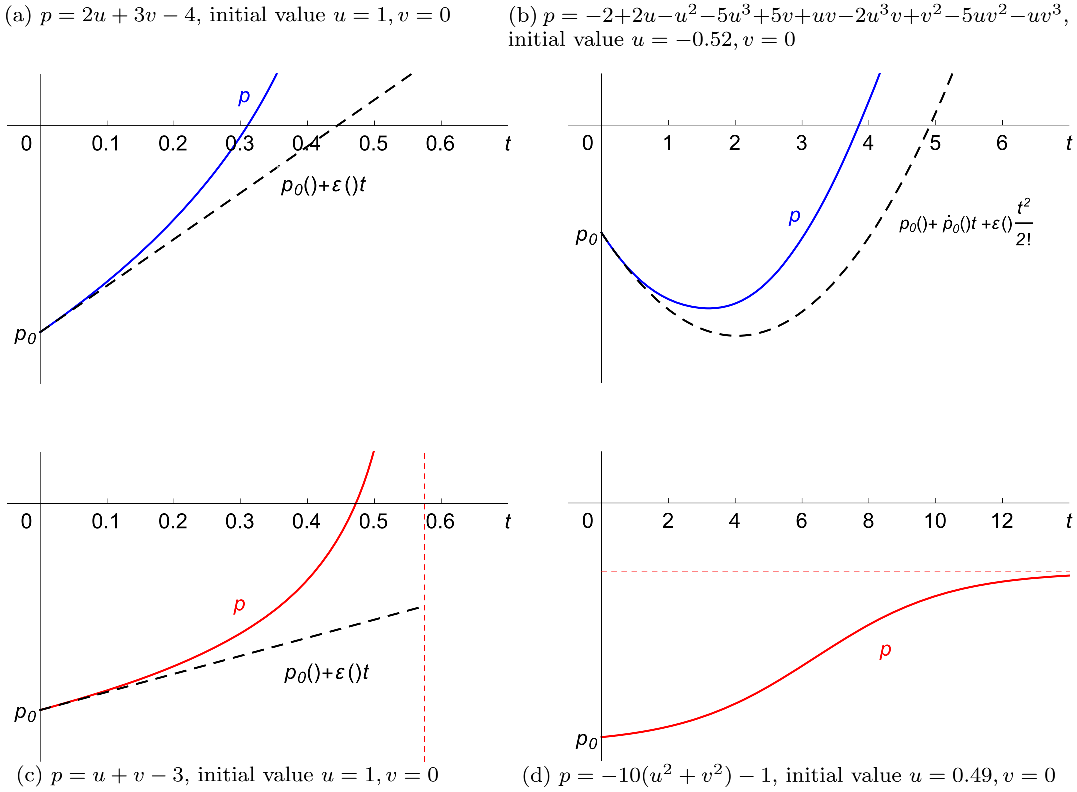
Monotonicity M['] strengthens the postcondition to $p \geq p_0() + \varepsilon()t$ with the domain constraint $\neg(p \succcurlyeq 0)$. A subsequent use of $\text{dI}_{\succcurlyeq}$ completes the derivation:

$$\text{M}[']\ \frac{\text{dI}_{\succcurlyeq}\ \dfrac{\neg(p \succcurlyeq 0) \vdash \dot{p} \geq \varepsilon()}{\Gamma, p = p_0(), t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg(p \succcurlyeq 0)]\big(p \geq p_0() + \varepsilon()t\big)}}{\Gamma, p = p_0(), t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg(p \succcurlyeq 0)]\big(p_0() + \varepsilon()t \leq 0\big)}$$

Rule $\text{dV}_{\succcurlyeq}$ is derived in Appendix B.2 as a corollary of rule $\text{dV}^{\Gamma}_{\succcurlyeq}$ because the ODE $x' = f(x)$ is assumed to have solutions which (provably) exist globally. □

In both rules $\text{dV}^{\Gamma}_{\succcurlyeq}$, $\text{dV}_{\succcurlyeq}$, the lower bound $\varepsilon() > 0$ on the Lie derivative $\dot{p}$ ensures that the value of p strictly increases along solutions to the ODE. Geometrically, as illustrated in Fig. 3a, the value of p is bounded below over time t by the line $p_0() + \varepsilon()t$ with offset $p_0()$ and positive slope $\varepsilon()$. Since $p_0() + \varepsilon()t$ is non-negative for sufficiently large values of t, the (lower bounded) value of p is also eventually non-negative.

Two key subtleties underlying rules $\text{dV}^{\Gamma}_{\succcurlyeq}$, $\text{dV}_{\succcurlyeq}$ are illustrated in Figs. 3c and 3d. The first subtlety, shown in Fig. 3c, is that ODE solutions must exist for sufficiently long for p or, more precisely its lower bound, to become non-negative. This is usually left as a soundness-critical side condition in liveness proof rules [Pla10, SJ15], but any such side condition is antithetical to approaches for minimizing the soundness-critical core in implementations [Pla17a] because it requires checking the (semantic) condition that solutions exist for sufficient duration. The conclusion of rule $\text{dV}^{\Gamma}_{\succcurlyeq}$ formalizes this side condition as an assumption. In contrast, rule $\text{dV}_{\succcurlyeq}$ requires provable global existence for the ODEs (provable as in Sect. 4). The rest of this article similarly develops ODE liveness proof rules that rely on the global existence proofs from Sect. 4. In all subsequent proof rules, the ODE $x' = f(x)$ is said to have *provable global solutions* if the global existence formula (8) for $x' = f(x)$ is provable. For example, if $x' = f(x)$ were globally Lipschitz (or, as a special case, linear), then its global existence can be proven using axiom GEx from Corollaries 7 and 8. For uniformity, all proof steps utilizing this assumption are marked with GEx, although proofs of global existence could use various other techniques described in Sect. 4. All subsequent proof rules can be soundly presented with sufficient duration assumptions like $\text{dV}^{\Gamma}_{\succcurlyeq}$, but those are omitted for brevity.


(a) $p = 2u + 3v - 4$, initial value $u = 1, v = 0$

(b) $p = -2+2u-u^2-5u^3+5v+uv-2u^3v+v^2-5uv^2-uv^3$, initial value $u = -0.52, v = 0$

(c) $p = u + v - 3$, initial value $u = 1, v = 0$

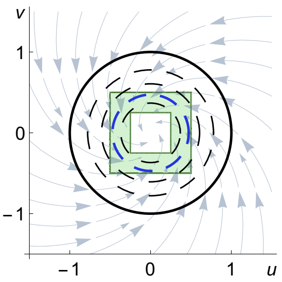
(d) $p = -10(u^2 + v^2) - 1$, initial value $u = 0.49, v = 0$

Fig. 3. The solid blue and red curves show the value of various terms p evaluated along solutions of the ODE α_n (2) from respective initial values p_0 over time t. The blue curves in Figs. 3a and 3b are respectively bounded below by a dashed black line (corresponding to Corollary 12) and a dashed quadratic curve (corresponding to Corollary 14) which imply that p is eventually non-negative along their respective ODE solutions. The red curve in Fig. 3c is also bounded below by the dashed black line, but its solution only exists for 0.575 time units (vertical red dashed asymptote) so the direct bound from Corollary 12 fails, even though p is eventually non-negative along the solution. The red curve in Fig. 3d has strictly positive time derivative but asymptotically increases towards a negative value (horizontal red dashed asymptote)

The second subtlety, shown in Fig. 3d, is that rules $\mathrm{dV}^{\Gamma}_{\succcurlyeq}$, $\mathrm{dV}_{\succcurlyeq}$ crucially need a *constant* positive lower bound on the Lie derivative $\dot{p} \geq \varepsilon()$ for soundness [Pla10] instead of merely requiring $\dot{p} > 0$. In the latter case, even though the value of p is strictly increasing along solutions, it is not guaranteed to become non-negative in finite time because the rate of increase can itself converge to zero. In fact, as Fig. 3d shows, p may stay negative by asymptotically increasing towards a negative value as t approaches ∞.

Example 4 (Linear liveness). The liveness property that Fig. 1 suggested for the linear ODE α_l (1) is proved by rule $\mathrm{dV}_{\succcurlyeq}$. The proof is shown on the left below and visualized on the right. The first monotonicity step $\mathrm{M}\langle'\rangle$ strengthens the postcondition to the inner blue circle $u^2 + v^2 = \frac{1}{4}$ contained within the green goal region, see refinement (4). Next, since solutions satisfy $u^2 + v^2 = 1$ initially (black circle), the $\mathrm{K}\langle\&\rangle$ step expresses an intermediate value property: to show that the *continuous* solution eventually reaches $u^2 + v^2 = \frac{1}{4}$, it suffices to show that it eventually reaches $u^2 + v^2 \leq \frac{1}{4}$ (also see Corollary 13 below). The postcondition is rearranged before $\mathrm{dV}_{\succcurlyeq}$ is used with $\varepsilon() = \frac{1}{2}$. Its premise is proved by $\mathbb{R}$ because the Lie derivative of $\frac{1}{4} - (u^2 + v^2)$ with respect to α_l is $2(u^2 + v^2)$, which is bounded below by $\frac{1}{2}$ under the assumption $\frac{1}{4} - (u^2 + v^2) < 0$.

$$\mathrm{M}\langle'\rangle\,\dfrac{\mathrm{K}\langle\&\rangle\,\dfrac{\dfrac{\mathrm{dV}_{\succcurlyeq}\,\dfrac{\dfrac{\mathbb{R}\,\dfrac{*}{\frac{1}{4} < u^2+v^2 \vdash 2(u^2+v^2) \geq \frac{1}{2}}}{\frac{1}{4} - (u^2+v^2) < 0 \vdash 2(u^2+v^2) \geq \frac{1}{2}}}{u^2+v^2 = 1 \vdash \langle\alpha_l\rangle \frac{1}{4} - (u^2+v^2) \geq 0}}{u^2+v^2 = 1 \vdash \langle\alpha_l\rangle u^2+v^2 \leq \frac{1}{4}}}{u^2+v^2 = 1 \vdash \langle\alpha_l\rangle u^2+v^2 = \frac{1}{4}}}{u^2+v^2 = 1 \vdash \langle\alpha_l\rangle \left(\frac{1}{4} \leq \|(u,v)\|_\infty \leq \frac{1}{2}\right)}$$



The Lie derivative calculation shows that the value of u^2+v^2 decreases along solutions of α_l with rate (at least) $\frac{1}{2}$ per unit time. This is visualized by the shrinking (dashed) circles with radii eventually smaller than $\frac{1}{4}$. Since the initial states satisfy $u^2+v^2 = 1$, a concrete upper bound on the time required for the solution to satisfy $u^2+v^2 \leq \frac{1}{4}$ is given by $(1-\frac{1}{4}) \,/\, \frac{1}{2} = \frac{3}{2}$ time units. It is also instructive to examine the chain of refinements (6) underlying the proof above. Since α_l is a linear ODE, the first $\mathrm{dV}_{\succcurlyeq}$ step refines the initial liveness property from GEx, i.e., that solutions exist globally (so for at least $\frac{3}{2}$ time units), to the property $u^2+v^2 \leq \frac{1}{4}$. Subsequent refinement steps can be read off from the steps above from top-to-bottom:

$$\langle\alpha_l, t'=1\rangle t > \frac{3}{2} \xrightarrow{\mathrm{dV}_{\succcurlyeq}} \langle\alpha_l\rangle u^2+v^2 \leq \frac{1}{4} \xrightarrow{\mathrm{K}\langle\&\rangle} \langle\alpha_l\rangle u^2+v^2 = \frac{1}{4} \xrightarrow{\mathrm{M}\langle'\rangle} \langle\alpha_l\rangle \left(\frac{1}{4} \leq \|(u,v)\|_\infty \leq \frac{1}{2}\right)$$

The latter two steps illustrate the idea behind the next two surveyed proof rules. In their original presentation [TT10], the ODE $x' = f(x)$ is only assumed to be locally Lipschitz continuous, which is insufficient for global existence of solutions, making the original rules unsound. See Appendix C for counterexamples. Compared to Corollary 12, Corollary 13 below uses the fact that the value of differential variant p evolves continuously along an ODE solution so it changes from $p \leq 0$ to $p > 0$ via $p = 0$.

Corollary 13 (Equational differential variants [TT10])**.** *The following proof rules are derivable in* dL. *Term* $\varepsilon()$ *is constant for ODE* $x' = f(x)$, *and the ODE has provable global solutions for both rules.*

$$\mathrm{dV}_{=}\ \dfrac{p < 0 \vdash \dot{p} \geq \varepsilon()}{\Gamma, \varepsilon() > 0, p \leq 0 \vdash \langle x' = f(x)\rangle p = 0} \qquad \mathrm{dV}^{M}_{=}\ \dfrac{p = 0 \vdash P \quad p < 0 \vdash \dot{p} \geq \varepsilon()}{\Gamma, \varepsilon() > 0, p \leq 0 \vdash \langle x' = f(x)\rangle P}$$

Proof in Appendix B.2.

The view of $\mathrm{dV}_{\succcurlyeq}$ as a refinement of GEx in Example 4 also yields generalizations of $\mathrm{dV}_{\succcurlyeq}$ to higher Lie derivatives. Indeed, it suffices that *any* higher Lie derivative $\dot{p}^{(k)}$ is bounded below by a positive constant $\varepsilon()$ rather than just the first. Geometrically, this guarantees that p is bounded below by a degree k polynomial in time variable t that is non-negative for large enough t, see Fig. 3b for an illustration with $k = 2$.

Corollary 14 (Atomic higher differential variants)**.** *The following proof rule (where* $\succcurlyeq$ *is either* $\geq$ *or* $>$*) is derivable in* dL. *Term* $\varepsilon()$ *is constant for ODE* $x' = f(x)$, $k \geq 1$ *is a freely chosen natural number, and the ODE has provable global solutions.*

$$\mathrm{dV}^{k}_{\succcurlyeq}\ \dfrac{\neg(p \succcurlyeq 0) \vdash \dot{p}^{(k)} \geq \varepsilon()}{\Gamma, \varepsilon() > 0 \vdash \langle x' = f(x)\rangle p \succcurlyeq 0}$$

Proof Sketch (Proof in Appendix B.2). Since $\dot{p}^{(k)}$ is strictly positive, all lower Lie derivatives $\dot{p}^{(i)}$ of p for $i < k$, including $p = \dot{p}^{(0)}$, eventually become positive. The derivation uses a sequence of dC, $\mathrm{dI}_{\succcurlyeq}$ steps. □

5.2. Staging sets

The *staging sets* [SJ15] proof rule adds flexibility to rules such as $\mathrm{dV}^{M}_{=}$ above by allowing users to choose a staging set formula S that *the ODE can only leave by entering the goal region* P. Staging sets are leaky invariants in the sense that they are almost invariant, except that they can be left by reaching the goal. This staging property is expressed in the contrapositive by the box modality formula $[x' = f(x)\,\&\,\neg P]S$.

Corollary 15 (Staging sets [SJ15]). *The following proof rule is derivable in* dL*. Term* $\varepsilon()$ *is constant for ODE* $x' = f(x)$*, and the ODE has provable global solutions.*

$$\text{SP}\ \frac{\Gamma \vdash [x' = f(x) \,\&\, \neg P]S \qquad S \vdash p \leq 0 \wedge \dot{p} \geq \varepsilon()}{\Gamma, \varepsilon() > 0 \vdash \langle x' = f(x)\rangle P}$$

Proof Sketch (Proof in Appendix B.2). The derivation starts by using refinement axiom $\mathrm{K}\langle\&\rangle$ with $G \equiv \neg S$. The rest of the derivation is similar to $\mathrm{dV}_{\succcurlyeq}^{\Gamma}$, $\mathrm{dV}_{\succcurlyeq}$. □

The added choice of staging set formula S allows users to choose a staging set that, e.g., enables a liveness proof that uses a simpler differential variant p. Furthermore, proof rules can be significantly simplified by choosing S with desirable topological properties. For example, all of the liveness proof rules derived so far either have an explicit sufficient duration assumption (like $\mathrm{dV}_{\succcurlyeq}^{\Gamma}$) or assume that the ODEs have provable global solutions (like $\mathrm{dV}_{\succcurlyeq}$ using axiom GEx). An alternative is to use axiom BEx, by choosing the staging set formula $S(x)$ to characterize a bounded or compact set over the variables x.

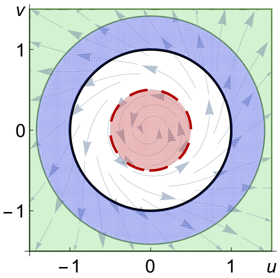
Corollary 16 (Bounded/compact staging sets). *The following proof rules are derivable in* dL*. Term* $\varepsilon()$ *is constant for* $x' = f(x)$*. In rule* SP_b*, formula* S *characterizes a bounded set over variables* x*. In rule* SP_c*, it characterizes a compact, i.e., closed and bounded, set over those variables.*

$$\mathrm{SP}_b\ \frac{\Gamma \vdash [x' = f(x) \,\&\, \neg P]S \qquad S \vdash \dot{p} \geq \varepsilon()}{\Gamma, \varepsilon() > 0 \vdash \langle x' = f(x)\rangle P} \qquad \mathrm{SP}_c\ \frac{\Gamma \vdash [x' = f(x) \,\&\, \neg P]S \qquad S \vdash \dot{p} > 0}{\Gamma \vdash \langle x' = f(x)\rangle P}$$

Proof Sketch (Proof in Appendix B.2). Rule SP_b is derived using axiom BEx with differential variant p to establish a time bound. Rule SP_c is an arithmetical corollary of SP_b, using the fact that continuous functions on compact domains attain their extrema. □

Example 5 (Nonlinear liveness). The liveness property that Fig. 1 suggested for the nonlinear ODE α_n (2) is proved using rule SP_c by choosing the staging set formula $S \equiv 1 \leq u^2 + v^2 \leq 2$ and the differential variant $p = u^2 + v^2$. The proof is shown on the left and visualized on the right below; the goal $u^2 + v^2 \geq 2$ is shown in green while S is shown as a blue annulus. The Lie derivative $\dot{p}$ with respect to α_n is $2(u^2+v^2)(u^2+v^2-\frac{1}{4})$, which is bounded below by $\frac{3}{2}$ in S. Thus, the right premise of SP_c closes trivially. The left premise requires proving that S is an invariant within the domain constraint $\neg(u^2 + v^2 \geq 2)$. Intuitively, this is true because the blue annulus can only be left by entering the goal. Its elided invariance proof is easy [PT20].

$$\mathrm{SP}_c\ \dfrac{\text{cut}, \mathbb{R}\ \dfrac{\dfrac{*}{S \vdash [\alpha_n \,\&\, \neg(u^2+v^2 \geq 2)]S}}{u^2 + v^2 = 1 \vdash [\alpha_n \,\&\, \neg(u^2+v^2 \geq 2)]S} \qquad \mathbb{R}\ \dfrac{*}{S \vdash \dot{p} > 0}}{u^2 + v^2 = 1 \vdash \langle \alpha_n \rangle u^2 + v^2 \geq 2}$$



This proof exploits the flexibility provided by staging sets in two ways. First, the formula S is chosen to characterize a compact set (as required by rule SP_c). As explained in Sect. 4, solutions of α_n can blow up in finite time which necessitates the use of BEx for proving its liveness properties. Second, S cleverly *excludes* the red disk (dashed boundary) characterized by $u^2 + v^2 \leq \frac{1}{4}$. Solutions of α_n behave differently in this region, e.g., the Lie derivative $\dot{p}$ is *non-positive* in this disk. The chain of refinements (6) behind this proof can be seen from the derivation of rules SP_b, SP_c in Appendix B.2. The chain starts from the initial liveness property BEx with concrete[8] time bound $\frac{2}{3}$. The first $\mathrm{K}\langle\&\rangle$ step shows that the staging set is ultimately exited ($\langle\alpha_n\rangle\neg S$), while the latter shows the desired liveness property:

$$\langle \alpha_n, t' = 1\rangle \left(t > \frac{2}{3} \vee \neg S\right) \xrightarrow{\mathrm{K}\langle\&\rangle} \langle\alpha_n\rangle\neg S \xrightarrow{\mathrm{K}\langle\&\rangle} \langle\alpha_n\rangle u^2 + v^2 \geq 2$$

[8] The value of $u^2 + v^2$ grows at rate $\frac{3}{2}$ per time unit along solutions and the initial states satisfy $u^2 + v^2 = 1$. Thus, a lower bound on time required to leave the staging set (when $u^2 + v^2 > 2$) is $(2 - 1) \,/\, \frac{3}{2} = \frac{2}{3}$ time units.

The need to use axiom BEx (or otherwise, assume global existence) is subtle and is often overlooked in the surveyed liveness arguments. An example of this is an incorrect claim [PR07, Remark 3.6] that a liveness argument [PR07, Theorem 3.5] works without assuming that the relevant sets are bounded. This article's axiomatic approach can be used to find and fix errors involving these subtleties. As another example, the following *set Lyapunov function* proof rule adapts ideas from the literature [RS10, Theorem 2.4, Corollary 2.5] for proving liveness when the postcondition P characterizes an open set. The latter assumption on P enables a convenient choice of staging set in rule SP_c because $\neg P$ characterizes a closed set.

Corollary 17 (Set Lyapunov functions [RS10])**.** *The following proof rule is derivable in* dL*. Formula K characterizes a compact set over variables x, while formula P characterizes an open set over those variables.*

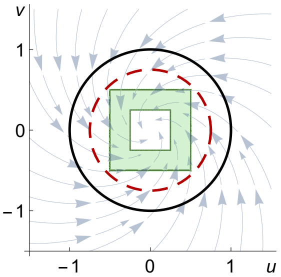
$$\text{SLyap}\quad \frac{p \geq 0 \vdash K \qquad \neg P, K \vdash \dot{p} > 0}{\Gamma, p \succcurlyeq 0 \vdash \langle x' = f(x) \rangle P}$$

Proof Sketch (Proof in Appendix B.2). Rule SLyap is derived from rule SP_c with $S \equiv \neg P \wedge K$, since $\neg P$ characterizes a closed set, and the intersection of a closed set with a compact set is compact. □

Rule SLyap was claimed [RS10, Theorem 2.4, Corollary 2.5] to hold for any closed set K, when, in fact, K crucially needs to be compact as seems to have been assumed implicitly in the proofs [RS10].

6. Liveness with domain constraints

This section presents proof rules for liveness properties $x' = f(x) \,\&\, Q$ with domain constraint Q. These properties are more subtle than liveness without domain constraints, because the limitation to a domain constraint Q may make it impossible for an ODE solution to reach a desired goal region without leaving Q.



Consider the following liveness property for α_l (1) (visualized on the right), which adds domain constraint $Q \equiv u^2 + v^2 \neq \frac{9}{16}$ restricting solutions from entering the red dashed circle before reaching the green goal region.

$$\langle \alpha_l \,\&\, u^2 + v^2 \neq \frac{9}{16} \rangle \Big(\frac{1}{4} \leq \|(u, v)\|_\infty \leq \frac{1}{2} \Big) \tag{16}$$

As proved in Example 4, solutions starting from the black circle $u^2 + v^2 = 1$ reach the green goal region. However, the continuous solutions must cross the red dashed circle $u^2 + v^2 = \frac{9}{16}$ to reach the goal, see discussion of implication (5). This violates the domain constraint and falsifies (16) for initial states on the black circle.

Axiom $\mathrm{DR}\langle\cdot\rangle$ with $R \equiv \mathit{true}$ provides one way of soundly and directly generalizing the proof rules from Sect. 5, as shown in the following example.

Example 6 (Nonlinear liveness with domain). The liveness property $u^2 + v^2 = 1 \rightarrow \langle \alpha_n \rangle u^2 + v^2 \geq 2$ was proved in Example 5 for the nonlinear ODE α_n (2). The following derivation proves a stronger liveness property with the added domain constraint $1 \leq u^2 + v^2$ by extending the proof from Example 5 with a $\mathrm{DR}\langle\cdot\rangle$ refinement step. The resulting left premise is an invariance property of the ODE whose proof is elided [PT20]; intuitively, solutions starting from $u^2 + v^2 = 1$ grow outwards, and so they remain in the domain $1 \leq u^2 + v^2$ (see Fig. 1). The resulting right premise is proved in Example 5.

$$\mathrm{DR}\langle\cdot\rangle\ \dfrac{\dfrac{*}{u^2 + v^2 = 1 \vdash [\alpha_n] 1 \leq u^2 + v^2} \qquad \dfrac{*}{u^2 + v^2 = 1 \vdash \langle \alpha_n \rangle u^2 + v^2 \geq 2}}{u^2 + v^2 = 1 \vdash \langle \alpha_n \,\&\, 1 \leq u^2 + v^2 \rangle u^2 + v^2 \geq 2}$$

However, liveness arguments become much more intricate when attempting to generalize beyond domain constraint refinement with $\mathrm{DR}\langle\cdot\rangle$, e.g., recall the unsound conjecture $\mathrm{DR}\langle\cdot\rangle\lightning$. Indeed, unlike the technical glitches of Sect. 5, this article uncovers several subtle soundness-critical errors in the literature. With dL's deductive approach, these intricacies are isolated to the topological axioms (Lemma 4) which have been proved sound once-and-for-all. Errors and omissions in the surveyed techniques are again highlighted in blue.

The following proof rule generalizes differential variants $\mathrm{dV}_{\succcurlyeq}$ to handle domain constraints. Like rule $\mathrm{dV}_{\succcurlyeq}$, the differential variant p is guaranteed to eventually become non-negative along solutions with constant positive lower bound $\dot{p} \geq \varepsilon()$ on its Lie derivative. The additional twist is that the domain constraint Q must be proved to hold as long as p is still negative, i.e., while the goal has not been reached. This is expressed in the contrapositive by the formula $[x' = f(x) \,\&\, \neg(p \succcurlyeq 0)]Q$ in the left premise of the rule.

Corollary 18 (Atomic differential variants with domains [Pla10])**.** *The following proof rule (where $\succcurlyeq$ is either $\geq$ or $>$) is derivable in* dL*. Term $\varepsilon()$ is constant for the ODE $x' = f(x)$, and the ODE has provable global solutions. Formula Q characterizes a closed (resp. open) set when $\succcurlyeq$ is $\geq$ (resp. $>$).*

$$\text{dV}_{\succcurlyeq}\& \quad \frac{\Gamma \vdash [x' = f(x) \,\&\, \neg(p \succcurlyeq 0)]Q \qquad \neg(p \succcurlyeq 0), Q \vdash \dot{p} \geq \varepsilon()}{\Gamma, \varepsilon() > 0, \neg(p \succcurlyeq 0) \vdash \langle x' = f(x) \,\&\, Q\rangle p \succcurlyeq 0}$$

Proof Sketch (Proof in Appendix B.3). The derivation uses axiom COR choosing $R \equiv \mathit{true}$, noting that $p \geq 0$ (resp. $p > 0$) characterizes a topologically closed (resp. open) set so the appropriate topological requirements of COR are satisfied. The highlighted $\neg(p \succcurlyeq 0)$ assumption is crucial for soundly using axiom COR:

$$\text{COR}\ \frac{\Gamma \vdash [x' = f(x) \,\&\, \neg(p \succcurlyeq 0)]Q \qquad \dfrac{\dfrac{\neg(p \succcurlyeq 0), Q \vdash \dot{p} \geq \varepsilon()}{\cdots}}{\Gamma, \varepsilon() > 0 \vdash \langle x' = f(x)\rangle p \succcurlyeq 0}}{\Gamma, \varepsilon() > 0, \neg(p \succcurlyeq 0) \vdash \langle x' = f(x) \,\&\, Q\rangle p \succcurlyeq 0}$$

The derivation steps on the right premise are similar to the ones used in $\text{dV}_{\succcurlyeq}$ although an intervening dC step is used to additionally assume Q in the antecedents. □

Rule $\text{dV}_{\succcurlyeq}\&$ uses the topological refinement axiom COR to extend the refinement chain for $\text{dV}_{\succcurlyeq}$ as follows:

$$\cdots \xrightarrow{\text{dV}_{\succcurlyeq}} \langle x' = f(x)\rangle p \succcurlyeq 0 \xrightarrow{\text{COR}} \langle x' = f(x) \,\&\, Q\rangle p \succcurlyeq 0 \tag{17}$$

A subtle advantage of placing the refinement COR at the end of the refinement chain (17) is it decouples reasoning about domain constraint Q from earlier steps refinement steps. Notably, earlier refinement steps like $\text{dV}_{\succcurlyeq}$ in the chain above can focus on handling other subtleties, such as sufficient duration existence of solutions (Sect. 4), *without* worrying about domain constraints. The original presentation of rule $\text{dV}_{\succcurlyeq}\&$ [Pla10] omits the highlighted $\neg(p \succcurlyeq 0)$ assumption, but the rule is unsound without it. In addition, the original presentation uses a form of syntactic weak negation [Pla10], which is unsound for open postconditions, as pointed out earlier [SJ15]. See Appendix C for counterexamples.

The proofs of the next two corollaries also make use of axiom COR to derive the proof rule $\text{dV}^{M}_{=}\&$ [TT10] and the adapted rule SLyap& [RS10]. These rules respectively generalize $\text{dV}^{M}_{=}$ and SLyap from Sect. 5 to handle domain constraints. The technical glitches in their original presentations [RS10, TT10], which were identified in Sect. 5, remain highlighted here.

Like rule $\text{dV}_{\succcurlyeq}\&$, rules $\text{dV}_{=}\&$, $\text{dV}^{M}_{=}\&$ below have an additional premise requiring that the domain constraint Q provably holds while the goal has not yet been reached $[x' = f(x) \,\&\, p < 0]Q$.

Corollary 19 (Equational differential variants with domains [TT10])**.** *The following proof rules are derivable in* dL*. Term $\varepsilon()$ is constant for the ODE $x' = f(x)$, and the ODE has provable global solutions for both rules. Formula Q characterizes a closed set over variables x.*

$$\text{dV}_{=}\& \quad \frac{\Gamma \vdash [x' = f(x) \,\&\, p < 0]Q \qquad p < 0, Q \vdash \dot{p} \geq \varepsilon()}{\Gamma, \varepsilon() > 0, p \leq 0, Q \vdash \langle x' = f(x) \,\&\, Q\rangle p = 0}$$

$$\text{dV}^{M}_{=}\& \quad \frac{Q, p = 0 \vdash P \qquad \Gamma \vdash [x' = f(x) \,\&\, p < 0]Q \qquad p < 0, Q \vdash \dot{p} \geq \varepsilon()}{\Gamma, \varepsilon() > 0, p \leq 0, Q \vdash \langle x' = f(x) \,\&\, Q\rangle P}$$

Proof Sketch (Proof in Appendix B.3). Rules $\text{dV}_{=}\&$, $\text{dV}^{M}_{=}\&$ are both derived from rule $\text{dV}_{\succcurlyeq}\&$ with $\geq$ for $\succcurlyeq$, since Q characterizes a closed set. Their derivations are respectively similar to the derivation of $\text{dV}_{=}$, $\text{dV}^{M}_{=}$ from $\text{dV}_{\succcurlyeq}$ and require the provable global solutions assumption for soundly applying rule $\text{dV}_{\succcurlyeq}\&$. □

Rule SLyap& below has identical premises to the corresponding SLyap rule (without domain constraints). The additional insight is that, assuming $p > 0$ is true initially, those same premises can be used to conclude the stronger liveness property $\langle x' = f(x) \,\&\, p > 0\rangle P$ because p can be additionally proved to stay positive along the solutions using the premises. This stronger conclusion can be used with a monotonicity step to prove more general liveness properties with an arbitrary domain constraint Q as exemplified by rule $\text{SLyap}^{M}\&$.

Corollary 20 (Set Lyapunov functions with domains [RS10])**.** *The following proof rules are derivable in* dL*. Formula K characterizes a compact set over variables x, while formula P characterizes an open set over those variables.*

$$\text{SLyap\&}\ \frac{p \geq 0 \vdash K \quad \neg P, K \vdash \dot{p} > 0}{\Gamma, p > 0 \vdash \langle x' = f(x) \,\&\, p > 0\rangle P}$$

$$\text{SLyap}^{M}\text{\&}\ \frac{p \geq 0 \vdash K \quad \neg P, K \vdash \dot{p} > 0 \quad p > 0 \vdash Q}{\Gamma, p > 0 \vdash \langle x' = f(x) \,\&\, Q\rangle P}$$

Proof Sketch (Proof in Appendix B.3). Rule SLyap^{M}& is derived from rule SLyap& by monotonicity on the domain constraints with the additional premise $p > 0 \vdash Q$. Rule SLyap& is derived from SLyap after a refinement step with COR since both formulas $p > 0$ and P characterize open sets as sketched below.

$$\text{COR}\ \frac{\dfrac{\dfrac{p \geq 0 \vdash K \qquad \neg P, K \vdash \dot{p} > 0}{\dots}}{\Gamma, p > 0 \vdash [x' = f(x) \,\&\, \neg P]p > 0} \qquad \text{SLyap}\ \dfrac{p \geq 0 \vdash K \qquad \neg P, K \vdash \dot{p} > 0}{\Gamma, p > 0 \vdash \langle x' = f(x)\rangle P}}{\Gamma, p > 0 \vdash \langle x' = f(x) \,\&\, p > 0\rangle P}$$

The left premise proves the invariance of $p > 0$ for ODE $x' = f(x)$ with domain constraint P. The elided derivation (see proof) reduces to two premises which are identical to those of rule SLyap. The right premise uses rule SLyap, which necessitates the compactness assumption for formula K for soundness. □

The following staging sets with domain constraints proof rule SP& [SJ15] generalizes rule SP using axiom SAR. Notably, unlike the preceding rules, rule SP& requires no topological assumptions[9] about the domain constraint Q nor of the goal region P so it can be used in proofs of more general liveness properties.

Corollary 21 (Staging sets with domains [SJ15])**.** *The following proof rule is derivable in* dL*. Term $\varepsilon()$ is constant for ODE $x' = f(x)$, and the ODE has provable global solutions.*

$$\text{SP\&}\ \frac{\Gamma \vdash [x' = f(x) \,\&\, \neg(P \wedge Q)]S \quad S \vdash Q \wedge p \leq 0 \wedge \dot{p} \geq \varepsilon()}{\Gamma, \varepsilon() > 0 \vdash \langle x' = f(x) \,\&\, Q\rangle P}$$

Proof Sketch (Proof in Appendix B.3). The derivation starts with a SAR refinement step. On the resulting left premise, an M['] monotonicity step yields the left premise and first (leftmost) conjunct of the right premise of rule SP&. On the resulting right premise, rule SP is used with a similar (see full proof) monotonicity step, which yields the remaining conjuncts of the right premise of rule SP&.

$$\text{SAR}\ \frac{\text{M[']}\ \dfrac{\Gamma \vdash [x' = f(x) \,\&\, \neg(P \wedge Q)]S \qquad S \vdash Q}{\Gamma \vdash [x' = f(x) \,\&\, \neg(P \wedge Q)]Q} \qquad \text{SP}\ \dfrac{\dfrac{S \vdash p \leq 0 \wedge \dot{p} \geq \varepsilon()}{\dots}}{\Gamma \vdash \langle x' = f(x)\rangle P}}{\Gamma \vdash \langle x' = f(x) \,\&\, Q\rangle P}$$ □

The rules derived in Corollaries 18–21 demonstrate the flexibility of dL's refinement approach for deriving the surveyed liveness arguments as proof rules. Indeed, their derivations are mostly straightforward adaptations of the corresponding rules presented in Sect. 6, with the appropriate addition of either a COR or SAR axiomatic refinement step. Moreover, the derived rules are sound, in contrast to the liveness arguments which were missing subtle assumptions in the literature (summarized in Table 1). The flexibility (and soundness) of this article's approach is not limited to the surveyed liveness arguments because refinement steps can also be freely mixed-and-matched for specific liveness questions.

Example 7 (Strengthening). The liveness property $u^2 + v^2 = 1 \rightarrow \langle\alpha_n\rangle u^2 + v^2 \geq 2$ for α_n (2) was proved in Example 5 using the staging set formula $S \equiv 1 \leq u^2 + v^2 \leq 2$, and provably strengthened in Example 6 by adding the domain constraint $u^2+v^2 \geq 1$ with a DR$\langle\cdot\rangle$ refinement. Since S and $u^2+v^2 \geq 2$ characterize closed sets, the refinement axiom COR proves an even stronger liveness property with the strengthened domain S, as shown in the derivation below. The derivation starts with axiom COR which yields three premises. The leftmost premise is proved by $\mathbb{R}$ since it is a real arithmetic fact, the middle premise proves because S is an invariant of the ODE α_n (proof elided [PT20]), and the rightmost premise is proved in Example 5.

[9] Aside from this article's standing assumption that P, Q are formulas of first-order real arithmetic which is crucial for the soundness of axiom SAR.

$$\text{COR}\,\dfrac{\mathbb{R}\dfrac{*}{u^2+v^2=1 \vdash \neg(u^2+v^2 \geq 2)} \quad \dfrac{*}{u^2+v^2=1 \vdash [\alpha_n \,\&\, \neg(u^2+v^2 \geq 2)]S} \quad \dfrac{*}{u^2+v^2=1 \vdash \langle \alpha_n \rangle u^2+v^2 \geq 2}}{u^2+v^2=1 \vdash \langle \alpha_n \,\&\, S \rangle u^2+v^2 \geq 2}$$

Axiom COR extends the chain of refinements (6) from Example 5 as follows:

$$\langle \alpha_n, t'=1 \rangle \left(t > \frac{2}{3} \lor \neg S \right) \xrightarrow{\text{K}\langle\&\rangle} \langle \alpha_n \rangle \neg S \xrightarrow{\text{K}\langle\&\rangle} \langle \alpha_n \rangle u^2+v^2 \geq 2 \xrightarrow{\text{COR}} \langle \alpha_n \,\&\, S \rangle u^2+v^2 \geq 2$$

The alternative staging set formula $\widetilde{S} \equiv 1 \leq u^2+v^2 < 2$ can also be used to prove Example 5 with a similar refinement chain (using SP_b instead of SP_c), but $\widetilde{S}$ does *not* characterize a closed set. The topological restriction of axiom COR crucially prevents its unsound use (indicated by $\lightning$):

$$\underbrace{\langle \alpha_n, t'=1 \rangle \left(t > \frac{2}{3} \lor \neg \widetilde{S} \right) \xrightarrow{\text{K}\langle\&\rangle} \langle \alpha_n \rangle \neg \widetilde{S} \xrightarrow{\text{K}\langle\&\rangle} \langle \alpha_n \rangle u^2+v^2 \geq 2}_{\text{Similar to Example 5}} \underbrace{\xrightarrow{\text{COR}\lightning}}_{\text{Unsound step!}} \langle \alpha_n \,\&\, S \rangle u^2+v^2 \geq 2$$

The liveness property $\langle \alpha_n \,\&\, \widetilde{S} \rangle u^2+v^2 \geq 2$ is unsatisfiable because $\widetilde{S}$ does not overlap with $u^2+v^2 \geq 2$. The weakening of an inequality between domain constraints S and $\widetilde{S}$ leads to a wholly different conclusion!

The refinement approach also enables the discovery of new, general liveness proof rules by combining the underlying refinement steps in alternative ways. As an example, the following chimeric proof rule combines ideas from Corollaries 14, 16, and 21:

Corollary 22 (Combination proof rule)**.** *The following proof rule is derivable in* dL. *Formula S characterizes a compact set over variables x.*

$$\text{SP}_c^k\&\ \dfrac{\Gamma \vdash [x'=f(x) \,\&\, \neg(P \land Q)]S \qquad S \vdash Q \land \dot{p}^{(k)} > 0}{\Gamma \vdash \langle x'=f(x) \,\&\, Q \rangle P}$$

Proof Sketch (Proof in Appendix B.3). The derivation combines ideas from the derivations of $\text{dV}_{\succcurlyeq}^k$ (generalizing $\text{dV}_{\succcurlyeq}$ to higher derivatives), SP_c (compact staging sets), and SP& (refining domain constraints). □

The logical approach of dL derives complicated proof rules like $\text{SP}_c^k\&$ from a small set of sound logical axioms, which ensures their correctness. The proof rule $\text{E}_c\&$ below is derived from rule $\text{SP}_c^k\&$ (for $k=1$) and is adapted from the literature [PR07, Theorem 3.5], where additional restrictions were imposed on the sets characterized by Γ, P, Q, and different conditions were given compared to the left premise of $\text{E}_c\&$ (highlighted below). These original conditions were overly permissive as they are checked on sets that are smaller than necessary for soundness. See Appendix C for counterexamples to those original conditions.

Corollary 23 (Compact eventuality [PR07])**.** *The following proof rule is derivable in* dL. *Formula $Q \land \neg P$ characterizes a compact set over variables x.*

$$\text{E}_c\&\ \dfrac{\underline{\Gamma \vdash [x'=f(x) \,\&\, \neg(P \land Q)]Q} \qquad Q, \neg P \vdash \dot{p} > 0}{\Gamma \vdash \langle x'=f(x) \,\&\, Q \rangle P}$$

Proof Sketch (Proof in Appendix B.3). Rule $\text{E}_c\&$ is derived from $\text{SP}_c^k\&$ (for $k=1$), with $S \equiv Q \land \neg P$. □

7. ODE liveness proofs in practice

The preceding sections show how axiomatic refinement can be used to fruitfully navigate and understand the zoo of ODE existence and liveness arguments from various applications (Table 1). The generality of the approach enables the sound and foundational derivation of those arguments from a parsimonious basis of refinement steps. This section provides a complementary study of how the refinement approach and its derived ODE existence and liveness proof rules are best implemented in practice. There are two canonical approaches for such an implementation:

1. Implement the foundational refinement steps and let users build their own arguments using those steps, e.g., by following the derivations and proofs from Sects. 4–6.

2. Implement the zoo of proof rules from Sects. 4–6 directly and let users pick from from those rules for their particular ODE liveness applications.

The low-level flexibility of Approach 1 is also its drawback in practice because users need to tediously reconstruct high-level ODE liveness arguments from basic refinements for each proof. Approach 2 provides users with those high-level arguments but limits users to proof rules that have been implemented, which squanders the generality of the refinement approach. Moreover, users would still need to navigate the redundancies and tradeoffs among the zoo of proof rules to select one that is best-suited for their proof. To account for these drawbacks, this section advocates for a middle ground between those two extremes: implementations should provide users with the basic refinement steps, bundled with a set of carefully curated, high-level proof rules (Sect. 7.1) and associated proof support (Sect. 7.2) that help users navigate the common cases in their liveness proofs.

These ideas are put into practice through an implementation of ODE existence and liveness proof rules in KeYmaera X [FMQ$^+$15]. Proof rules and proof support are implemented as *tactics* in KeYmaera X [FMBP17], which are not soundness-critical. Such an arrangement allows for the implementation of useful ODE liveness proof rules and their associated proof support with KeYmaera X's sound kernel as a safeguard against implementation errors or mistakes in their derivations and side conditions. This core design decision underlying KeYmaera X is discussed elsewhere [FMQ$^+$15, FMBP17, Pla17a]. All of the ODE liveness examples in this article have been formally proved in KeYmaera X (Sect. 7.2.3). By leveraging existing infrastructure in KeYmaera X, the implementation can also be used as part of liveness proofs for hybrid systems. It is used for the liveness proofs of a case study involving a robot model driving along circular arcs in the plane [BTM$^+$19].

The basic refinements steps from Sect. 3 and the proof rules in Sects. 4–6 are mostly straightforward to implement by following their respective proofs. Thus, Sects. 7.1 and 7.2 focus on a select number of new proof rules and proof support that are beneficial in the implementation. For the sake of completeness, syntactic derivations of all liveness proof rules presented in these sections are given in Appendix B.4.

7.1. Liveness proof rules

Atomic differential variants $\mathrm{dV}_{\succcurlyeq}$ is a useful primitive proof rule to implement in KeYmaera X because many ODE liveness proof rules, e.g., $\mathrm{dV}_{=}^{M}$, SP, derive from it. From a practical perspective though, rule $\mathrm{dV}_{\succcurlyeq}$ as presented in Corollary 12 still requires users to provide a choice of the constant $\varepsilon()$, e.g., the proof in Example 4 uses $\varepsilon() = \frac{1}{2}$. The following slight rephrasing of $\mathrm{dV}_{\succcurlyeq}$ enables a more automated implementation.

Corollary 24 (Existential atomic differential variants [Pla10])**.** *The following proof rule (where $\succcurlyeq$ is either $\geq$ or $>$) is derivable in* dL*, where ε is a fresh variable and ODE $x' = f(x)$ has provable global solutions.*

$$\mathrm{dV}_{\succcurlyeq}^{\exists}\ \frac{\Gamma \vdash \exists \varepsilon > 0\, \forall x \left(\neg(p \succcurlyeq 0) \rightarrow \dot{p} \geq \varepsilon\right)}{\Gamma \vdash \langle x' = f(x)\rangle p \succcurlyeq 0}$$

Proof Sketch (Proof in Appendix B.4). Rule $\mathrm{dV}_{\succcurlyeq}^{\exists}$ is derived from $\mathrm{dV}_{\succcurlyeq}$ as a corollary. □

Just like rule $\mathrm{dV}_{\succcurlyeq}$, rule $\mathrm{dV}_{\succcurlyeq}^{\exists}$ requires a positive lower bound $\varepsilon > 0$ on the derivative of p along solutions. The difference is that the premise of rule $\mathrm{dV}_{\succcurlyeq}^{\exists}$ is rephrased to ask a purely arithmetical question about the existence of a suitable choice for ε. This can be decided automatically to save user effort in identifying ε, but such automation comes at added computational cost because the decision procedure must *find* a suitable instance of ε for the $\exists$ quantifier (or decide that none exist) rather than simply *check* a user-provided instance. Thus, the implementation gives users control over the desired degree of automation in their proof by giving them the option of either invoking an arithmetic decision procedure $\mathbb{R}$ on the premise of $\mathrm{dV}_{\succcurlyeq}^{\exists}$ or manually instantiating the existential quantifier with a specific term for ε.

Another useful variation of rule $\mathrm{dV}_{\succcurlyeq}$ is its *semialgebraic* generalization, i.e., where the goal region is described by a formula P formed from conjunctions and disjunctions of (in)equalities. Rules $\mathrm{dV}_{=}^{M}$, SP provide examples of such a generalization, but they are indirect generalizations because users must still identify an underlying (atomic) differential variant p as input when applying either rule. In contrast, the new semialgebraic generalization of $\mathrm{dV}_{\succcurlyeq}$ below directly examines the syntactic structure of the goal region described by formula P. Its implementation is enabled by KeYmaera X's ODE invariance proving capabilities which are, in turn, based on dL's complete axiomatization for ODE invariants [PT20].

Corollary 25 (Semialgebraic differential variants)**.** *Let b be a fresh variable, and term $\varepsilon()$ be constant for ODE $x' = f(x), t' = 1$. Let P be a semialgebraic formula in the following normal form* [PT20, Eq 5]*, and G_P be its corresponding ε-progress formula (also in normal form):*

$$P \equiv \bigvee_{i=0}^{M} \left(\bigwedge_{j=0}^{m(i)} p_{ij} \geq 0 \wedge \bigwedge_{j=0}^{n(i)} q_{ij} > 0 \right) \qquad G_P \equiv \bigvee_{i=0}^{M} \left(\bigwedge_{j=0}^{m(i)} p_{ij} - (b + \varepsilon()t) \geq 0 \wedge \bigwedge_{j=0}^{n(i)} q_{ij} - (b + \varepsilon()t) \geq 0 \right)$$

The following proof rule is derivable in dL*, where the ODE $x' = f(x)$ has provable global solutions, and $(\dot{\neg P})^{(*)}, (\dot{G_P})^{(*)}$ are semialgebraic progress formulas* [PT20, Def. 6.4][10] *with respect to $x' = f(x), t' = 1$.*

$$\text{dV}\ \frac{\neg P, (\dot{\neg P})^{(*)}, G_P \vdash (\dot{G_P})^{(*)}}{\Gamma, \varepsilon() > 0 \vdash \langle x' = f(x) \rangle P}$$

$$\text{dV}^{\exists}\ \frac{\Gamma \vdash \exists \varepsilon > 0\, \forall b\, \forall t\, \forall x \left(\neg P \wedge (\dot{\neg P})^{(*)} \wedge G_P \rightarrow (\dot{G_P})^{(*)} \right)}{\Gamma, \varepsilon() > 0 \vdash \langle x' = f(x) \rangle P}$$

Proof Sketch (Proof in Appendix B.4). Rule $\text{dV}^{\exists}$ is derived from dV similar to the derivation of rule $\text{dV}^{\exists}_{\succcurlyeq}$ from $\text{dV}_{\succcurlyeq}$. The derivation of dV is similar to rules $\text{dV}^{\Gamma}_{\succcurlyeq}$, $\text{dV}_{\succcurlyeq}$, but replaces the use of rule $\text{dI}_{\succcurlyeq}$ with the complete ODE invariance proof rule [PT20, Theorem 6.8]. The fresh variable b is used as a lower bound of the value of all polynomials p_{ij}, q_{ij} appearing in the description of P along solutions of the ODE. □

The intuition behind rule dV is similar to rule $\text{dV}_{\succcurlyeq}$: as long as the solution has not yet reached the goal P, it grows towards P at "rate" $\varepsilon()$. The technical challenge is how to formally phrase the "rate" of growth for a semialgebraic formula P, which does not have a well-defined notion of derivative. Rule dV uses the ε-progress formula G_P, together with the semialgebraic progress formulas $(\dot{\neg P})^{(*)}, (\dot{G_P})^{(*)}$ and dL's completeness result for ODE invariants [PT20, Theorem 6.8] for this purpose. These formulas give sufficient, although implicit, arithmetical conditions for proving liveness for P. Rule $\text{dV}^{\exists}$ rephrases dV with an arithmetical premise, similar to how $\text{dV}^{\exists}_{\succcurlyeq}$ rephrases $\text{dV}_{\succcurlyeq}$, to give users the added flexibility of choosing between invoking an automated decision procedure or manually instantiating the existential quantifier for ε and reasoning about the resulting progress formulas. More explicit arithmetical premises for dV, $\text{dV}^{\exists}$ can be obtained by unfolding the definitions [PT20, Def. 6.4] of $(\dot{\neg P})^{(*)}, (\dot{G_P})^{(*)}$ as exemplified below.

Example 8 (Non-differentiable progress functions [SJ15]). Consider the following liveness formula with two inequalities in its postcondition:

$$\langle u' = -u \rangle (-1 \leq u \leq 1) \tag{18}$$

Using the min function, formula (18) can be written equivalently with a single atomic inequality:

$$\langle u' = -u \rangle \min(1 - u, u + 1) \geq 0 \tag{19}$$

However, the postcondition of (19) is not a formula of real arithmetic (Sect. 2.1) and it does not have well-defined dL semantics. Indeed, rule $\text{dV}_{\succcurlyeq}$ does not prove (19) because the Lie derivative of its postcondition is not well-defined. One possible solution is to generalize $\text{dV}_{\succcurlyeq}$ by considering directional derivatives of continuous (but non-differentiable) functions such as min, max [SJ15, Section 5.2]. However, justifying the correctness of this option would require delicate changes to dL semantics [BFP19, Pla17a]. Rule dV instead proves (18) directly without requiring rephrasing, nor complications associated with directional derivatives. The proof is as follows, with $\varepsilon() = 1$ and $P \equiv u+1 \geq 0 \wedge 1-u \geq 0, G_P \equiv u+1-(b+t) \geq 0 \wedge 1-u-(b+t) \geq 0$:

[10] The arithmetic formula $\dot{P}^{(*)}$ exactly characterizes that the ODE $x' = f(x)$ makes local progress in P for some nonzero duration, see prior work [PT20, Def 6.4, Thm. 6.6]. The semialgebraic progress formula operator commutes with logical negation for semialgebraic formulas P, i.e., the equivalence $(\dot{\neg P})^{(*)} \leftrightarrow \neg(\dot{P}^{(*)})$ is provable [PT20, Cor 6.7]. Hence, local progress into $\neg P$ is equivalent to the solution locally staying away from P for nonzero duration.

$$\text{dV}\,\dfrac{\dfrac{\dfrac{\mathbb{R}\,\dfrac{*}{u+1<0 \lor 1-u<0, u+1-(b+t) \geq 0 \land 1-u-(b+t) \geq 0 \vdash (u+1-(b+t)=0 \to -u-1>0) \land \ldots}}{\neg P, G_P \vdash (\dot{G_P})^{(*)}}}{\neg P, (\dot{\neg P})^{(*)}, G_P \vdash (\dot{G_P})^{(*)}}}{\vdash \langle u' = -u \rangle (-1 \leq u \leq 1)}$$

The proof starts by using rule dV, where the assumption $(\dot{\neg P})^{(*)}$ in its premise is weakened as it is unnecessary for the proof. Unfolding the definition of $(\dot{G_P})^{(*)}$ and simplifying leaves an arithmetical question in the succedent with two conjuncts; the right conjunct is omitted for brevity since the subsequent argument is symmetric. The left conjunct in the succedent is proved by $\mathbb{R}$ because the assumptions $u+1-(b+t)=0$ and $u+1-(b+t) \geq 0 \land 1-u-(b+t) \geq 0$ imply $1-u \geq u+1$. This, in turn, implies $-u-1>0$ using the assumption $u+1<0 \lor 1-u<0$.

More generally, for a liveness postcondition comprising a conjunction of atomic inequalities $p \succcurlyeq 0 \land q \succcurlyeq 0$ (where $\succcurlyeq$ is either $\geq$ or $>$ in either conjunct), the premise resulting from applying dV can be simplified in real arithmetic to the following arithmetical premise:

$$\neg(p \succcurlyeq 0 \land q \succcurlyeq 0) \vdash (p<q \to \dot{p} > \varepsilon()) \land (p>q \to \dot{q} > \varepsilon()) \land (p=q \to \dot{p} > \varepsilon() \land \dot{q} > \varepsilon()) \tag{20}$$

The arithmetical premise (20) is equivalent to the arithmetical progress conditions for $\min(p,q) \geq 0$ [SJ15, Example 14], and both are decidable in real arithmetic. The intuition behind (20) is that whenever p is further from the goal than q, then p is required to make ε progress towards the goal (symmetrically when q is further than p from the goal). A similar simplification of dV for a disjunctive postcondition $p \succcurlyeq 0 \lor q \succcurlyeq 0$ is shown in (21), which asks for the term closer to the goal to make ε progress towards the goal instead. Further simplifications for semialgebraic formulas P are obtained as nested combinations of (20) and (21).

$$\neg(p \succcurlyeq 0 \lor q \succcurlyeq 0) \vdash (p<q \to \dot{q} > \varepsilon()) \land (p>q \to \dot{p} > \varepsilon()) \land (p=q \to \dot{p} > \varepsilon() \lor \dot{q} > \varepsilon()) \tag{21}$$

This example shows the intricate definition of semialgebraic progress formulas, even for the simple-looking conjunctive postcondition $-1 \leq u \leq 1$, which highlights the need for a careful and trustworthy implementation of rules dV, $\text{dV}^{\exists}$, as provided by KeYmaera X.

The variations of $\text{dV}_{\succcurlyeq}$ shown in Corollaries 24 and 25 (and their implementation) allow users to focus on high-level liveness arguments in KeYmaera X rather than low-level derivation steps. Another key usability improvement afforded by an implementation is the sound and automatic enforcement of the appropriate side conditions for every proof rule. The common side conditions for ODE liveness proof rules presented in this article can be broadly classified as follows:

1. Freshness side conditions on variables, e.g., in rules $\text{dV}_{\succcurlyeq}$, $\text{dV}_{\succcurlyeq}^{\exists}$, dV, $\text{dV}^{\exists}$. These are automatically enforced in the implementation because KeYmaera X's kernel insists on fresh names when required for soundness. Renaming with fresh variables is also automatically supported.
2. Global existence of ODE solutions. These are semi-automatically proved (Sect. 7.2).
3. Topological side conditions, e.g., in axiom COR and rules $\text{dV}_{\succcurlyeq}\&$, $\text{dV}_{=}^{M}\&$. These conditions are important to correctly enforce because they may otherwise lead to the subtle soundness errors (Sect. 6). The implementation uses syntactic criteria for checking these side conditions (Appendix A.3).

An example topological refinement axiom (Lemma 4) and its corresponding proof rule implemented in KeYmaera X with syntactic topological side conditions is given next.

Lemma 26 (Closed domain refinement axiom)**.** *The following topological $\langle\cdot\rangle$ ODE refinement axiom is sound, where formula Q characterizes a topologically closed set over variables x, and formula $\mathring{Q}$ characterizes the topological interior of the set characterized by Q.*

CR $\neg P \land [x' = f(x) \,\&\, R \land \neg P]\mathring{Q} \to \big(\langle x' = f(x) \,\&\, R\rangle P \to \langle x' = f(x) \,\&\, Q\rangle P\big)$

Proof in Appendix *A.2*.

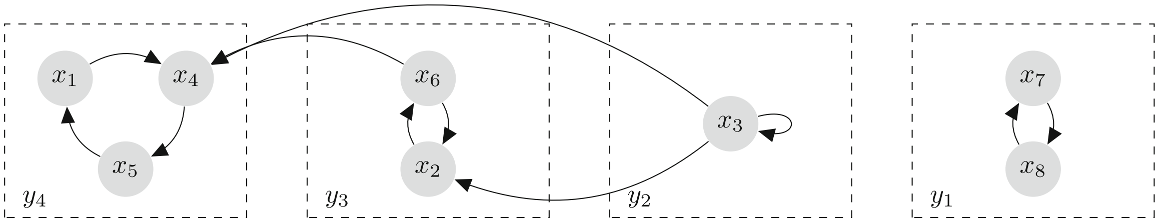


Fig. 4. A dependency graph for the ODE (22) over the variables $x_1, \ldots, x_8$. There is a directed edge $x_i \longrightarrow x_j$ if the RHS for x'_j depends on free variable x_i. Each dashed rectangle is a strongly connected component. Topologically sorting these components (according to the order induced by the edges) yields one possible grouping of the variables $y_1, \ldots, y_4$ in dependency order. The vertices in y_1 are not connected to those in y_2, y_3, y_4, so the order between these groups can be chosen arbitrarily.

Corollary 27 (Closed domain refinement rule)**.** *The following proof rule is derivable in* dL*, where formula Q is formed from finite conjunctions and disjunctions of non-strict inequalities $\geq, \leq$, and formula $Q_{\geq}^{>}$ is identical to Q but with strict inequalities $>, <$ in place of $\geq, \leq$ respectively.*

$$\text{cR}\ \frac{\Gamma \vdash Q \quad \Gamma \vdash [x' = f(x) \,\&\, R \land \neg P \land Q] Q_{\geq}^{>} \quad \Gamma \vdash \langle x' = f(x) \,\&\, R \rangle P}{\Gamma \vdash \langle x' = f(x) \,\&\, Q \rangle P}$$

Proof in Appendix B.4.

Axiom CR is a variant of axiom COR with different topological conditions. It says that if the ODE solution can reach goal P while staying in domain R then it can also reach that goal while staying in the new (closed) domain Q, provided that it stays within the *interior* $\mathring{Q}$ of the new domain while it has not yet reached P. Solutions cannot sneak out of the topologically open interior $\mathring{Q}$ as it enters the goal because, by definition of an open set, the solution must locally remain in $\mathring{Q}$ for a short time as it enters the goal (see the proof for a detailed explanation). In contrast to the semantical conditions of CR, its corresponding derived rule cR gives syntactic side conditions for the formulas $Q, Q_{\geq}^{>}$ which are easily checked in an implementation. In particular, formula $Q_{\geq}^{>}$, which syntactically underapproximates the interior $\mathring{Q}$, can be automatically generated from Q through its syntactic structure. Another advantage of the derived rule cR is that the closed domain constraint Q can be additionally assumed when proving that solutions stay within $Q_{\geq}^{>}$ in its middle premise. This addition is soundly justified using dL's ODE invariance proof rules [PT20] (see proof) and it makes rule cR a powerful primitive for refining domain constraints amongst other options such as axiom DR⟨·⟩.

7.2. Proof support

Beyond enabling the sound implementation of complex ODE liveness proof rules such as those in Sect. 7.1, tactics can also provide substantial proof support for users.

7.2.1. Automatic dependency ordering

Recall derived axiom GBEx from Corollary 10, which proves (global) existence of solutions for an ODE $x' = f(x)$. Users of the axiom must still identify precisely which dependency order (9) to use, and provide the sequence of bounded sets B_i for each group of variables y_i involving nonlinear ODEs. The canonical choice of such a dependency order can be automatically produced by a tactic using a topological sort of the *strongly connected components* (SCCs)[11] of the dependency graph of the ODE.

More precisely, to prove global existence for an ODE $x' = f(x)$, consider the dependency graph G where each variable x_i is a vertex and with a directed edge $x_i \longrightarrow x_j$ if the RHS $f_j(x)$ for x'_j depends on free variable x_i. First, compute the SCCs of G, and then topologically sort the SCCs.

[11] A strongly connected component of a directed graph is a maximal subset of vertices that are pairwise connected by paths.

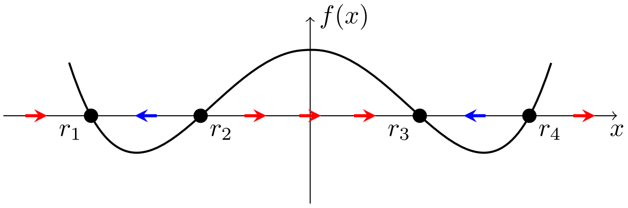


Fig. 5. The univariate ODE $x' = x^4 - 5x^2 + 4$ is can be illustrated by plotting its RHS $f(x) = x^4 - 5x^2 + 4$ (vertical axis) against x (horizontal axis). Points on the horizontal axis evolve towards the right (red arrow) when $f(x) \geq 0$ and towards the left (blue arrow) when $f(x) \leq 0$. The fixed points r_1, r_2, r_3, r_4 are roots of the polynomial RHS where $f(x) = 0$. These fixed points either attract trajectories (like r_1, r_3), or repel them (like r_2, r_4). All points on the horizontal axis evolve asymptotically towards exactly one fixed point or approach ∞.

The groups of variables y_i in dependency order can be chosen according to the vertices in each SCC in topological order. An illustrative dependency graph with four SCCs for the following 8-dimensional ODE is shown in Fig. 4.

$$x_1' = x_5, x_2' = x_3 + x_6^2, x_3' = x_3^2, x_4' = x_1 + x_3^2 + x_6^2, x_5' = x_4, x_6' = x_2^2, x_7' = x_8, x_8' = -x_7 \tag{22}$$

After finding the appropriate SCC-induced dependency order (as in Fig. 4), the global existence tactic can prove global existence for the variable clusters y_i that have affine dependencies within the cluster automatically. For example, the SCC $y_4 \equiv \{x_1, x_4, x_5\}$ has affine dependencies because the RHS of the ODEs x_1', x_4', x_5' are affine in x_1, x_4, x_5, so the solution of ODE (22) is automatically proved to be global in those variables following the proof of Corollary 8. The generated dependency order enables such a proof even though the RHS of x_4' depends nonlinearly on variables x_3, x_6 from earlier clusters. On the other hand, the SCC $y_3 \equiv \{x_2, x_6\}$ has nonlinear dependencies on x_2, x_6, so users are prompted to input a bounded set (or a bound on derivatives) over variables x_2, x_6 in order to prove global existence for those variables. This continues similarly for the SCCs y_2 (nonlinear dependency) and y_1 (affine dependency) until global existence is proved for the full ODE. This semi-automated proof support minimizes the manual effort required of the user in proving global existence by focusing their attention on the automatically identified nonlinear parts of the ODE that may cause finite-time blowup of solutions.

To drive global existence proof automation further, key special cases can be added to the method described above. One such special case for univariate ODEs is shown below.

Remark 2 (Global existence for univariate ODEs). Consider the case where a variable group has just one variable and no incoming dependencies, e.g., $y_2 \equiv \{x_3\}$ in Fig. 4 or α_b (7). Global existence for such univariate polynomials ODEs is decidable [GBC08], even if the RHS is highly nonlinear, because all of its solutions either asymptotically approach a root of the polynomial RHS or diverge to infinity.

This result is best illustrated through the dynamical systems view of ODEs shown in Fig. 5 for the ODE $x' = x^4 - 5x^2 + 4$. This example ODE has global solutions from all initial states satisfying $x \leq r_4$ because the solution from all such states are globally attracted to one of the fixed points. Conversely, for all other initial conditions ($x > r_4$), the ODE blows up in finite time because the RHS is quartic in x.

More generally, for a nonlinear univariate polynomial ODE $x' = f(x)$ and initial assumptions Γ, it suffices to check validity of the following arithmetical sequent to decide global existence:

$$\Gamma \vdash \exists r\, \big(f(r) = 0 \land (\underbrace{f(x) \geq 0 \land r \geq x}_{\textcircled{a}} \lor \underbrace{f(x) \leq 0 \land r \leq x}_{\textcircled{b}})\big)$$

The existentially quantified variable r corresponds to a fixed point (a root with $f(r) = 0$). Disjunct $\textcircled{a}$ checks whether the solution approaches r from the left, e.g., the points between r_2 and r_3 in Fig. 5 approach r_3 from the left. Alternatively, disjunct $\textcircled{b}$ checks whether the solution approaches r from the right. The implementation checks validity of this sequent for univariate nonlinear ODEs and then proves global existence using BDG$\langle\cdot\rangle$ because the solution is provably trapped between the initial value of x and the fixed point r.

7.2.2. Differential cuts for liveness proofs

Differential cuts dC provide a convenient way to structure and stage safety proofs for ODEs in dL. An in-depth discussion is available elsewhere [Pla18], but the idea is illustrated by the following derivation:

$$\text{dC}\,\cfrac{\Gamma \vdash [x'=f(x)\,\&\,Q]C_1 \qquad \text{dC}\,\cfrac{\cdots \qquad \text{dC}\,\cfrac{\text{dW}\,\cfrac{Q \land C_1 \land C_2 \land \cdots \land C_n \vdash P}{\vdots}}{\Gamma \vdash [x'=f(x)\,\&\,Q \land C_1 \land C_2]P}}{\Gamma \vdash [x'=f(x)\,\&\,Q \land C_1]P}}{\Gamma \vdash [x'=f(x)\,\&\,Q]P}$$

The derivation uses a sequence of differential cut steps to progressively add the cuts $C_1, C_2, \ldots, C_n$ to the domain constraint. A final dW step completes the proof when the postcondition P is already implied by the (now strengthened) domain constraint. Intuitively, the differential cuts are akin to dynamical lemmas in this derivation. For example, by proving the premise $\Gamma \vdash [x'=f(x)\,\&\,Q]C_1$, the cut C_1 can now be assumed in the domain constraints of subsequent steps. Just like the cut rule from sequent calculus, differential cuts dC allow safety proofs for ODEs to be staged through a sequence of lemmas about those ODEs.

For proof modularity and maintainability, it is desirable to enable a similar staging for ODE liveness proofs. Concretely, suppose that the formula $[x'=f(x)\,\&\,Q]C$ has been proved as a cut:

$$\text{cut}\,\cfrac{\Gamma \vdash [x'=f(x)\,\&\,Q]C \qquad \cdots}{\Gamma \vdash \langle x'=f(x)\,\&\,Q\rangle P}$$

The challenge is how to (soundly) use this lemma in subsequent derivation steps (shown as $\cdots$). Naïvely replacing Q with $Q \land C$ in the domain constraint of the succedent does not work. This may even do more harm than good because the resulting ODE liveness question becomes more difficult (Sect. 6).

The refinement-based approach to ODE liveness provides a natural answer: recall that each refinement step in the chain (6) requires the user to prove an additional box modality formula. The insight is that, for these box modality formulas, any relevant lemmas that have been proved can be soundly added to the domain constraint. For example, suppose that rule K⟨&⟩ is used to continue the proof after the cut. The left premise of K⟨&⟩ can now be strengthened to include C in its domain constraint:

$$\text{K}\langle\&\rangle\,\cfrac{\text{dC}\,\cfrac{\Gamma, [x'=f(x)\,\&\,Q]C \vdash [x'=f(x)\,\&\,Q \land \neg P \land C]\neg G}{\Gamma, [x'=f(x)\,\&\,Q]C \vdash [x'=f(x)\,\&\,Q \land \neg P]\neg G} \qquad \Gamma, [x'=f(x)\,\&\,Q]C \vdash \langle x'=f(x)\,\&\,Q\rangle G}{\Gamma, [x'=f(x)\,\&\,Q]C \vdash \langle x'=f(x)\,\&\,Q\rangle P}$$

Users could manually track and apply lemmas using dC as shown above, but this becomes tedious in larger liveness proofs. The implementation instead provides users with tactics that automatically search the antecedents Γ for compatible assumptions that can be used to strengthen the domain constraints. These tactics also use a form of *ODE unification* when determining compatibility. More precisely, consider the sequent $\Gamma \vdash [x'=f(x)\,\&\,Q]P$, which may arise as a box refinement during a liveness proof. An antecedent formula $[y'=g(y)\,\&\,R]C$ in Γ is called a *compatible assumption* for the succedent $[x'=f(x)\,\&\,Q]P$ if:

1. The set of ODEs $y'=g(y)$ is a subset of the set of ODEs $x'=f(x)$. This is order-agnostic, e.g., the ODE $u'=v, v'=u$ is a subset of the ODE $v'=u, u'=v, w'=u+v+w$.
2. The domain constraint Q implies domain constraint R, i.e., $Q \to R$ is valid.

Under these conditions, the ODE $y'=g(y)\,\&\,R$ permits more trajectories than the ODE $x'=f(x)\,\&\,Q$. Thus, if formula C is always true along solutions of the former ODE, then it also stays true along solutions of the latter. Combining compatible assumptions with implementations of liveness proof rules yields turbocharged versions of those rules. For example, in rule $\text{dV}^{\exists}_{\succcurlyeq}$, instead of simply assuming the negation of the postcondition ($\neg(p \succcurlyeq 0) \to \cdots$) when determining the existence of suitable ε, all postconditions of compatible assumptions can be assumed, e.g., with $\neg(p \succcurlyeq 0) \land C \to \cdots$ for postcondition C of a compatible assumption.

7.2.3. Microbenchmarks

The KeYmaera X implementation is used to formally prove all of the ODE liveness examples from this article and elsewhere [SJ15, BTM$^+$19]. Table 2 provides a summary of statistics from these proofs: “Tactic Steps” counts the number of (manual) user proof steps; “Kernel Steps” counts the number of internal steps taken by the soundness-critical KeYmaera X kernel; and “Proof Time” measures the time taken (in seconds, averaged over 5 runs, rounded to 3 decimal places) for the proof to execute in KeYmaera X.

Table 2. Proof statistics for ODE existence and liveness properties proved using the implementation

Liveness property	Tactic steps		Kernel Steps		Proof time (s)	
	(M)	(A)	(M)	(A)	(M)	(A)
Example 1	7	**3**	**2040**	12156	**1.778**	3.716
Example 2	8	**2**	962	**898**	0.220	**0.203**
Example 3	7	**3**	**1562**	1580	**0.551**	0.759
Example 4	29	**5**	3958	**3501**	3.286	**3.034**
Example 7 (Examples 5 and 6)	50	**20**	**5549**	6141	**1.714**	1.952
Example 8	28	**1**	**1747**	2571	**0.575**	0.990
[SJ15] Example 11	–	50	–	11272	–	9.090
[SJ15] Example 12	–	19	–	4818	–	1.388
[SJ15] Example 15	–	1	–	4781	–	1.730
[BTM+19] goal position reachability	–	34	–	8159	–	2.182
[BTM+19] velocity bounds reachability	–	37	–	10521	–	3.042

For this article's Examples 1–8, two proofs are presented: (M)anual proofs closely follow the pen-and-paper derivations shown in this article, while (A)utomatic proofs make extensive use of the implemented proof support. The cells in **bold** font indicate lower (more desirable) values. The stronger ODE liveness property proved in Example 7 implies those from Examples 5 and 6. Examples 11, 12 and 15 refer to the correspondingly numbered examples from Sogokon and Jackson [SJ15]

All experiments were run on an Ubuntu 18.04 laptop with a 2.70 GHz Intel Core i7-6820HQ CPU and 16GB memory. None of the proofs have been optimized to favor any specific metric. The specific timings and proof steps are naturally subject to change on different hardware and as various aspects of the KeYmaera X theorem prover are improved. Nevertheless, the key takeaways from these microbenchmarks remain broadly applicable.

(M)anual and (A)utomatic proofs. The implementation provides users with powerful proof support but also exposes low-level primitives for users who prefer more fine-grained control over (parts of) their proofs. Both types of proofs are shown for this article's examples in Table 2. Proofs that heavily exploit the proof support and automation are more convenient for users and require fewer manual tactic invocations. This gap is most pronounced for Example 8, where the 28 step manual proof requires just one automated dV step.

On the other hand, the automated proofs are slower than their manual counterparts on four out of six examples. Most of this overhead arises when there is significant proof search in the automation. In particular, the automated proof of Example 1 is significantly slower and requires almost six times more kernel steps compared to its manual counterpart. This gap arises because the automated proof uses the decision procedure for univariate global existence outlined in Remark 2 while the manual proof uses the direct argument in Example 1. However, the latter proof required user insight about the physical system. This illustrates the need for a flexible implementation that lets users navigate the convenience and efficiency tradeoff according to their needs and proof insights.

Finally, the automated proofs are in fact *faster* for Examples 2 and 4, which both involve linear ODEs. The speedups here can be attributed to the well-tuned implementation of global existence proofs for affine systems and to the use of rule $\mathrm{dV}^{\exists}_{\succcurlyeq}$ for the latter example. Thus, the aforementioned tradeoff can be further skewed towards favoring user convenience by tuning the implemented automation.

Trusted kernel with untrusted tactics. All of the proofs in Table 2 make extensive use of KeYmaera X's existing tactics framework [FMBP17] to handle low-level interactions with KeYmaera X soundness-critical kernel, as shown by the large number of kernel steps that each proof requires. The soundness guarantee provided by the KeYmaera X kernel makes this implementation effort a worthy tradeoff because it ensures that the proved results in Table 2 are trustworthy *without* needing to trust the implementation of the tactics.

Applicability. The insights of this section are not limited to this article's examples and they scale to larger proofs from elsewhere (Table 2). Notably, Sogokon and Jackson [SJ15] Example 11 proves two separate liveness properties for the same ODE, which makes it the largest (and slowest) microbenchmark. The examples from Bohrer et al. [BTM+19] are liveness properties drawn from a larger case study with a hybrid system model of a robot driving along circular arcs in the plane [BTM+19]. The use of proof automation (in both senses of the preceding paragraphs) is indispensable for handling the scale of these proofs.

8. Related work

Existence and liveness proof rules. The ODE liveness arguments surveyed in this article were originally presented in various notations, ranging from proof rules [Pla10, SJ15, TT10] to other mathematical notation [PR05, PR07, RS10, SJ15]. All of them were justified directly through semantical or mathematical means. This article unifies and corrects all of these arguments, and presents them as dL proof rules which are syntactically derived by refinement from dL axioms.

To the best of the authors' knowledge, this article is also the first to present a deductive approach for syntactic proofs of existence properties for ODEs. In the surveyed liveness arguments [Pla10, PR05, PR07, RS10, SJ15, TT10], sufficient existence duration is either assumed explicitly or is implicitly used in the correctness proofs. Such a hypothesis is unsatisfactory, since the global existence of solutions for (nonlinear) ODEs is a non-trivial question; in fact, it is undecidable even for polynomial ODEs [GBC08]. Formal proofs of any underlying existence assumptions thus yield stronger (unconditional) ODE liveness proofs. Of course, such existence properties are an additional proof burden, but Sect. 7 also shows that proof support can help by automating easy existence questions, e.g., for affine systems where global existence is well-known. A related problem arising in the study of hybrid systems is *Zeno phenomena* [Hen96, ZJLS01], where a trajectory of a hybrid model makes infinitely many (discrete) transitions in finite (continuous) time. Like finite-time blow up, Zeno phenomena typically occur as abstraction artifacts of hybrid systems models, and they do not occur in real systems. Thus, analogous to the question of global existence, absence of Zeno phenomena must either be assumed (or Zeno trajectories explicitly excluded) [Hen96, Pla10], or proved when specifying and verifying properties of such systems [ZJLS01].

The refinement-based approach to ODE existence and liveness proofs underlies this article's implementation described in Sect. 7. Compared to an earlier implementation [PQ08], where rules like $\mathrm{dV}_{\succcurlyeq}\&$ are implemented monolithically, this article's approach and implementation build those rules from smaller building blocks which yields a flexible implementation together with powerful (untrusted) proof support. The high-level lessons discussed in Sect. 7 are also broadly applicable to other deductive tools for ODEs and hybrid systems [WZZ15, FyMS20] that currently lack support for ODE liveness proofs.

Other liveness properties. The liveness property studied in this article is the continuous analog of *eventually* [MP92] or *eventuality* [PR07, SJ15] from temporal logics. In discrete settings, temporal logic specifications give rise to a zoo of other liveness properties [MP92]. In continuous settings, *weak eventuality* (requiring *almost all* initial states to reach the goal region) and *eventuality-safety* have been studied [PR05, PR07]. In adversarial settings, *differential game variants* [Pla17b] enable proofs of winning strategies for differential games. In dynamical systems and controls, the study of *asymptotic stability* requires both stability (an invariance property) with asymptotic attraction towards a fixed point or periodic orbit (an eventuality-like property) [Chi06, RS10]. For hybrid systems, various authors have proposed generalizations of classical asymptotic stability, such as *persistence* [SJJ19], *stability* [PW06], and *inevitability* [DM12]. *Controlled* versions of these properties are also of interest, e.g., *(controlled) reachability and attractivity* [ADBS09, TT10]. Eventuality(-like) properties are fundamental to all of these advanced liveness properties. The formal understanding of eventuality in this article is therefore a key step towards enabling formal analysis of more advanced liveness properties.

Automated liveness proofs. Automated reachability analysis tools [CÁS13, FGD+11] can also be used to answer certain liveness verification questions. For an ODE and initial set $\mathcal{X}_0$, computing an over-approximation $\mathcal{O}$ of the reachable set $\mathcal{X}_t \subseteq \mathcal{O}$ at time t shows that *all* states in $\mathcal{X}_0$ reach $\mathcal{O}$ at time t [SJJ19] (if solutions do not blow up). Similarly, an under-approximation $\mathcal{U} \subseteq \mathcal{X}_t$ shows that *some* state in $\mathcal{X}_0$ eventually reaches $\mathcal{U}$ [GP17] (if $\mathcal{U}$ is non-empty). Neither approach handles domain constraints directly [GP17, SJJ19] and, unlike deductive approaches, the use of reachability tools limits them to concrete time bounds t and bounded initial sets $\mathcal{X}_0$. Deductive liveness approaches can also be (partially) automated, as shown in Sect. 7. Lyapunov functions guaranteeing (asymptotic) stability can be found by sum-of-squares (SOS) optimization [PP02]. Liveness arguments can be similarly combined with SOS optimization to find suitable differential variants [PR05, PR07]. Other approaches are possible, e.g., a constraint solving-based approach can be used for finding the so-called *set Lyapunov functions* [RS10] (e.g., the term p used in SLyap, SLyap&). Crucially, automated approaches must ultimately be based on sound underlying liveness arguments. The correct justification of these arguments is precisely what this article enables.

Refinement calculi. This article's view of ODE liveness arguments as step-by-step refinements is closely related to *refinement proof calculi* [BvW98, Koz97]. The shared idea is that the proof of a complex property, like ODE liveness or program correctness, should be broken down into (simpler) step-by-step refinements. The key difference is that, for refinement calculi, refinement typically takes place between programs (or implementations) and their specification. For example, a concrete implementation β is said to *refine* its abstract specification α if the set of transitions of β is a subset of those of α [BvW98]. Proving such a refinement for hybrid programs α, β would, for example, prove the implication:

$$\langle\beta\rangle P \rightarrow \langle\alpha\rangle P \tag{23}$$

Program refinement is not directly applicable to this article's focus on proving liveness for specific ODEs. Instead, as hinted by (23), program refinement plays an important role for generalizing this article's results beyond ODEs to hybrid systems, where, e.g., one may use implications like (23) as part of a refinement chain (6). There are a number of refinement calculi for hybrid systems [LP16, FyMS20, BAB16, RRS03]. Notably, *differential refinement logic* [LP16] formally extends dL with a refinement operator $\beta \leq \alpha$, and can be used together with this article's results. Another direction for generalizing this article's results is to consider larger classes of continuous dynamics, such as differential inclusions, differential-algebraic constraints [Pla10], and differential games [Pla17b]. These open up the possibility of proving refinements between concrete (ODE) descriptions and their more abstract continuous counterparts [Pla10, FyMS20, DAPS19, Pla17b].

9. Conclusion

This article presents a refinement-based approach for proving liveness and, as a special case, global existence properties for ODEs in dL. The associated KeYmaera X implementation demonstrates the utility of this approach for formally proving concrete ODE liveness questions. Beyond the particular proof rules derived in the article, the exploration of new and more general ODE liveness proof rules is enabled by simply piecing together more refinement steps in dL, or in the KeYmaera X implementation of those steps. Given its wide applicability and correctness guarantees, this approach is a suitable framework for justifying ODE liveness arguments, even for readers less interested in the logical aspects.

Acknowledgements

The authors thank the guest editors for handling this article and the anonymous reviewers for their insightful comments and feedback. The authors also thank members of the Logical Systems Lab at Carnegie Mellon University for their feedback on the KeYmaera X implementation, and Katherine Cordwell, Frank Pfenning, Andrew Sogokon, and the FM'19 anonymous reviewers for their feedback on the earlier conference version. This material is based upon work supported by the Alexander von Humboldt Foundation and the AFOSR under grant number FA9550-16-1-0288. The first author was also supported by A*STAR, Singapore.

A. Proof calculus

This appendix presents the dL proof calculus that underlies the refinement approach of this article. For ease of reference, all of the core axioms and proof rules presented in the main article are summarized here, along with their proofs (where necessary).

A.1. Base calculus

The following lemma summarizes the base dL axioms and proof rules used in this article. Lemma 28 subsumes Lemma 1 with the addition of the differential ghost axiom (DG from Sect. 2.3) and three axioms ($[\cdot]\wedge$, DMP, DX). The latter three additions are used in derivations in Appendix B.

Lemma 28 (Axioms and proof rules of dL [Pla17a, Pla18, PT20]). *The following are sound axioms and proof rules of* dL*. In axiom* DG*, the* $\exists$ *quantifier can be replaced with a* $\forall$ *quantifier.*

$\langle\cdot\rangle$ $\langle\alpha\rangle P \leftrightarrow \neg[\alpha]\neg P$ K $[\alpha](R \rightarrow P) \rightarrow ([\alpha]R \rightarrow [\alpha]P)$

$$\text{dI}_{\succcurlyeq}\ \frac{Q \vdash \dot{p} \geq \dot{q}}{\Gamma, p \succcurlyeq q \vdash [x' = f(x) \,\&\, Q] p \succcurlyeq q} \quad \text{(where } \succcurlyeq \text{ is either } \geq \text{ or } >\text{)}$$

$$\text{dC}\ \frac{\Gamma \vdash [x' = f(x) \,\&\, Q]C \quad \Gamma \vdash [x' = f(x) \,\&\, Q \wedge C]P}{\Gamma \vdash [x' = f(x) \,\&\, Q]P} \qquad \text{dW}\ \frac{Q \vdash P}{\Gamma \vdash [x' = f(x) \,\&\, Q]P}$$

$$\text{M}[']\ \frac{Q, R \vdash P \quad \Gamma \vdash [x' = f(x) \,\&\, Q]R}{\Gamma \vdash [x' = f(x) \,\&\, Q]P} \qquad \text{M}\langle'\rangle\ \frac{Q, R \vdash P \quad \Gamma \vdash \langle x' = f(x) \,\&\, Q\rangle R}{\Gamma \vdash \langle x' = f(x) \,\&\, Q\rangle P}$$

$$\text{DG}\ \ [x' = f(x) \,\&\, Q(x)]P(x) \leftrightarrow \exists y\, [x' = f(x), y' = a(x)y + b(x) \,\&\, Q(x)]P(x)$$

$$[\cdot]\wedge\ \ [\alpha](P \wedge R) \leftrightarrow [\alpha]P \wedge [\alpha]R$$

$$\text{DMP}\ \ [x' = f(x) \,\&\, Q](Q \rightarrow R) \rightarrow ([x' = f(x) \,\&\, R]P \rightarrow [x' = f(x) \,\&\, Q]P)$$

$$\text{DX}\ \ [x' = f(x) \,\&\, Q]P \leftrightarrow (Q \rightarrow P \wedge [x' = f(x) \,\&\, Q]P) \quad (x' \notin P, Q)$$

Proof of Lemma 28 (implies Lemma 1). The soundness of all axioms and proof rules in Lemma 28 are proved elsewhere [Pla17a, Pla18, PT20]. □

Axiom $[\cdot]\wedge$ is derived from axiom K [Pla17a, Pla18]. It commutes box modalities and their conjunctive postconditions because the conjunction $P \wedge R$ is true after all runs of hybrid program α iff the individual conjuncts P, R are themselves true after all runs of α. Axiom DMP is the modus ponens principle for domain constraints. The *differential skip* axiom DX is a reflexivity property of differential equation solutions. The "←" direction says if domain constraint Q is initially false, then the formula $[x' = f(x) \,\&\, Q]P$ is trivially true in that initial state because no solution of the ODE stays in the domain constraint. Thus, this direction of DX allows domain constraint Q to be assumed true initially when proving $[x' = f(x) \,\&\, Q]P$ (shown below, on the left). The "→" direction has the following equivalent contrapositive reading using $\langle\cdot\rangle$ and propositional simplification: $Q \wedge P \rightarrow \langle x' = f(x) \,\&\, Q\rangle P$, i.e., if the domain constraint Q and postcondition P were both true initially, then $\langle x' = f(x) \,\&\, Q\rangle P$ is true because of the trivial solution of duration zero. When proving the liveness property $\langle x' = f(x) \,\&\, Q\rangle P$, one can therefore always additionally assume $\neg(Q \wedge P)$ because, by DX, there is nothing to prove otherwise (shown below, on the right).

$$\text{DX}\frac{\Gamma, Q \vdash [x' = f(x) \,\&\, Q]P}{\Gamma \vdash [x' = f(x) \,\&\, Q]P} \qquad \text{DX}\frac{\Gamma, \neg(Q \wedge P) \vdash \langle x' = f(x) \,\&\, Q\rangle P}{\Gamma \vdash \langle x' = f(x) \,\&\, Q\rangle P}$$

Rule dGt from Sect. 4 is useful for adding a fresh time variable t in ODE existence and liveness proofs. Its derivation is shown below, using axiom $\langle\cdot\rangle$ to switch between the box and diamond modalities and axiom DG to introduce a universally quantified time variable t which is then instantiated by $\forall$L to $t = 0$.

$$\text{dGt}\ \frac{\Gamma, t = 0 \vdash \langle x' = f(x), t' = 1 \,\&\, Q\rangle P}{\Gamma \vdash \langle x' = f(x) \,\&\, Q\rangle P} \qquad \begin{array}{lr} & \Gamma, t{=}0 \vdash \langle x' = f(x), t' = 1 \,\&\, Q\rangle P \\ \cline{2-2} \langle\cdot\rangle,\, \neg\text{L} & \Gamma, t{=}0, [x' = f(x), t' = 1 \,\&\, Q]\neg P \vdash \mathit{false} \\ \cline{2-2} \forall\text{L} & \Gamma, \forall t\, [x' = f(x), t' = 1 \,\&\, Q]\neg P \vdash \mathit{false} \\ \cline{2-2} \text{DG} & \Gamma, [x' = f(x) \,\&\, Q]\neg P \vdash \mathit{false} \\ \cline{2-2} \langle\cdot\rangle,\, \neg\text{R} & \Gamma \vdash \langle x' = f(x) \,\&\, Q\rangle P \end{array}$$

The bounded differential ghost axiom BDG from Lemma 2 (quoted and proved below) is a new vectorial generalization of DG which allows differential ghosts with provably bounded ODEs to be added.

$$\text{BDG}\quad \begin{array}{l} [x' = f(x), y' = g(x,y) \,\&\, Q(x)]\, \|y\|^2 \le p(x) \\ \quad \to \big([x' = f(x) \,\&\, Q(x)]P(x) \leftrightarrow [x' = f(x), y' = g(x,y) \,\&\, Q(x)]P(x)\big) \end{array}$$

Proof of Lemma 2. The proof of BDG is similar to that for the differential ghosts axiom [Pla17a], but generalizes it to support vectorial, nonlinear ODEs by adding a precondition on boundedness of solutions. Let y be a vector of m fresh variables and $y' = g(x, y)$ be its corresponding vector of ghost ODEs. Both directions of the (inner) equivalence of axiom BDG are proved separately.

"$\to$" The (easier) "$\to$" direction does not require the outer bounding assumption of BDG, i.e., the implication $[x' = f(x) \,\&\, Q(x)]P(x) \to [x' = f(x), y' = g(x, y) \,\&\, Q(x)]P(x)$ is valid for any ODE $y' = g(x, y)$ meeting the freshness condition on y. The proof for this direction is identical to the proof of soundness for differential ghosts [Pla17a, Theorem 38].

"$\leftarrow$" In the "$\leftarrow$" direction, consider an initial state $\omega \in \mathbb{S}$ and let $\boldsymbol{\varphi} : [0, T) \to \mathbb{S}, 0 < T \le \infty$ be the unique, right-maximal solution [Chi06, Wal98] to the ODE $x' = f(x)$ with initial value $\boldsymbol{\varphi}(0) = \omega$. Similarly, let $\boldsymbol{\varphi}_y : [0, T_y) \to \mathbb{S}, 0 < T_y \le \infty$ be the unique, right-maximal solution to the ODE $x' = f(x), y' = g(x, y)$ with initial value $\boldsymbol{\varphi}_y(0) = \omega$. Assume that ω satisfies both of the following assumptions in BDG:

$$\omega \in [\![[x' = f(x), y' = g(x, y) \,\&\, Q(x)]\, \|y\|^2 \le p(x)]\!] \tag{24}$$

$$\omega \in [\![[x' = f(x), y' = g(x, y) \,\&\, Q(x)]P(x)]\!] \tag{25}$$

To show $\omega \in [\![[x' = f(x) \,\&\, Q(x)]P(x)]\!]$, unfold the semantics of the box modality and consider any finite time τ with $0 \le \tau < T$ where $\boldsymbol{\varphi}(\zeta) \in [\![Q(x)]\!]$ for all $0 \le \zeta \le \tau$. It is proved further below that τ is also in the existence interval for solution $\boldsymbol{\varphi}_y$, i.e., $\circledast$: $\tau < T_y$. By uniqueness, $\boldsymbol{\varphi}, \boldsymbol{\varphi}_y$ agree on the values of x on their common existence interval, which includes the time interval $[0, \tau]$ by $\circledast$. Therefore, by coincidence for terms and formulas [Pla17a], $\boldsymbol{\varphi}_y(\zeta) \in [\![Q(x)]\!]$ for all $0 \le \zeta \le \tau$. Thus, by (25), $\boldsymbol{\varphi}_y(\tau) \in [\![P(x)]\!]$ and by coincidence for formulas [Pla17a], $\boldsymbol{\varphi}(\tau) \in [\![P(x)]\!]$.

In order to prove $\circledast$, suppose for contradiction that $T_y \le \tau$. Let $x(\cdot) : [0, T) \to \mathbb{R}^n$ denote the projection of solution $\boldsymbol{\varphi}$ onto its x coordinates, and let $p(x(\cdot)) : [0, T) \to \mathbb{R}$ denote the evaluation of term p along $x(\cdot)$. Since the projection $x(\cdot)$ and its composition with a polynomial evaluation function $p(x(\cdot))$ are continuous in t [Pla17a], $p(x(\cdot))$ is bounded above by (and attains) its maximum value $p_{\max} \in \mathbb{R}$ on the compact interval $[0, \tau]$.

Let $y(\cdot) : [0, T_y) \to \mathbb{R}^m$ similarly denote the projection of $\boldsymbol{\varphi}_y$ onto its y coordinates and $\|y(\cdot)\|^2$ denote the squared norm evaluated along $y(\cdot)$. Since $T_y \le \tau < T$, note that $y(\cdot)$ must be the unique right-maximal solution of the time-dependent differential equation $y' = g(x(t), y)$. Otherwise, if there is a longer solution $\psi : [0, \zeta) \to \mathbb{R}^m$ for $y' = g(x(t), y)$ which exists for time ζ with $T_y < \zeta \le T$, then the combined solution given by $(x(t), \psi(t)) : [0, \zeta) \to \mathbb{R}^n \times \mathbb{R}^m$ extends $\boldsymbol{\varphi}_y$ beyond T_y (by keeping all variables other than x, y constant at their initial values in state ω). This contradicts right-maximality of $\boldsymbol{\varphi}_y$. Moreover, for all times $0 \le \zeta < T_y$, by assumption $\zeta \le \tau$ and $\boldsymbol{\varphi}(\zeta) \in [\![Q(x)]\!]$, so the solution $\boldsymbol{\varphi}_y$ satisfies $\boldsymbol{\varphi}_y(\zeta) \in [\![Q(x)]\!]$ by coincidence for formulas [Pla17a]. Thus, from (24), for all times $0 \le \zeta < T_y$, the squared norm is bounded by $p_{\max}$, with:

$$\|y(\zeta)\|^2 \le p(x(\zeta)) \le p_{\max}$$

Hence, $y(\cdot)$ remains trapped within the compact $\mathbb{R}^m$ ball of radius $\sqrt{p_{\max}}$ on its domain of definition $[0, T_y)$. By [Chi06, Theorem 1.4], and right-maximality of $y(\cdot)$ for the time-dependent ODE $y' = g(x(t), y)$, the domain of definition of solution $y(\cdot)$ is equal to the domain of definition of $y' = g(x(t), y)$, i.e., $T_y = T$, which contradicts $T_y \le \tau < T$. □

The following lemma presents additional dL ODE invariance proof rules that are used in the derivations in Appendix B. These invariance proof rules are not the main focus of this article but they are nevertheless useful for simplifying or deriving the premises of this article's ODE existence and liveness proof rules.

Lemma 29 (ODE invariance proof rules of dL [PT20]). *The following are derived ODE invariance proof rules of* dL*. In rule* $\text{dbx}_{\succcurlyeq}$*, g is any polynomial cofactor term. In rule* sAI&*, $\dot{Q}^{(*)}$, $\dot{P}^{(*)}$, $\dot{Q}^{-(*)}$, $(\dot{\neg P})^{-(*)}$ are semialgebraic progress formulas* [PT20, Def. 6.4] *with respect to $x' = f(x)$. In rule* Enc*, formula P is formed from finite conjunctions and disjunctions of strict inequalities $>, <$, and formula $P^{\geq}_{>}$ is identical to P but with non-strict inequalities $\geq, \leq$ in place of $>, <$ respectively.*

$$\text{dbx}_{\succcurlyeq}\ \frac{Q \vdash \dot{p} \geq gp}{p \succcurlyeq 0 \vdash [x' = f(x) \,\&\, Q]p \succcurlyeq 0} \quad \text{(where $\succcurlyeq$ is either $\geq$ or $>$)}$$

$$\text{sAI\&}\ \frac{P, Q, \dot{Q}^{(*)} \vdash \dot{P}^{(*)} \qquad \neg P, Q, \dot{Q}^{-(*)} \vdash (\dot{\neg P})^{-(*)}}{P \vdash [x' = f(x) \,\&\, Q]P}$$

$$\text{Barr}\ \frac{Q, p = 0 \vdash \dot{p} > 0}{\Gamma, p \succcurlyeq 0 \vdash [x' = f(x) \,\&\, Q]p \succcurlyeq 0} \quad \text{(where $\succcurlyeq$ is either $\geq$ or $>$)}$$

$$\text{Enc}\ \frac{\Gamma \vdash P^{\geq}_{>} \qquad \Gamma \vdash [x' = f(x) \,\&\, Q \wedge P^{\geq}_{>}]P}{\Gamma \vdash [x' = f(x) \,\&\, Q]P}$$

Proof. These ODE invariance proof rules are all derived from the complete dL axiomatization for ODE invariants [PT20]. □

Rule $\text{dbx}_{\succcurlyeq}$ is the Darboux inequality proof rule for the invariance of $p \succcurlyeq 0$ which is derived using rules $\text{dI}_{\succcurlyeq}$, dC, DG. An extensive explanation of the rule is available elsewhere [PT20, Section 3.2]. Rule sAI& is dL's complete proof rule for ODE invariants, i.e., the formula P is invariant for ODE $x' = f(x) \,\&\, Q$ iff it can be proved invariant by rule sAI&. For closed (resp. open) semialgebraic formulas P, the right (resp. left) premise of rule sAI& closes trivially [PT20]. This simplification is useful for obtaining more succinct proof rules, e.g., rule dV makes use of sAI& with a closed semialgebraic formula. Rule Barr is a dL rendition of the strict barrier certificates proof rule [DFPP18, PJP07] for invariance of $p \succcurlyeq 0$, which is derived as a special case of rule sAI&. Intuitively, the premise says that $p = 0$ is a *barrier* along which the value of p is increasing along solutions (succedent $\dot{p} > 0$), so it is impossible for solutions starting from $p \succcurlyeq 0$ to cross this barrier into $p \preccurlyeq 0$. Finally, rule Enc says that, in order to prove that solutions stay in postcondition P which characterizes an open set, it suffices to prove it assuming $P^{\geq}_{>}$ in the domain constraint, where $P^{\geq}_{>}$ relaxes all strict inequalities in P and thus provides an over-approximation of the topological closure of the set characterized by P. The rule can also be understood in the contrapositive: if a continuous solution leaves P, then it either already started outside the closure (ruled out by left premise), or it starts in the closure and leaves P on its topological boundary (included in the closure). The latter case is ruled out by the right premise of Enc because solutions that remain in the closure must stay in P.

A.2. Refinement calculus

The following ODE liveness refinement axioms are quoted from Lemma 3, and their syntactic derivations in the dL proof calculus are given below.

$$\text{K}\langle\&\rangle \quad [x' = f(x) \,\&\, Q \wedge \neg P]\neg G \rightarrow \big(\langle x' = f(x) \,\&\, Q\rangle G \rightarrow \langle x' = f(x) \,\&\, Q\rangle P\big)$$

$$\text{DR}\langle\cdot\rangle \quad [x' = f(x) \,\&\, R]Q \rightarrow \big(\langle x' = f(x) \,\&\, R\rangle P \rightarrow \langle x' = f(x) \,\&\, Q\rangle P\big)$$

$$\begin{aligned}\text{BDG}\langle\cdot\rangle \quad & [x' = f(x), y' = g(x,y) \,\&\, Q(x)]\, \|y\|^2 \leq p(x) \\ & \rightarrow \big(\langle x' = f(x) \,\&\, Q(x)\rangle P(x) \rightarrow \langle x' = f(x), y' = g(x,y) \,\&\, Q(x)\rangle P(x)\big)\end{aligned}$$

$$\begin{aligned}\text{DDG}\langle\cdot\rangle \quad & [x' = f(x), y' = g(x,y) \,\&\, Q(x)]\, 2y \cdot g(x,y) \leq L(x)\|y\|^2 + M(x) \\ & \rightarrow \big(\langle x' = f(x) \,\&\, Q(x)\rangle P(x) \rightarrow \langle x' = f(x), y' = g(x,y) \,\&\, Q(x)\rangle P(x)\big)\end{aligned}$$

Proof of Lemma 3. The four axioms are derived in order.

K⟨&⟩ Axiom K⟨&⟩ is derived as follows, starting with ⟨·⟩, ¬L, ¬R to dualize the diamond modalities in the antecedent and succedent to box modalities. A dC step using the right antecedent completes the proof.

$$\text{⟨·⟩, ¬L, ¬R}\;\dfrac{\text{dC}\;\dfrac{*}{[x' = f(x)\,\&\,Q \land \neg P]\neg G, [x' = f(x)\,\&\,Q]\neg P \vdash [x' = f(x)\,\&\,Q]\neg G}}{[x' = f(x)\,\&\,Q \land \neg P]\neg G, \langle x' = f(x)\,\&\,Q\rangle G \vdash \langle x' = f(x)\,\&\,Q\rangle P}$$

DR⟨·⟩ Axiom DR⟨·⟩ is similarly derived from axiom DMP with ⟨·⟩ [PT20].

BDG⟨·⟩ Axiom BDG⟨·⟩ is derived from axiom BDG after using axiom ⟨·⟩ to dualize diamond modalities to box modalities. The leftmost antecedent is abbreviated $R \equiv [x' = f(x), y' = g(x,y)\,\&\,Q(x)]\, \|y\|^2 \leq p(x)$.

$$\text{⟨·⟩, ¬L, ¬R}\;\dfrac{\text{BDG}\;\dfrac{*}{R, [x' = f(x), y' = g(x,y)\,\&\,Q(x)]\neg P(x) \vdash [x' = f(x)\,\&\,Q(x)]\neg P(x)}}{R, \langle x' = f(x)\,\&\,Q(x)\rangle P(x) \vdash \langle x' = f(x), y' = g(x,y)\,\&\,Q(x)\rangle P(x)}$$

DDG⟨·⟩ Axiom DDG⟨·⟩ is derived as a differential version of axiom BDG⟨·⟩ with the aid of DG. The derivation starts with ⟨·⟩, ¬L, ¬R to turn diamond modalities in the sequent to box modalities. Axiom DG then introduces a fresh ghost ODE $z' = L(x)z + M(x)$, where the antecedents are universally quantified over ghost variable z by DG, while the succedent is existentially quantified. All quantifiers are then instantiated using ∀L, ∃R, with $z = \|y\|^2$ so that z stores the initial value of the squared norm of y. Axiom BDG is used with $y' = g(x,y)$ as the ghost ODEs and with $p(x,z) = z$. The antecedents are abbreviated:

$$\begin{aligned}
R &\equiv [x' = f(x), y' = g(x,y)\,\&\,Q(x)]\, 2y \cdot g(x,y) \leq L(x)\|y\|^2 + M(x)\\
R_z &\equiv [x' = f(x), y' = g(x,y), z' = L(x)z + M(x)\,\&\,Q(x)]\, 2y \cdot g(x,y) \leq L(x)\|y\|^2 + M(x)\\
S &\equiv [x' = f(x), y' = g(x,y)\,\&\,Q(x)]\neg P(x)\\
S_z &\equiv [x' = f(x), y' = g(x,y), z' = L(x)z + M(x)\,\&\,Q(x)]\neg P(x)
\end{aligned}$$

$$\text{⟨·⟩, ¬L, ¬R}\;\dfrac{\text{DG}\;\dfrac{\forall\text{L}, \exists\text{R}\;\dfrac{\text{BDG}\;\dfrac{z = \|y\|^2, R_z \vdash [x' = f(x), y' = g(x,y), z' = L(x)z + M(x)\,\&\,Q(x)]\|y\|^2 \leq z}{z = \|y\|^2, R_z, S_z \vdash [x' = f(x), z' = L(x)z + M(x)\,\&\,Q(x)]\neg P(x)}}{\forall z\, R_z, \forall z\, S_z \vdash \exists z\, [x' = f(x), z' = L(x)z + M(x)\,\&\,Q(x)]\neg P(x)}}{R, S \vdash [x' = f(x)\,\&\,Q(x)]\neg P(x)}}{R, \langle x' = f(x)\,\&\,Q(x)\rangle P(x) \vdash \langle x' = f(x), y' = g(x,y)\,\&\,Q(x)\rangle P(x)}$$

From the resulting open premise, a dC step adds the postcondition of R_z to the domain constraint of the succedent, while M['] rearranges the postcondition into the form expected by rule $\text{dbx}_{\succcurlyeq}$. The proof is completed using $\text{dbx}_{\succcurlyeq}$ with cofactor $g = L(x)$. Its resulting arithmetical premise is proved by $\mathbb{R}$ because the Lie derivative of $z - \|y\|^2$ is bounded above by the following calculation, where the inequality from the domain constraint is used in the second step.

$$\begin{aligned}
\mathcal{L}_{x'=f(x), y'=g(x,y), z'=L(x)z+M(x)}(z - \|y\|^2) &= L(x)z + M(x) - 2y \cdot g(x,y)\\
&\geq L(x)z + M(x) - (L(x)\|y\|^2 + M(x))\\
&= L(x)(z - \|y\|^2)
\end{aligned}$$

The ODEs $x' = f(x), y' = g(x,y), z' = L(x)z + M(x)$ are abbreviated … in the derivation below.

$$\text{dC}\;\dfrac{\text{M[′]}\;\dfrac{\text{dbx}_{\succcurlyeq}\;\dfrac{\mathbb{R}\;\dfrac{*}{2y \cdot g(x,y) \leq L(x)\|y\|^2 + M(x) \vdash L(x)z + M(x) - 2y \cdot g(x,y) \geq L(x)(z - \|y\|^2)}}{z = \|y\|^2 \vdash [\ldots\,\&\,Q(x) \land 2y \cdot g(x,y) \leq L(x)\|y\|^2 + M(x)]\, z - \|y\|^2 \geq 0}}{z = \|y\|^2 \vdash [\ldots\,\&\,Q(x) \land 2y \cdot g(x,y) \leq L(x)\|y\|^2 + M(x)]\, \|y\|^2 \leq z}}{z = \|y\|^2, R_z \vdash [\ldots\,\&\,Q(x)]\, \|y\|^2 \leq z}$$ □

The following topological ⟨·⟩ ODE refinement axioms are quoted from Lemmas 4 and 26. The topological side conditions for these axioms are listed in Lemmas 4 and 26 respectively. For semialgebraic postcondition P and domain constraints Q, R, these refinement axioms are derived syntactically from dL's real induction axiom [PT20, Lemma A.2]. For the sake of generality, the proofs below directly use the topological conditions.

$$\text{COR}\quad \neg P \land [x' = f(x) \,\&\, R \land \neg P]Q \rightarrow \big(\langle x' = f(x) \,\&\, R\rangle P \rightarrow \langle x' = f(x) \,\&\, Q\rangle P\big)$$

$$\text{CR}\quad \neg P \land [x' = f(x) \,\&\, R \land \neg P]\mathring{Q} \rightarrow \big(\langle x' = f(x) \,\&\, R\rangle P \rightarrow \langle x' = f(x) \,\&\, Q\rangle P\big)$$

$$\text{SAR}\quad [x' = f(x) \,\&\, R \land \neg(P \land Q)]Q \rightarrow \big(\langle x' = f(x) \,\&\, R\rangle P \rightarrow \langle x' = f(x) \,\&\, Q\rangle P\big)$$

Proof of Lemmas 4 and 26. Let $\omega \in \mathbb{S}$ and $\boldsymbol{\varphi} : [0, T) \rightarrow \mathbb{S}, 0 < T \leq \infty$ be the unique, right-maximal solution [Chi06, Wal98] to the ODE $x' = f(x)$ with initial value $\boldsymbol{\varphi}(0) = \omega$. By definition, $\boldsymbol{\varphi}$ is differentiable, and therefore continuous. This proof uses the fact that preimages under continuous functions of open sets are open [Rud76, Theorem 4.8]. In particular, for an open set $\mathcal{O}$, if $\boldsymbol{\varphi}(t) \in \mathcal{O}$ at some time $0 < t < T$ then the preimage of a sufficiently small open ball $\mathcal{O}_\varepsilon \subseteq \mathcal{O}$ centered at $\boldsymbol{\varphi}(t)$ is open. Thus, if $t > 0$ and $\boldsymbol{\varphi}(t) \in \mathcal{O}$, then $\boldsymbol{\varphi}$ stays in the open set $\mathcal{O}$ for some open time interval[12]around t, i.e., for some $\varepsilon > 0$:

$$\boldsymbol{\varphi}(\zeta) \in \mathcal{O} \text{ for all } t - \varepsilon \leq \zeta \leq t + \varepsilon \tag{26}$$

For the soundness proof of axioms COR, CR, and SAR, assume that $\omega \in [\![\langle x' = f(x) \,\&\, R\rangle P]\!]$, i.e., there is a time $\tau \in [0, T)$ such that $\boldsymbol{\varphi}(\tau) \in [\![P]\!]$ and $\boldsymbol{\varphi}(\zeta) \in [\![R]\!]$ for all $0 \leq \zeta \leq \tau$. The proofs make use of the following set $\mathbb{T}$ containing all times t such that the solution $\boldsymbol{\varphi}$ never enters P on the time interval $[0, t]$.

$$\mathbb{T} \equiv \{t \mid \boldsymbol{\varphi}(\zeta) \notin [\![P]\!] \text{ for all } 0 \leq \zeta \leq t\} \tag{27}$$

COR For axiom COR, assume that $\omega \in [\![\neg P \land [x' = f(x) \,\&\, R \land \neg P]Q]\!]$. The set of times $\mathbb{T}$ (27) is non-empty since $\omega = \boldsymbol{\varphi}(0) \notin [\![P]\!]$ so it has a supremum t with $0 \leq t \leq \tau$ and $\boldsymbol{\varphi}(\zeta) \notin [\![P]\!]$ for all $0 \leq \zeta < t$.

- Suppose P, Q both characterize topologically closed sets. Since P characterizes a topologically closed set, its complement formula $\neg P$ characterizes a topologically open set. If $\boldsymbol{\varphi}(t) \notin [\![P]\!]$, i.e., $\boldsymbol{\varphi}(t) \in [\![\neg P]\!]$, then $t < \tau$ and by (26), the solution stays in $\neg P$ until time $t + \varepsilon$ for some $\varepsilon > 0$, so t is not the supremum of $\mathbb{T}$, which is a contradiction. Thus, $\boldsymbol{\varphi}(t) \in [\![P]\!]$ and $0 < t$ because $\boldsymbol{\varphi}(0) \notin [\![P]\!]$. Hence, $\boldsymbol{\varphi}(\zeta) \in [\![R \land \neg P]\!]$ for all $0 \leq \zeta < t$, which, together with the assumption $\omega \in [\![[x' = f(x) \,\&\, R \land \neg P]Q]\!]$ implies $\boldsymbol{\varphi}(\zeta) \in [\![Q]\!]$ for all $0 \leq \zeta < t$. Since Q characterizes a topologically closed set, this implies $\boldsymbol{\varphi}(t) \in [\![Q]\!]$; otherwise, $\boldsymbol{\varphi}(t) \in [\![\neg Q]\!]$ and $\neg Q$ characterizes an open set, so (26) implies $\boldsymbol{\varphi}(\zeta) \in [\![\neg Q]\!]$ for some $0 \leq \zeta < t$, which contradicts the earlier observation that $\boldsymbol{\varphi}(\zeta) \in [\![Q]\!]$ for all $0 \leq \zeta < t$. Thus, $\omega \in [\![\langle x' = f(x) \,\&\, Q\rangle P]\!]$ because $\boldsymbol{\varphi}(t) \in [\![P]\!]$ and $\boldsymbol{\varphi}(\zeta) \in [\![Q]\!]$ for all $0 \leq \zeta \leq t$.
- Suppose P, Q both characterize topologically open sets. Then, $\boldsymbol{\varphi}(t) \notin [\![P]\!]$; otherwise, $\boldsymbol{\varphi}(t) \in [\![P]\!]$ and since P characterizes an open set, by (26), there is a time $0 \leq \zeta < t$ where $\boldsymbol{\varphi}(\zeta) \in [\![P]\!]$, which contradicts t being the supremum of $\mathbb{T}$. Note that $t < \tau$ and $\boldsymbol{\varphi}(\zeta) \in [\![R \land \neg P]\!]$ for all $0 \leq \zeta \leq t$, which, together with the assumption $\omega \in [\![[x' = f(x) \,\&\, R \land \neg P]Q]\!]$ implies $\boldsymbol{\varphi}(\zeta) \in [\![Q]\!]$ for all $0 \leq \zeta \leq t$. Since Q characterizes a topologically open set, by (26), there exists $\varepsilon > 0$ where $t + \varepsilon < \tau$ such that $\boldsymbol{\varphi}(t + \zeta) \in [\![Q]\!]$ for all $0 \leq \zeta \leq \varepsilon$. By definition of the supremum, for every such $\varepsilon > 0$, there exists ζ where $0 < \zeta \leq \varepsilon$ and $\boldsymbol{\varphi}(t + \zeta) \in [\![P]\!]$, which yields the desired conclusion.

CR For axiom CR, assume that $\omega \in [\![\neg P]\!]$ and

$$\omega \in [\![[x' = f(x) \,\&\, R \land \neg P]\mathring{Q}]\!] \tag{28}$$

The set of times $\mathbb{T}$ (27) is non-empty since $\omega = \boldsymbol{\varphi}(0) \notin [\![P]\!]$ so it has a supremum t with $0 \leq t \leq \tau$ and $\boldsymbol{\varphi}(\zeta) \notin [\![P]\!]$ for all $0 \leq \zeta < t$. Furthermore, $\boldsymbol{\varphi}(\zeta) \in [\![R \land \neg P]\!]$ for all $0 \leq \zeta < t$, so by (28), $\boldsymbol{\varphi}(\zeta) \in [\![\mathring{Q}]\!]$ for all $0 \leq \zeta < t$. By assumption, formula $\mathring{Q}$ characterizes the open topological interior of the closed formula Q so by continuity of $\boldsymbol{\varphi}$, $\boldsymbol{\varphi}(t) \in [\![Q]\!]$. Furthermore, the interior of a set is contained in the set itself, i.e., $[\![\mathring{Q}]\!] \subseteq [\![Q]\!]$, so $\boldsymbol{\varphi}(\zeta) \in [\![Q]\!]$ for all $0 \leq \zeta \leq t$. Classically, either $\boldsymbol{\varphi}(t) \in [\![P]\!]$ or $\boldsymbol{\varphi}(t) \notin [\![P]\!]$.

- If $\boldsymbol{\varphi}(t) \in [\![P]\!]$, then since $\boldsymbol{\varphi}(\zeta) \in [\![Q]\!]$ for all $0 \leq \zeta \leq t$, by definition, $\omega \in [\![\langle x' = f(x) \,\&\, Q\rangle P]\!]$.
- If $\boldsymbol{\varphi}(t) \notin [\![P]\!]$, then $t < \tau$ and furthermore, by (28), $\boldsymbol{\varphi}(t) \in [\![\mathring{Q}]\!]$. Since the interior is topologically open, by (26), there exists $\varepsilon > 0$ where $t + \varepsilon < \tau$ such that $\boldsymbol{\varphi}(t + \zeta) \in [\![\mathring{Q}]\!] \subseteq [\![Q]\!]$ for all $0 \leq \zeta \leq \varepsilon$. By definition of the supremum, for every such $\varepsilon > 0$, there exists ζ where $0 < \zeta \leq \varepsilon$ and $\boldsymbol{\varphi}(t + \zeta) \in [\![P]\!]$, which yields the desired conclusion.

[12] In case $t = 0$, the time interval in (26) is truncated to the left with $\boldsymbol{\varphi}(\zeta) \in \mathcal{O}$ for all $0 \leq \zeta < t + \varepsilon$.

SAR For axiom SAR, assume that

$$\omega \in \llbracket [x' = f(x) \,\&\, R \wedge \neg(P \wedge Q)]Q \rrbracket \tag{29}$$

If $\omega \in \llbracket P \wedge Q \rrbracket$, then $\omega \in \langle x' = f(x) \,\&\, Q \rangle P$ trivially by following the solution $\boldsymbol{\varphi}$ for duration 0. Thus, assume $\omega \notin \llbracket P \wedge Q \rrbracket$. From (29), $\omega \in \llbracket Q \rrbracket$ which further implies $\omega \notin \llbracket P \rrbracket$. The set of times $\mathbb{T}$ (27) is non-empty since $\omega = \boldsymbol{\varphi}(0) \notin \llbracket P \rrbracket$ and has a supremum t with $0 \leq t \leq \tau$ and $\boldsymbol{\varphi}(\zeta) \notin \llbracket P \rrbracket$ for all $0 \leq \zeta < t$. Thus, $\boldsymbol{\varphi}(\zeta) \in \llbracket R \wedge \neg(P \wedge Q) \rrbracket$ for all $0 \leq \zeta < t$. By (29), $\boldsymbol{\varphi}(\zeta) \in \llbracket Q \rrbracket$ for all $0 \leq \zeta < t$. Classically, either $\boldsymbol{\varphi}(t) \in \llbracket P \rrbracket$ or $\boldsymbol{\varphi}(t) \notin \llbracket P \rrbracket$.

- Suppose $\boldsymbol{\varphi}(t) \in \llbracket P \rrbracket$, if $\boldsymbol{\varphi}(t) \in \llbracket Q \rrbracket$, then $\boldsymbol{\varphi}(\zeta) \in \llbracket Q \rrbracket$ for all $0 \leq \zeta \leq t$ and so, by definition, $\omega \in \llbracket \langle x' = f(x) \,\&\, Q \rangle P \rrbracket$. On the other hand, if $\boldsymbol{\varphi}(t) \notin \llbracket Q \rrbracket$, then $\boldsymbol{\varphi}(\zeta) \in \llbracket R \wedge \neg(P \wedge Q) \rrbracket$ for all $0 \leq \zeta \leq t$, so from (29), $\boldsymbol{\varphi}(t) \in \llbracket Q \rrbracket$, which yields a contradiction.
  If the formula P is further assumed to characterize a closed set, this sub-case (with $\boldsymbol{\varphi}(t) \in \llbracket P \rrbracket$) is the only possibility. Otherwise, $\boldsymbol{\varphi}(t) \in \llbracket \neg P \rrbracket$ and $\neg P$ characterizes an open set, so by (26), for some $\varepsilon > 0$, $\boldsymbol{\varphi}(t + \zeta) \in \llbracket \neg P \rrbracket$ for all $0 \leq \zeta < \varepsilon$ which contradicts t being the supremum of $\mathbb{T}$.
- Suppose $\boldsymbol{\varphi}(t) \notin \llbracket P \rrbracket$, then $t < \tau$ and $\boldsymbol{\varphi}(\zeta) \in \llbracket R \wedge \neg(P \wedge Q) \rrbracket$ for all $0 \leq \zeta \leq t$, so from (29), $\boldsymbol{\varphi}(t) \in \llbracket Q \rrbracket$. Since Q is a formula of first-order real arithmetic, solutions of polynomial ODEs either locally progress into the set characterized by Q or $\neg Q$ [PT20, SJ15][13], i.e., there exists $\varepsilon > 0$, where $t + \varepsilon < \tau$, such that either ① $\boldsymbol{\varphi}(t + \zeta) \in \llbracket Q \rrbracket$ for all $0 < \zeta \leq \varepsilon$ or ② $\boldsymbol{\varphi}(t + \zeta) \notin \llbracket Q \rrbracket$ for all $0 < \zeta \leq \varepsilon$. Since t is the supremum of $\mathbb{T}$, by definition, for every such ε there exists ζ where $0 < \zeta \leq \varepsilon$ and $\boldsymbol{\varphi}(t + \zeta) \in \llbracket P \rrbracket$. In case ①, since $\boldsymbol{\varphi}(t+\zeta) \in \llbracket P \rrbracket$ and $\boldsymbol{\varphi}(\nu) \in \llbracket Q \rrbracket$ for all $0 \leq \nu \leq t+\zeta$, then $\omega \in \llbracket \langle x' = f(x) \,\&\, Q \rangle P \rrbracket$. If the formula Q is further assumed to characterize an open set, this sub-case (①) is the only possibility, even if Q is not a formula of first-order real arithmetic, because $\boldsymbol{\varphi}(t) \in \llbracket Q \rrbracket$ implies $\boldsymbol{\varphi}$ continues to satisfy Q for some time interval to the right of t by (26). In case ②, observe that $\boldsymbol{\varphi}(\nu) \in \llbracket R \wedge \neg(P \wedge Q) \rrbracket$ for all $0 \leq \nu \leq t + \zeta$, from (29), $\boldsymbol{\varphi}(t + \zeta) \in \llbracket Q \rrbracket$, which yields a contradiction. □

The refinement axioms are pieced together in refinement chains (6) to build ODE existence and liveness proof rules in a step-by-step manner. However, all such refinement chains (6) start from an initial hypothesis $\langle x' = f(x) \,\&\, Q_0 \rangle P_0$ from which the subsequent implications are proved. The time existence axiom TEx from Sect. 4.1 provides the sole initial hypothesis that is needed for the refinement approach of this article.

TEx $\forall \tau \, \langle t' = 1 \rangle t > \tau$

Proof of Lemma 5. Axiom TEx is derived directly from dL's solution axiom [Pla17a]. It also has an easy semantic soundness proof which is given here. Consider an initial state ω and the corresponding modified state ω_τ^d where the value of variable τ is replaced by an arbitrary $d \in \mathbb{R}$. The (right-maximal) solution of ODE $t' = 1$ from state ω_τ^d is given by the function $\boldsymbol{\varphi} : [0, \infty) \to \mathbb{S}$, where $\boldsymbol{\varphi}(\zeta)(t) = \omega_\tau^d(t) + \zeta = \omega(t) + \zeta$, and $\boldsymbol{\varphi}(\zeta)(y) = \omega_\tau^d(y)$ for all other variables y. In particular, $\boldsymbol{\varphi}(\zeta)(\tau) = d$. Thus, at any time $\zeta > d - \omega(t)$, $\boldsymbol{\varphi}(\zeta)(t) = \omega(t) + \zeta > d = \boldsymbol{\varphi}(\zeta)(\tau)$. This time ζ witnesses $\langle t' = 1 \rangle t > \tau$. □

A.3. Topological side conditions

In Sect. 2.2, topological conditions are defined for formulas ϕ that only mention free variables x occurring in an ODE $x' = f(x)$. For example, ϕ is said to characterize an open set with respect to x iff the set $\llbracket \phi \rrbracket$ is open when considered as a subset of $\mathbb{R}^n$ (over variables $x = (x_1, \ldots, x_n)$). This section defines a more general notion, where ϕ is allowed to mention additional free parameters y that do not occur in the ODE. Adopting these (parametric) side conditions makes the topological refinement axioms that use them, like COR, CR, more general. Let $(y_1, \ldots, y_r) = \mathbb{V} \backslash \{x\}$ be parameters, and $\omega \in \mathbb{S}$ be a state. For brevity, write $y = (y_1, \ldots, y_r)$ for the parameters and $\omega(y) = (\omega(y_1), \ldots, \omega(y_r)) \in \mathbb{R}^r$ for the component-wise projection, and similarly for $\omega(x) \in \mathbb{R}^n$. Given the set $\llbracket \phi \rrbracket \subseteq \mathbb{S}$ and $\gamma \in \mathbb{R}^r$, define:

$$\llbracket \phi \rrbracket_\gamma \overset{\text{def}}{=} \{\omega(x) \in \mathbb{R}^n \mid \omega \in \llbracket \phi \rrbracket, \omega(y) = \gamma\}$$

[13] This property is specific to sets characterized by first-order formulas of real arithmetic and polynomial ODEs (and certain topologically well-behaved extensions [PT20]) and is not true for arbitrary sets and ODEs.

The set $[\![\phi]\!]_\gamma \subseteq \mathbb{R}^n$ is the projection onto variables x of all states ω that satisfy ϕ and having values γ for the parameters y. Formula ϕ *characterizes* a (topologically) open (resp. closed, bounded, compact) set with respect to variables x iff for all $\gamma \in \mathbb{R}^r$, the set $[\![\phi]\!]_\gamma \subseteq \mathbb{R}^n$ is topologically open (resp. closed, bounded, compact) with respect to the Euclidean topology.

These topological side conditions are decidable [BCR98] for first-order formulas of real arithmetic P, Q because in Euclidean spaces they can be phrased as conditions using first-order real arithmetic. The following conditions are standard [BCR98], although special care is taken to universally quantify over the parameters y. Let $P(x, y)$ be a formula mentioning variables x and parameters y, then it is (with respect to variables x):

- *open* if the formula $\forall y\, \forall x \left(P(x, y) \to \exists \varepsilon{>}0\, \forall z \left(\|x - z\|^2 < \varepsilon^2 \to P(z, y)\right)\right)$ is valid, where the variables $z = (z_1, \ldots, z_n)$ are fresh for $P(x, y)$,
- *closed* if its complement formula $\neg P(x, y)$ is open,
- *bounded* if the formula $\forall y\, \exists r{>}0\, \forall x \left(P(x, y) \to \|x\|^2{<}r^2\right)$ is valid, where variable r is fresh for $P(x, y)$,
- *compact* if it is closed and bounded, by the Heine-Borel theorem [Rud76, Theorem 2.4.1].

There are syntactic criteria that are sufficient (but not necessary[14]) for checking whether a formula satisfies the semantic conditions. For example, the formula $P(x, y)$ is (with respect to variables x):

- *open* if it is formed from finite conjunctions and disjunctions of strict inequalities ($\neq, >, <$),
- *closed* if it is formed from finite conjunctions and disjunctions of non-strict inequalities ($=, \geq, \leq$),
- *bounded* if it is of the form $\|x\|^2 \preccurlyeq p(y) \wedge R(x, y)$, where $p(y)$ is a term depending only on parameters y and $R(x, y)$ is a formula. This syntactic criterion uses the fact that the intersection of a bounded set (characterized by $\|x\|^2 \preccurlyeq p(y)$) with any set (characterized by $R(x, y)$) is bounded. The formula $P(x, y)$ is also *compact* if $\preccurlyeq$ is $\leq$ and $R(x, y)$ is closed.

These syntactic criteria are easily checkable by an implementation that inspects the syntactic shape of input formulas P. In contrast, checking the semantic topological conditions for P requires invoking expensive real arithmetic decision procedures. For example, such a syntactic side condition enables the effective implementation of rule cR from Corollary 27 compared to its underlying axiom CR from Lemma 26 which is more general but uses requires checking semantic side conditions.

B. Derived existence and liveness proof rules

This appendix syntactically derives all of the existence and liveness proof rules of the main article. These derivations only use the sound dL axioms and proof rules presented in Appendix A. For ease of reference, this appendix is organized into four sections, corresponding to Sects. 4–7 of the main article. The high-level intuition behind these proofs is available as proof sketches in the main article while motivation for important proof steps is given directly in the subsequent proofs. Further motivation for the surveyed liveness arguments can also be found in their original presentations [Pla10, PR05, PR07, RS10, SJ15, TT10].

B.1. Proofs for finite-time blow up and global existence

Proof of Corollary 6. Assume that the ODE $x' = f(x)$ is in dependency order (9). The derivation successively removes the ODEs $y_k, y_{k-1}, \ldots, y_1$ in reverse dependency order using either axiom BDG$\langle\cdot\rangle$ or DDG$\langle\cdot\rangle$, as shown below. This continues until all of the ODEs are removed and the rightmost premise closes by axiom TEx. The left premises arising from refinement with axioms BDG$\langle\cdot\rangle$, DDG$\langle\cdot\rangle$ are the premises of rule DEx. They are collectively labeled $\circledast$ and explained below.

[14] If there are no parameters y, these syntactic checks are "necessary" conditions in the sense that every open (resp. closed) formula P is provably equivalent in real arithmetic to a (computable) formula formed from finite conjunctions and disjunctions of strict (resp. non-strict) inequalities [BCR98, Theorem 2.7.2].

$$\dfrac{\dfrac{\circledast \quad \dfrac{\circledast \quad \dfrac{\circledast \quad \dfrac{*}{\Gamma \vdash \langle t' = 1 \rangle t > \tau}\,\text{TEx}}{\vdots}\,\text{BDG}\langle\cdot\rangle,\ \text{DDG}\langle\cdot\rangle}{\Gamma \vdash \langle y_1' = g_1(y_1), \ldots, y_{k-1}' = g_{k-1}(y_1, \ldots, y_{k-1}), t' = 1 \rangle\, t > \tau}\,\text{BDG}\langle\cdot\rangle,\ \text{DDG}\langle\cdot\rangle}{\Gamma \vdash \langle y_1' = g_1(y_1), \ldots, y_{k-1}' = g_{k-1}(y_1, \ldots, y_{k-1}), y_k' = g_k(y_1, \ldots, y_k), t' = 1 \rangle\, t > \tau}\,\text{BDG}\langle\cdot\rangle,\ \text{DDG}\langle\cdot\rangle}{\Gamma \vdash \forall \tau\, \langle \underbrace{y_1' = g_1(y_1), \ldots, y_{k-1}' = g_{k-1}(y_1, \ldots, y_{k-1}), y_k' = g_k(y_1, \ldots, y_k)}_{x'=f(x) \text{ written in dependency order}}, t' = 1 \rangle\, t > \tau}\,\forall\text{R}$$

At each step i, for $i = k, \ldots, 1$, the ODE y_i in the succeedent is removed using either axiom BDG⟨·⟩ or DDG⟨·⟩, depending on the user-chosen form (Corollary 6) of postcondition P_i.

Ⓑ In case formula $P_i \equiv \|y_i\|^2 \le p_i(t, y_1, \ldots, y_{i-1})$ is of form Ⓑ (as defined in Corollary 6), axiom BDG⟨·⟩ is used. This yields the two stacked premises shown below, where the top premise corresponds to premise ⊛ above. The dependency order (9) enables the sound use of axiom BDG⟨·⟩ for this refinement step because the ODEs for $y_1, \ldots, y_{i-1}$ are not allowed to depend on variables y_i. The term $p(t, y_1, \ldots, y_{i-1})$ also meets the dependency requirements of BDG⟨·⟩ because it does not depend on y_i.

$$\text{BDG}\langle\cdot\rangle\,\dfrac{\begin{array}{l}\Gamma \vdash [y_1' = g_1(y_1), \ldots, y_{i-1}' = g_{i-1}(y_1, \ldots, y_{i-1}), y_i' = g_i(y_1, \ldots, y_i), t' = 1] P_i \\ \Gamma \vdash \langle y_1' = g_1(y_1), \ldots, y_{i-1}' = g_{i-1}(y_1, \ldots, y_{i-1}), t' = 1 \rangle\, t > \tau\end{array}}{\Gamma \vdash \langle y_1' = g_1(y_1), \ldots, y_{i-1}' = g_{i-1}(y_1, \ldots, y_{i-1}), y_i' = g_i(y_1, \ldots, y_i), t' = 1 \rangle\, t > \tau}$$

Ⓓ In case formula $P_i \equiv 2y_i \cdot g_i(y_1, \ldots, y_i) \le L_i(t, y_1, \ldots, y_{i-1})\|y_i\|^2 + M_i(t, y_1, \ldots, y_{i-1})$ is of form Ⓓ (as defined in Corollary 6), axiom DDG⟨·⟩ is used instead. Again, terms $L_i(t, y_1, \ldots, y_{i-1}), M_i(t, y_1, \ldots, y_{i-1})$ meet the dependency requirements of DDG⟨·⟩ because they do not depend on y_i. The top premise corresponds to premise ⊛ above, while the ODE for y_i is removed in the bottom premise.

$$\text{DDG}\langle\cdot\rangle\,\dfrac{\begin{array}{l}\Gamma \vdash [y_1' = g_1(y_1), \ldots, y_{i-1}' = g_{i-1}(y_1, \ldots, y_{i-1}), y_i' = g_i(y_1, \ldots, y_i), t' = 1] P_i \\ \Gamma \vdash \langle y_1' = g_1(y_1), \ldots, y_{i-1}' = g_{i-1}(y_1, \ldots, y_{i-1}), t' = 1 \rangle\, t > \tau\end{array}}{\Gamma \vdash \langle y_1' = g_1(y_1), \ldots, y_{i-1}' = g_{i-1}(y_1, \ldots, y_{i-1}), y_i' = g_i(y_1, \ldots, y_i), t' = 1 \rangle\, t > \tau}$$

□

Proof of Corollary 7. The proof closely follows the proof sketch for Corollary 7 but with an extra step to ensure that the chosen terms L, M are within the term language of dL. Let the ODE $x' = f(x)$ be globally Lipschitz and C be the (positive) Lipschitz constant for f, i.e., $\|f(x) - f(y)\| \le C\|x - y\|$. Then f satisfies the following inequality, where the first step (12) is proved in the sketch but its RHS contains norms $\|\cdot\|$ which are not in the term syntax (Sect. 2.1). The inequality (12) is prolonged by using inequality (10) to remove these non-squared norm terms, which yields corresponding choices of bounding dL terms L, M.

$$2x \cdot f(x) \overset{(12)}{\le} \big(2C + \|f(0)\|\big)\|x\|^2 + \|f(0)\| \overset{(10)}{\le} \underbrace{\Big(2C + \frac{1}{2}(1 + \|f(0)\|^2)\Big)}_{L}\|x\|^2 + \underbrace{\frac{1}{2}(1 + \|f(0)\|^2)}_{M} \tag{30}$$

The inequality (30) is a valid real arithmetic formula and is thus provable by rule $\mathbb{R}$. This enables the derivation below using axiom DDG⟨·⟩ because L, M satisfy the respective variable constraints of the axiom. The resulting left premise is proved, after a dW step, by $\mathbb{R}$. The resulting right premise, after the ODEs $x' = f(x)$ have been removed, is proved by axiom TEx.

$$\dfrac{\text{DDG}\langle\cdot\rangle\,\dfrac{\text{dW}\,\dfrac{\mathbb{R}\,\dfrac{*}{\vdash 2x \cdot f(x) \le L\|x\|^2 + M}}{\vdash [x' = f(x), t' = 1]\, 2x \cdot f(x) \le L\|x\|^2 + M} \qquad \text{TEx}\,\dfrac{*}{\vdash \langle t' = 1 \rangle\, t > \tau}}{\vdash \langle x' = f(x), t' = 1 \rangle\, t > \tau}}{\vdash \forall \tau\, \langle x' = f(x), t' = 1 \rangle\, t > \tau}\,\forall\text{R}$$

□

Proof of Corollary 8. Assume that the ODE $x' = f(x)$ has affine dependency order (9), i.e., where each ODE $y_i' = g_i(y_1, \ldots, y_i)$ is of the affine form $y_i' = A_i(y_1, \ldots, y_{i-1})y_i + b_i(y_1, \ldots, y_{i-1})$ for some matrix and vector terms A_i, b_i respectively with the indicated variable dependencies. From the proof sketch for Corollary 8, A_i, b_i satisfy inequality (13) for each $i = 1, \ldots, k$. Like the proof of inequality (30), inequality (13) is prolonged by inequality (10) to remove non-squared norm terms in its RHS, which yields corresponding choices of bounding dL terms L_i, M_i.

$$2y_i \cdot (A_i y_i + b_i) \overset{(13)}{\leq} (2\|A_i\| + \|b_i\|)\|y_i\|^2 + \|b_i\| \overset{(10)}{\leq} \underbrace{\left(1+\|A_i\|^2 + \frac{1}{2}(1+\|b_i\|^2)\right)}_{L_i} \|y_i\|^2 + \underbrace{\frac{1}{2}(1+\|b_i\|^2)}_{M_i} \tag{31}$$

The inequality from (31) is a valid real arithmetic formula, and thus provable by $\mathbb{R}$ for each $i = 1, \dots, k$. The derivation uses rule DEx, where the postcondition of each premise is chosen to be of form $\textcircled{D}$. The resulting premises are all proved, after a dW step, by $\mathbb{R}$ with the above choice of L_i, M_i for each $i = 1, \dots, k$.

$$\text{DEx}\ \dfrac{\text{dW}\ \dfrac{\mathbb{R}\ \dfrac{*}{\vdash 2y_1 \cdot (A_1 y_1 + b_1) \leq L_1\|y_1\|^2 + M_1}}{\vdash [y_1' = g_1(y_1), t' = 1]P_1} \quad \cdots \quad \text{dW}\ \dfrac{\mathbb{R}\ \dfrac{*}{\vdash 2y_k \cdot (A_k y_k + b_k) \leq L_k\|y_k\|^2 + M_k}}{\vdash [y_1' = g_1(y_1), \dots, y_k' = g_k(y_1, \dots, y_k), t' = 1]P_k}}{\vdash \forall \tau\, \langle x' = f(x), t' = 1\rangle\, t > \tau} \qquad \square$$

Proof of Corollary 9. The derivation starts by Skolemizing with ∀R, then switching the diamond modality in the succedent to a box modality in the antecedent using $\langle\cdot\rangle$, ¬R. The postcondition of the box modality is simplified using the propositional tautologies $\neg(\phi \vee \psi) \leftrightarrow \neg\phi \wedge \neg\psi$ and $\neg\neg\phi \leftrightarrow \phi$. Axiom $[\cdot]\wedge$, ∧L splits the conjunction in the antecedent, before $\langle\cdot\rangle$ is used again to flip the left antecedent to a diamond modality in the succedent. These (mostly) propositional steps recover the more verbose phrasing of BEx from (14).

$$\forall\text{R}\ \dfrac{\langle\cdot\rangle,\neg\text{R}\ \dfrac{[\cdot]\wedge,\wedge\text{L}\ \dfrac{\langle\cdot\rangle,\neg\text{L}\ \dfrac{[x' = f(x), t' = 1]B(x) \vdash \langle x' = f(x), t' = 1\rangle\, t > \tau}{[x' = f(x), t' = 1]\neg(t > \tau), [x' = f(x), t' = 1]B(x) \vdash \mathit{false}}}{[x' = f(x), t' = 1](\neg(t > \tau) \wedge B(x)) \vdash \mathit{false}}}{\vdash \langle x' = f(x), t' = 1\rangle(t > \tau \vee \neg B(x))}}{\vdash \forall \tau\, \langle x' = f(x), t' = 1\rangle(t > \tau \vee \neg B(x))}$$

The formula $B(x)$ is assumed to characterize a bounded set with respect to the variables x. The closure of this set (with respect to x) is compact so the continuous norm function $\|\cdot\|^2$ attains its maximum value on that set. Hence, the formula $\exists D\, \forall x\, (B(x) \rightarrow \|x\|^2 \leq D)$ is valid in first-order real arithmetic, and is thus provable by $\mathbb{R}$. The derivation continues with a cut of this formula and Skolemizing with ∃L. Axiom BDG$\langle\cdot\rangle$ is then used to remove the ODE $x' = f(x)$ with $p(x) = D$. The resulting right premise is proved by axiom TEx, while the resulting left premise is labeled ① and continued below.

$$\text{cut}, \mathbb{R}, \exists\text{L}\ \dfrac{\text{BDG}\langle\cdot\rangle\ \dfrac{① \qquad \text{TEx}\ \dfrac{*}{\vdash \langle t' = 1\rangle\, t > \tau}}{[x' = f(x), t' = 1]B(x), \forall x\, (B(x) \rightarrow \|x\|^2 \leq D) \vdash \langle x' = f(x), t' = 1\rangle\, t > \tau}}{[x' = f(x), t' = 1]B(x) \vdash \langle x' = f(x), t' = 1\rangle\, t > \tau}$$

From premise ①, a dC step adds the postcondition of the leftmost antecedent, $B(x)$, to the domain constraint. Since the remaining antecedent is universally quantified over variables x, it is soundly kept across an application of a subsequent dW step, and the proof is completed with ∀L, →L.

$$\text{dC}\ \dfrac{\text{dW}\ \dfrac{\forall\text{L},\rightarrow\text{L}\ \dfrac{*}{\forall x\, (B(x) \rightarrow \|x\|^2 \leq D), B(x) \vdash \|x\|^2 \leq D}}{\forall x\, (B(x) \rightarrow \|x\|^2 \leq D) \vdash [x' = f(x), t' = 1 \,\&\, B(x)]\, \|x\|^2 \leq D}}{[x' = f(x), t' = 1]B(x), \forall x\, (B(x) \rightarrow \|x\|^2 \leq D) \vdash [x' = f(x), t' = 1]\, \|x\|^2 \leq D} \qquad \square$$

Proof of Corollary 10. Assume the ODE $x' = f(x)$ is in dependency order (9), and the indices $i = 1, \dots, k$ are partitioned into disjoint sets L, N as in Corollary 10. The first step Skolemizes with ∀R.

$$\forall\text{R}\ \dfrac{\vdash \langle x' = f(x), t' = 1\rangle\big(t > \tau \vee \bigvee_{j \in N} \neg B_j(y_j)\big)}{\vdash \forall \tau\, \langle x' = f(x), t' = 1\rangle\big(t > \tau \vee \bigvee_{j \in N} \neg B_j(y_j)\big)}$$

The derivation uses ideas from Corollaries 6,8, and 9 to remove the ODE $y_i' = g_i(y_1, \dots, y_i)$ at each step. The corresponding disjunct $\neg B_i(y_i)$ (if present) is also removed from the succedent when $i \in N$. More precisely, at each step i, the derivation turns a succedent of the form (32) to the form (33) below which removes the variables y_i from the formula.

$$\langle y_1' = g_1(y_1), \ldots, y_{i-1}' = g_{i-1}(y_1, \ldots, y_{i-1}), y_i' = g_i(y_1, \ldots, y_i), t' = 1\rangle \left(t > \tau \lor \bigvee_{j \in N \cap \{1,\ldots,i\}} \neg B_j(y_j) \right) \tag{32}$$

$$\langle y_1' = g_1(y_1), \ldots, y_{i-1}' = g_{i-1}(y_1, \ldots, y_{i-1}), t' = 1\rangle \left(t > \tau \lor \bigvee_{j \in N \cap \{1,\ldots,i-1\}} \neg B_j(y_j) \right) \tag{33}$$

The derivation proceeds with two cases depending on whether $i \in L$ or $i \in N$.

- For each $i \in L$ (similarly to Corollary 8), the ODE $y_i' = A_i(y_1, \ldots, y_{i-1})y_i + b_i(y_1, \ldots, y_{i-1})$ is affine for some matrix and vector terms A_i, b_i respectively with the indicated variable dependencies. The RHS of this affine ODE satisfies the inequality (31) with terms L_i, M_i as given in (31). Axiom DDG$\langle\cdot\rangle$ is used with those choices of L_i, M_i, which removes the ODEs for y_i in the resulting right premise. The resulting left premise is labeled ① and explained below. Note that the freshness conditions of axiom DDG$\langle\cdot\rangle$ are met because the postcondition of the succedent does not mention variables y_i for $i \in L$. Similarly, the indices from $j \in N \cap \{1, \ldots, i\}$ are equal to those from $j \in N \cap \{1, \ldots, i-1\}$ because $i \notin N$.

$$\text{DDG}\langle\cdot\rangle\;\dfrac{① \qquad \vdash \langle y_1' = g_1(y_1), \ldots, y_{i-1}' = g_{i-1}(y_1, \ldots, y_{i-1}), t' = 1\rangle \big(t > \tau \lor \bigvee_{i \in N \cap \{1,\ldots,i-1\}} \neg B_i(y_i) \big)}{\vdash \langle y_1' = g_1(y_1), \ldots, y_{i-1}' = g_{i-1}(y_1, \ldots, y_{i-1}), y_i' = g_i(y_1, \ldots, y_i), t' = 1\rangle \big(t > \tau \lor \bigvee_{i \in N \cap \{1,\ldots,i\}} \neg B_i(y_i) \big)}$$

From premise ①, the proof is completed with a dW and $\mathbb{R}$ step using inequality (31).

$$\text{dW}\;\dfrac{\mathbb{R}\;\dfrac{*}{\vdash 2y_i \cdot (A_i y_i + b_i) \leq L_i \|y_i\|^2 + M_i}}{\vdash [y_1' = g_1(y_1), \ldots, y_i' = g_i(y_1, \ldots, y_i), t' = 1]\, 2y_i \cdot (A_i y_i + b_i) \leq L_i \|y_i\|^2 + M_i}$$

- For each $i \in N$ (similarly to Corollary 9), the boundedness assumption on y_i is first extracted from the succedent, with the abbreviation $R \equiv (t > \tau \lor \bigvee_{j \in N \cap \{1,\ldots,i-1\}} \neg B_j(y_j))$. The bottommost succedent is similarly abbreviated using the propositional tautology $\big(t > \tau \lor \bigvee_{j \in N \cap \{1,\ldots,i\}} \neg B_j(y_j)\big) \leftrightarrow R \lor \neg B_i(y_i)$.

$$\langle\cdot\rangle, \neg\text{R}\;\dfrac{[\cdot]\land, \land\text{L}\;\dfrac{\langle\cdot\rangle, \neg\text{L}\;\dfrac{[y_1' = g_1(y_1), \ldots, y_i' = g_i(y_1, \ldots, y_i), t' = 1]B_i(y_i) \vdash \langle y_1' = g_1(y_1), \ldots, y_i' = g_i(y_1, \ldots, y_i), t' = 1\rangle R}{[y_1' = g_1(y_1), \ldots, y_i' = g_i(y_1, \ldots, y_i), t' = 1]\neg R, [y_1' = g_1(y_1), \ldots, y_i' = g_i(y_1, \ldots, y_i), t' = 1]B_i(y_i) \vdash \mathit{false}}}{[y_1' = g_1(y_1), \ldots, y_i' = g_i(y_1, \ldots, y_i), t' = 1]\big(\neg R \land B_i(y_i)\big) \vdash \mathit{false}}}{\vdash \langle y_1' = g_1(y_1), \ldots, y_i' = g_i(y_1, \ldots, y_i), t' = 1\rangle (R \lor \neg B_i(y_i))}$$

The formula $B_i(y_i)$ is assumed to characterize a bounded set with respect to the variables y_i. Thus, like Corollary 9, the cut of the formula $\exists D_i\, \forall y_i\, (B_i(y_i) \rightarrow \|y_i\|^2 \leq D_i)$ is proved by $\mathbb{R}$. The derivation continues by Skolemizing, abbreviating $S \equiv [y_1' = g_1(y_1), \ldots, y_i' = g_i(y_1, \ldots, y_i), t' = 1]B_i(y_i)$. Axiom BDG$\langle\cdot\rangle$ is then used with $p(y_i) = D_i$, which removes the ODEs for y_i in the resulting right premise. The resulting left premise is labeled ② and explained below.

$$\text{cut}, \mathbb{R}, \exists\text{L}\;\dfrac{\text{BDG}\langle\cdot\rangle\;\dfrac{② \qquad \vdash \langle y_1' = g_1(y_1), \ldots, y_{i-1}' = g_{i-1}(y_1, \ldots, y_{i-1}), t' = 1\rangle R}{S, \forall y_i\, (B_i(y_i) \rightarrow \|y_i\|^2 \leq D_i) \vdash \langle y_1' = g_1(y_1), \ldots, y_i' = g_i(y_1, \ldots, y_i), t' = 1\rangle R}}{S \vdash \langle y_1' = g_1(y_1), \ldots, y_i' = g_i(y_1, \ldots, y_i), t' = 1\rangle R}$$

The derivation continues from premise ② identically to Corollary 9, with a dC step to add the postcondition of the antecedent S to the domain constraint. The proof is completed with dW and $\forall$L, $\rightarrow$L. The universally quantified antecedent $\forall y_i \ldots$ is soundly kept across the use of dW since it does not mention any of the bound variables $y_1,\dots,y_i,t$ of the ODE free.

$$\text{dC}\;\dfrac{\text{dW}\;\dfrac{\forall\text{L},\,\to\!\text{L}\;\dfrac{*}{\forall y_i\,(B(y_i)\to\|y_i\|^2\le D_i),B(y_i)\vdash\|y_i\|^2\le D_i}}{\forall y_i\,(B(y_i)\to\|y_i\|^2\le D_i)\vdash[y_1'=g_1(y_1),\dots,y_i'=g_i(y_1,\dots,y_i),t'=1\,\&\,B(y_i)]\,\|y_i\|^2\le D_i}}{S,\forall y_i\,(B(y_i)\to\|y_i\|^2\le D_i)\vdash[y_1'=g_1(y_1),\dots,y_i'=g_i(y_1,\dots,y_i),t'=1]\,\|y_i\|^2\le D_i}$$

Using the steps for $i=k,\dots,1$ (where either $i\in L$ or $i\in N$) successively removes the ODEs for $y_k,\dots,y_i$ from the succedent. This is shown in the derivation below and the proof is completed using TEx.

$$\dfrac{\dfrac{\dfrac{\dfrac{\text{TEx}\;\dfrac{*}{\vdash\langle t'=1\rangle t>\tau}}{\vdash\langle t'=1\rangle\big(t>\tau\lor\bigvee_{j\in N\cap\emptyset}\neg B_j(y_j)\big)}}{\vdots}}{\vdash\langle y_1'=g_1(y_1),\dots,y_{k-1}'=g_{k-1}(y_1,\dots,y_{k-1}),t'=1\rangle\big(t>\tau\lor\bigvee_{j\in N\cap\{1,\dots,k-1\}}\neg B_j(y_j)\big)}}{\vdash\langle y_1'=g_1(y_1),\dots,y_{k-1}'=g_{k-1}(y_1,\dots,y_{k-1}),y_k'=g_k(y_1,\dots,y_k),t'=1\rangle\big(t>\tau\lor\bigvee_{j\in N}\neg B_j(y_j)\big)}\qquad\square$$

Proof of Proposition 11. The ODE $x'=f(x)$ is assumed to have a global solution that is syntactically representable by polynomial term $X(t)$ in the term language (Sect. 2.1). Formally, this representability condition means that for any initial state ω, the mathematical solution $\boldsymbol{\varphi}:[0,\infty)\to\mathbb{S}$ exists globally and in addition, for each time $\tau\in[0,\infty)$, the solution satisfies $\boldsymbol{\varphi}(\tau)=\omega_t^\tau[\![X(t)]\!]$, where $\omega_t^\tau[\![X(t)]\!]$ is the value of term $X(t)$ in state ω with the value of time variable t set to τ. This implies that the following formula is valid because terms $x,t-t_0$ have value $\boldsymbol{\varphi}(\tau)$ and τ respectively at time $\tau\in[0,\infty)$ along the ODE $x'=f(x),t'=1$. The variables x_0,t_0 store the initial values of x,t respectively, which may be needed for the syntactic representation $X(t)$ of the solution. Additionally, the syntactic representation $X(t)$ may mention parameters $y\notin x$ that remain constant for the ODE $x'=f(x)$.

$$t=t_0\land x=x_0\to[x'=f(x),t'=1]\,x=X(t-t_0)\tag{34}$$

Validity of formula (34) further implies that (34) is provable because of the dL completeness theorem for equational invariants [Pla17a, PT20, Theorem 4.5]. The derivation of global existence for $x'=f(x)$ first Skolemizes with ∀R, then introduces fresh variables x_0,t_0 storing the initial values of x,t with cut, $\mathbb{R}$, ∃L. Axiom BDG⟨·⟩ is used with $p(t)=\|X(t-t_0)\|^2$ to remove the ODEs $x'=f(x)$. The resulting right premise is proved by axiom TEx, while the resulting left premise is abbreviated ① and proved below.

$$\forall\text{R}\;\dfrac{\text{cut},\mathbb{R},\exists\text{L}\;\dfrac{\text{BDG}\langle\cdot\rangle\;\dfrac{①\qquad\text{TEx}\;\dfrac{*}{\vdash\langle t'=1\rangle\,t>\tau}}{t=t_0\land x=x_0\vdash\langle x'=f(x),t'=1\rangle\,t>\tau}}{\vdash\langle x'=f(x),t'=1\rangle\,t>\tau}}{\vdash\forall\tau\,\langle x'=f(x),t'=1\rangle\,t>\tau}$$

From ①, the derivation continues with a dC using the provable formula (34). The premise after dW is proved by $\mathbb{R}$ after rewriting the succedent with the equality $x=X(t-t_0)$ and by reflexivity of $\le$.

$$\text{dC}\;\dfrac{\text{dW}\;\dfrac{\mathbb{R}\;\dfrac{*}{x=X(t-t_0)\vdash\|x\|^2\le\|X(t-t_0)\|^2}}{\vdash[x'=f(x),t'=1\,\&\,x=X(t-t_0)]\,\|x\|^2\le\|X(t-t_0)\|^2}}{t=t_0\land x=x_0\vdash[x'=f(x),t'=1]\,\|x\|^2\le\|X(t-t_0)\|^2}$$

Note that, instead of assuming that $X(t)$ is a syntactically representable (global) solution for the ODE $x'=f(x)$, it also suffices for this derivation to assume that premise ① is provable, i.e., that the term $\|X(t-t_0)\|^2$ (with free variables t,x_0,t_0 and parameters y) is a provable upper bound on the squared norm of x along solutions of the ODE. □

B.2. Proofs for liveness without domain constraints

Proof of Corollary 12. The complete derivation of rule $\mathrm{dV}_{\succcurlyeq}^{\Gamma}$ using refinement axiom $\mathrm{K}\langle\&\rangle$ and rule $\mathrm{dI}_{\succcurlyeq}$ is already given in the proof sketch for Corollary 12 so it is not repeated here.

The derivation of $\mathrm{dV}_{\succcurlyeq}$ (as a corollary of $\mathrm{dV}_{\succcurlyeq}^{\Gamma}$) starts by introducing fresh variables p_0, i representing the initial values of p and the multiplicative inverse of $\varepsilon()$ respectively using arithmetic cuts (cut, $\mathbb{R}$) and Skolemizing ($\exists$L). It then uses dGt to introduce a fresh time variable to the system of differential equations:

$$\text{cut},\mathbb{R}\;\dfrac{\exists\text{L}\;\dfrac{\text{dGt}\;\dfrac{\Gamma, \varepsilon() > 0, p = p_0, i\varepsilon() = 1, t = 0 \vdash \langle x' = f(x), t' = 1\rangle p \succcurlyeq 0}{\Gamma, \varepsilon() > 0, p = p_0, i\varepsilon() = 1 \vdash \langle x' = f(x)\rangle p \succcurlyeq 0}}{\Gamma, \varepsilon() > 0, \exists p_0\, (p = p_0), \exists i\, (i\varepsilon() = 1) \vdash \langle x' = f(x)\rangle p \succcurlyeq 0}}{\Gamma, \varepsilon() > 0 \vdash \langle x' = f(x)\rangle p \succcurlyeq 0}$$

Next, an initial liveness assumption $\langle x' = f(x), t' = 1\rangle p_0 + \varepsilon()t > 0$ is cut into the antecedents after which rule $\mathrm{dV}_{\succcurlyeq}^{\Gamma}$ is used to obtain the premise of $\mathrm{dV}_{\succcurlyeq}$. Intuitively, this initial liveness assumption says that the solution exists for sufficiently long, so that the term $p_0 + \varepsilon()t$ (which is proved to lower bound p) becomes positive for sufficiently large t. This cut is abbreviated $\textcircled{1}$ and proved below.

$$\text{cut}\;\dfrac{\mathrm{dV}_{\succcurlyeq}^{\Gamma}\;\dfrac{\neg(p \succcurlyeq 0) \vdash \dot{p} \geq \varepsilon()}{\Gamma, p = p_0, t = 0, \langle x' = f(x), t' = 1\rangle\, p_0 + \varepsilon()t > 0 \vdash \langle x' = f(x), t' = 1\rangle p \succcurlyeq 0} \quad \textcircled{1}}{\Gamma, \varepsilon() > 0, p = p_0, i\varepsilon() = 1, t = 0 \vdash \langle x' = f(x), t' = 1\rangle p \succcurlyeq 0}$$

From premise $\textcircled{1}$, a monotonicity step $\mathrm{M}\langle'\rangle$ equivalently rephrases the postcondition of the cut in real arithmetic. The arithmetic rephrasing works using the constant assumption $\varepsilon() > 0$ and the choice of i as the multiplicative inverse of $\varepsilon()$. Since the ODE $x' = f(x)$ is assumed to have provable global solutions, axiom GEx finishes the derivation by instantiating $\tau = -ip_0$, which is constant for the ODE.

$$\mathbb{R}, \mathrm{M}\langle'\rangle\;\dfrac{\text{GEx}\;\dfrac{*}{\Gamma \vdash \langle x' = f(x), t' = 1\rangle\, t > -ip_0}}{\Gamma, \varepsilon() > 0, i\varepsilon() = 1 \vdash \langle x' = f(x), t' = 1\rangle\, p_0 + \varepsilon()t > 0}$$

□

Proof of Corollary 13. Rule $\mathrm{dV}_{=}^{M}$ is derived directly from $\mathrm{dV}_{=}$ with a $\mathrm{M}\langle'\rangle$ monotonicity step:

$$\mathrm{M}\langle'\rangle\;\dfrac{p = 0 \vdash P \qquad \mathrm{dV}_{=}\;\dfrac{p < 0 \vdash \dot{p} \geq \varepsilon()}{\Gamma, \varepsilon() > 0, p \leq 0 \vdash \langle x' = f(x)\rangle p = 0}}{\Gamma, \varepsilon() > 0, p \leq 0 \vdash \langle x' = f(x)\rangle P}$$

The derivation of rule $\mathrm{dV}_{=}$ starts by using axiom $\mathrm{K}\langle\&\rangle$ with $G \equiv p \geq 0$ and rule $\mathrm{dV}_{\succcurlyeq}$ (with $\succcurlyeq$ being $\geq$) on the resulting right premise, which yields the sole premise of $\mathrm{dV}_{=}$ (on the right, after $\mathrm{dV}_{\succcurlyeq}$):

$$\mathrm{K}\langle\&\rangle\;\dfrac{p \leq 0 \vdash [x' = f(x) \,\&\, p \neq 0]p < 0 \qquad \mathrm{dV}_{\succcurlyeq}\;\dfrac{p < 0 \vdash \dot{p} \geq \varepsilon()}{\Gamma, \varepsilon() > 0 \vdash \langle x' = f(x)\rangle p \geq 0}}{\Gamma, \varepsilon() > 0, p \leq 0 \vdash \langle x' = f(x)\rangle p = 0}$$

From the left premise after using $\mathrm{K}\langle\&\rangle$, axiom DX allows the domain constraint $p \neq 0$ to be assumed true initially, which strengthens the antecedent $p \leq 0$ to $p < 0$. Rule Barr proves the invariance of formula $p < 0$ for the ODE $x' = f(x) \,\&\, p \neq 0$ because the antecedents $p{\neq}0, p{=}0$ in its resulting premise are contradictory.

$$\text{DX}\;\dfrac{\text{Barr}\;\dfrac{\mathbb{R}\;\dfrac{*}{p \neq 0, p = 0 \vdash \dot{p} < 0}}{p < 0 \vdash [x' = f(x) \,\&\, p \neq 0]p < 0}}{p \leq 0 \vdash [x' = f(x) \,\&\, p \neq 0]p < 0}$$

□

Proof of Corollary 14. Rule $\mathrm{dV}_{\succcurlyeq}^{k}$ can be derived in several ways. For example, because $\dot{p}^{(k)}$ is strictly positive, one can prove that the solution successively reaches states where $\dot{p}^{(k-1)}$ is strictly positive and remains positive thereafter, followed by reaching states where $\dot{p}^{(k-2)}$ is strictly positive (and remains positive thereafter), and so on. The following derivation shows how dC can be elegantly used for this argument. The idea is to extend the derivation of rule $\text{dV}_{\succcurlyeq}$ to higher Lie derivatives by (symbolically) integrating with respect to the time variable t using the following sequence of inequalities, where $\dot{p}_0^{(i)}$ is a symbolic constant that represents the initial value of the i-th Lie derivative of p along $x' = f(x)$ for $i = 0, 1, \ldots, k-1$:

$$\begin{aligned}
\dot{p}^{(k)} &\geq \varepsilon() \\
\dot{p}^{(k-1)} &\geq \dot{p}_0^{(k-1)} + \varepsilon()t \\
\dot{p}^{(k-2)} &\geq \dot{p}_0^{(k-2)} + \dot{p}_0^{(k-1)}t + \varepsilon()\frac{t^2}{2} \\
&\vdots \\
\dot{p}^{(1)} &\geq \dot{p}_0^{(1)} + \cdots + \dot{p}_0^{(k-1)}\frac{t^{k-2}}{(k-2)!} + \varepsilon()\frac{t^{k-1}}{(k-1)!} \\
p &\geq \underbrace{p_0 + \dot{p}_0^{(1)}t + \cdots + \dot{p}_0^{(k-1)}\frac{t^{k-1}}{(k-1)!} + \varepsilon()\frac{t^k}{k!}}_{q(t)}
\end{aligned} \tag{35}$$

The RHS of the final inequality in (35) is a polynomial in the time variable t, denoted $q(t)$, which is positive for sufficiently large values of t because its leading coefficient $\varepsilon()$ is strictly positive. That is, with antecedent $\varepsilon() > 0$, the formula $\exists t_1\, \forall t > t_1\, q(t) > 0$ is provable in real arithmetic.

The derivation of $\text{dV}^k_{\succcurlyeq}$ starts by introducing fresh ghost variables that remember the initial values of p and the (higher) Lie derivatives $\dot{p}^{(1)}, \ldots, \dot{p}^{(k-1)}$ using cut, $\mathbb{R}$, $\exists$L. The resulting antecedents are abbreviated with $\Gamma_0 \equiv \big(\Gamma, p = p_0, \ldots, \dot{p}^{(k-1)} = \dot{p}_0^{(k-1)}\big)$. It also uses dGt to introduce a fresh time variable t into the system. The arithmetic fact that $q(t)$ is eventually positive for all times $t > t_1$ is introduced with cut, $\mathbb{R}$, $\exists$L.

$$\scriptstyle{\text{cut},\,\mathbb{R},\,\exists\text{L}}\ \dfrac{\scriptstyle{\text{dGt}}\ \dfrac{\scriptstyle{\text{cut},\,\mathbb{R},\,\exists\text{L}}\ \dfrac{\Gamma_0, t = 0, \forall t > t_1\, q(t) > 0 \vdash \langle x' = f(x), t' = 1\rangle p \succcurlyeq 0}{\Gamma_0, \varepsilon() > 0, t = 0 \vdash \langle x' = f(x), t' = 1\rangle p \succcurlyeq 0}}{\Gamma, \varepsilon() > 0, p = p_0, \ldots, \dot{p}^{(k-1)} = \dot{p}_0^{(k-1)} \vdash \langle x' = f(x)\rangle p \succcurlyeq 0}}{\Gamma, \varepsilon() > 0 \vdash \langle x' = f(x)\rangle p \succcurlyeq 0}$$

Next, an initial liveness assumption, $\langle x' = f(x), t' = 1\rangle q(t) > 0$, is cut into the assumptions. Like the derivation of rule $\text{dV}_{\succcurlyeq}$, this initial liveness assumption says that the solution exists for sufficiently long so that the term $q(t)$ from (35), which is proved to lower bound p, becomes positive for sufficiently large t. The cut premise is abbreviated ① and further proved below. The derivation continues from the remaining (unabbreviated) premise by refinement axiom K⟨&⟩, with $G \equiv q(t) > 0$:

$$\scriptstyle{\text{cut}}\ \dfrac{\scriptstyle{\text{K}\langle\&\rangle}\ \dfrac{\Gamma_0, t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg(p \succcurlyeq 0)]q(t) \leq 0}{\Gamma_0, t = 0, \langle x' = f(x), t' = 1\rangle q(t) > 0 \vdash \langle x' = f(x), t' = 1\rangle p \succcurlyeq 0} \quad \text{①}}{\Gamma_0, t = 0, \forall t > t_1\, q(t) > 0 \vdash \langle x' = f(x), t' = 1\rangle p \succcurlyeq 0}$$

From the resulting open premise after K⟨&⟩, monotonicity M[′] strengthens the postcondition to $p \geq q(t)$ using the domain constraint $\neg(p \succcurlyeq 0)$ and the provable real arithmetic fact $\neg(p \succcurlyeq 0) \land p \geq q(t) \rightarrow q(t) \leq 0$. Notice that the resulting postcondition $p \geq q(t)$ is the final inequality from the sequence of inequalities (35):

$$\scriptstyle{\text{M}[']}\ \dfrac{\Gamma_0, t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg(p \succcurlyeq 0)]p \geq q(t)}{\Gamma_0, t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg(p \succcurlyeq 0)]q(t) \leq 0}$$

The derivation continues by using dC to sequentially cut in the inequality bounds outlined in (35). The first differential cut dC step adds $\dot{p}^{(k-1)} \geq \dot{p}_0^{(k-1)} + \varepsilon()t$ to the domain constraint. The proof of this cut yields the premise of $\text{dV}^k_{\succcurlyeq}$ after a $\text{dI}_{\succcurlyeq}$ step, see the derivation labeled $\circledast$ immediately below.

$$\scriptstyle{\text{dC}}\ \dfrac{\Gamma_0, t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg(p \succcurlyeq 0) \land \dot{p}^{(k-1)} \geq \dot{p}_0^{(k-1)} + \varepsilon()t]p \geq q(t) \quad \circledast}{\Gamma_0, t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg(p \succcurlyeq 0)]p \geq q(t)}$$

From $\textcircled{\star}$:

$$\begin{array}{rc}
 & \neg(p \succcurlyeq 0) \vdash \dot{p}^{(k)} \geq \varepsilon() \\ \cline{2-2}
\text{dI}_{\succcurlyeq} & \Gamma_0, t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg(p \succcurlyeq 0)]\dot{p}^{(k-1)} \geq \dot{p}_0^{(k-1)} + \varepsilon()t
\end{array}$$

Subsequent dC, $\text{dI}_{\succcurlyeq}$ steps progressively add the inequality bounds from (35) to the domain constraint until the last step where the postcondition is proved invariant with $\text{dI}_{\succcurlyeq}$:

$$\begin{array}{rc}
 & * \\ \cline{2-2}
\text{dI}_{\succcurlyeq} & \Gamma_0, t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \cdots \wedge \dot{p}^{(1)} \geq \dot{p}_0^{(1)} + \cdots + \varepsilon()\frac{t^{k-1}}{(k-1)!}]p \geq q(t) \\ \cline{2-2}
\text{dC, dI}_{\succcurlyeq} & \vdots \\ \cline{2-2}
\text{dC, dI}_{\succcurlyeq} & \Gamma_0, t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \cdots \wedge \dot{p}^{(k-2)} \geq \dot{p}_0^{(k-2)} + \dot{p}_0^{(k-1)}t + \varepsilon()\frac{t^2}{2}]p \geq q(t) \\ \cline{2-2}
\text{dC, dI}_{\succcurlyeq} & \Gamma_0, t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg(p \succcurlyeq 0) \wedge \dot{p}^{(k-1)} \geq \dot{p}_0^{(k-1)} + \varepsilon()t]p \geq q(t)
\end{array}$$

From premise $\textcircled{1}$, a monotonicity step $\text{M}\langle'\rangle$ rephrases the postcondition of the cut using the (constant) assumption $\forall t > t_1\, q(t) > 0$. Axiom GEx, with instance $\tau = t_1$, finishes the derivation because the ODE $x' = f(x)$ is assumed to have provable global solutions.

$$\begin{array}{rc}
 & * \\ \cline{2-2}
\text{GEx} & \Gamma \vdash \langle x' = f(x), t' = 1\rangle t > t_1 \\ \cline{2-2}
\text{M}\langle'\rangle & \Gamma, \forall t > t_1\, q(t) > 0 \vdash \langle x' = f(x), t' = 1\rangle q(t) > 0
\end{array} \qquad \square$$

Proof of Corollary 15. The derivation of rule SP begins by using axiom $\text{K}\langle\&\rangle$ with $G \equiv \neg S$. The resulting left premise is the left premise of SP, which is the staging property of the formula S expressing that solutions of the ODE $x' = f(x)$ can only leave S by entering P:

$$\begin{array}{rc}
 & \Gamma \vdash [x' = f(x) \,\&\, \neg P]S \qquad \Gamma, \varepsilon() > 0 \vdash \langle x' = f(x)\rangle \neg S \\ \cline{2-2}
\text{K}\langle\&\rangle & \Gamma, \varepsilon() > 0 \vdash \langle x' = f(x)\rangle P
\end{array}$$

The derivation continues on the right premise, similarly to $\text{dV}_{\succcurlyeq}$, by introducing fresh variables p_0, i representing the initial value of p and the multiplicative inverse of $\varepsilon()$ respectively using arithmetic cuts (cut, $\mathbb{R}$). It then uses dGt to introduce a fresh time variable:

$$\begin{array}{rc}
 & \Gamma, \varepsilon() > 0, p = p_0, i\varepsilon() = 1, t = 0 \vdash \langle x' = f(x), t' = 1\rangle \neg S \\ \cline{2-2}
\text{dGt} & \Gamma, \varepsilon() > 0, p = p_0, i\varepsilon() = 1 \vdash \langle x' = f(x)\rangle \neg S \\ \cline{2-2}
\exists\text{L} & \Gamma, \varepsilon() > 0, \exists p_0\, (p = p_0), \exists i\, (i\varepsilon() = 1) \vdash \langle x' = f(x)\rangle \neg S \\ \cline{2-2}
\text{cut}, \mathbb{R} & \Gamma, \varepsilon() > 0 \vdash \langle x' = f(x)\rangle \neg S
\end{array}$$

The next cut introduces an initial liveness assumption, where the cut premise is abbreviated $\textcircled{1}$. The premise $\textcircled{1}$ is proved identically to the correspondingly abbreviated premise from the derivation of $\text{dV}_{\succcurlyeq}$ using axiom GEx because the ODE $x' = f(x)$ is assumed have provable global solutions.

$$\begin{array}{rc}
 & \Gamma, p = p_0, t = 0, \langle x' = f(x), t' = 1\rangle\, p_0 + \varepsilon()t > 0 \vdash \langle x' = f(x), t' = 1\rangle \neg S \qquad \textcircled{1} \\ \cline{2-2}
\text{cut} & \Gamma, \varepsilon() > 0, p = p_0, i > 0, i\varepsilon() = 1, t = 0 \vdash \langle x' = f(x), t' = 1\rangle \neg S
\end{array}$$

From the remaining open premise, axiom $\text{K}\langle\&\rangle$ is used with $G \equiv p_0 + \varepsilon()t > 0$:

$$\begin{array}{rc}
 & \Gamma, p = p_0, t = 0 \vdash [x' = f(x), t' = 1 \,\&\, S]\, p_0 + \varepsilon()t \leq 0 \\ \cline{2-2}
\text{K}\langle\&\rangle & \Gamma, p = p_0, t = 0, \langle x' = f(x), t' = 1\rangle\, p_0 + \varepsilon()t > 0 \vdash \langle x' = f(x), t' = 1\rangle \neg S
\end{array}$$

A monotonicity step $\text{M}[']$ simplifies the postcondition using domain constraint S, yielding the left conjunct of the right premise of rule SP. The right premise after monotonicity is abbreviated $\textcircled{2}$ and continued below.

$$\begin{array}{rc}
 & \mathbb{R}\dfrac{S \vdash p \leq 0}{S, p \geq p_0 + \varepsilon()t \vdash p_0 + \varepsilon()t \leq 0} \qquad \textcircled{2} \\ \cline{2-2}
\text{M}['] & \Gamma, p = p_0, t = 0 \vdash [x' = f(x), t' = 1 \,\&\, S]\, p_0 + \varepsilon()t \leq 0
\end{array}$$

From ②, rule $\mathrm{dI}_{\succcurlyeq}$ yields the right conjunct of the right premise of rule SP.

$$\mathrm{dI}_{\succcurlyeq}\ \frac{S \vdash \dot{p} \geq \varepsilon()}{\Gamma, p = p_0, t = 0 \vdash [x' = f(x), t' = 1 \,\&\, S]\, p \geq p_0 + \varepsilon()t} \qquad \square$$

Proof of Corollary 16. Rule SP_b is derived first since rule SP_c follows from SP_b as a corollary. Both proof rules make use of the fact that continuous functions on compact domains attain their extrema [Rud76, Theorem 4.16]. Polynomial functions are continuous, so the fact that a polynomial has bounded values on a compact (semialgebraic) domain can be stated and proved as a formula of first-order real arithmetic by $\mathbb{R}$ [BCR98]. The derivation of SP_b is essentially similar to SP except replacing the use of the global existence axiom GEx with the bounded existence axiom BEx. It starts by using axiom $\mathrm{K}\langle\&\rangle$ with $G \equiv \neg S$, yielding the left premise of SP_b:

$$\mathrm{K}\langle\&\rangle\ \frac{\Gamma \vdash [x' = f(x) \,\&\, \neg P]S \qquad \Gamma, \varepsilon() > 0 \vdash \langle x' = f(x)\rangle \neg S}{\Gamma, \varepsilon() > 0 \vdash \langle x' = f(x)\rangle P}$$

Continuing on the resulting right from $\mathrm{K}\langle\&\rangle$ (similarly to SP), the derivation introduces fresh variables p_0, i representing the initial value of p and the multiplicative inverse of $\varepsilon()$ respectively using arithmetic cuts and Skolemizing (cut, $\mathbb{R}$, $\exists$L). Rule dGt is also used to introduce a fresh time variable t with $t = 0$ initially.

$$\text{cut}, \mathbb{R}, \exists\text{L}, \text{dGt}\ \frac{\Gamma, \varepsilon() > 0, p = p_0, i\varepsilon() = 1, t = 0 \vdash \langle x' = f(x), t' = 1\rangle \neg S}{\Gamma, \varepsilon() > 0 \vdash \langle x' = f(x)\rangle \neg S}$$

The set characterized by formula S is bounded so its closure is compact (with respect to variables x). On this compact closure, the continuous polynomial function p attains its maximum value, which implies that the value of p is bounded above in S and cannot increase unboundedly while staying in S. That is, the formula $\exists p_1\, R(p_1)$ where $R(p_1) \equiv \forall x\, (S(x) \rightarrow p \leq p_1)$ is valid in first-order real arithmetic and thus provable by $\mathbb{R}$. This formula is added to the assumptions with a cut, and the existential quantifier is Skolemized with $\exists$L. The resulting symbolic constant p_1 represents the upper bound of p on S. Note that $R(p_1)$ is constant for the ODE $x' = f(x), t' = 1$ because it does not mention any of the variables x (nor t) free:

$$\text{cut}, \mathbb{R}\ \frac{\exists\text{L}\ \dfrac{\Gamma, \varepsilon() > 0, p = p_0, i\varepsilon() = 1, t = 0, R(p_1) \vdash \langle x' = f(x), t' = 1\rangle \neg S}{\Gamma, \varepsilon() > 0, p = p_0, i\varepsilon() = 1, t = 0, \exists p_1\, R(p_1) \vdash \langle x' = f(x), t' = 1\rangle \neg S}}{\Gamma, \varepsilon() > 0, p = p_0, i\varepsilon() = 1, t = 0 \vdash \langle x' = f(x), t' = 1\rangle \neg S}$$

Next, a cut introduces an initial liveness assumption saying that *either* the solution exists for sufficient time for the bound $p_0 + \varepsilon()t > p_1$ to be satisfied (at sufficiently large t) *or* the solution leaves S. This assumption is abbreviated $T \equiv \langle x' = f(x), t' = 1\rangle(p_0 + \varepsilon()t > p_1 \vee \neg S)$. The main difference from SP is that the postcondition of assumption T adds a disjunction for the possibility of leaving S (which characterizes a bounded set). This cut premise is abbreviated ① and proved further below.

$$\text{cut}\ \frac{\Gamma, p = p_0, t = 0, R(p_1), T \vdash \langle x' = f(x), t' = 1\rangle \neg S \qquad \textcircled{1}}{\Gamma, \varepsilon() > 0, p = p_0, i\varepsilon() = 1, t = 0, R(p_1) \vdash \langle x' = f(x), t' = 1\rangle \neg S}$$

Continuing from the open premise on the left, axiom $\mathrm{K}\langle\&\rangle$ is used with $G \equiv p_0 + \varepsilon()t > p_1 \vee \neg S$:

$$\mathrm{K}\langle\&\rangle\ \frac{\Gamma, p = p_0, t = 0, R(p_1) \vdash [x' = f(x), t' = 1 \,\&\, S](p_0 + \varepsilon()t \leq p_1 \wedge S)}{\Gamma, p = p_0, t = 0, R(p_1), T \vdash \langle x' = f(x), t' = 1\rangle \neg S}$$

The postcondition of the resulting box modality is simplified to $p \geq p_0 + \varepsilon()t$ with a M['] monotonicity step. This crucially uses the assumption $R(p_1)$ which is constant for the ODE. A $\mathrm{dI}_{\succcurlyeq}$ step yields the remaining premise of SP_b on the right, see the derivation labeled ⊛ immediately below:

$$\text{M[']}\ \frac{\mathbb{R}\ \dfrac{\mathbb{R}\ \dfrac{*}{S, R(p_1) \vdash p \leq p_1}}{S, R(p_1), p \geq p_0 + \varepsilon()t \vdash p_0 + \varepsilon()t \leq p_1 \wedge S} \qquad \circledast}{\Gamma, p = p_0, t = 0, R(p_1) \vdash [x' = f(x), t' = 1 \,\&\, S](p_0 + \varepsilon()t \leq p_1 \wedge S)}$$

From ⋆:

$$\text{dI}_{\succcurlyeq}\ \dfrac{S \vdash \dot{p} \geq \varepsilon()}{\Gamma, p = p_0, t = 0 \vdash [x' = f(x), t' = 1 \,\&\, S]p \geq p_0 + \varepsilon()t}$$

From premise ①, a monotonicity step M⟨′⟩ equivalently rephrases the postcondition of the cut. Axiom BEx finishes the proof because formula $S(x)$ is assumed to be bounded over variables x.

$$\mathbb{R},\ \text{M}\langle{}'\rangle\ \dfrac{\text{BEx}\ \dfrac{*}{\vdash \langle x' = f(x), t' = 1\rangle (t > i(p_1 - p_0) \lor \neg S)}}{\varepsilon() > 0, i\varepsilon() = 1 \vdash T}$$

To derive rule SP$_c$ from SP$_b$, the compactness of the set characterized by $S(x)$ implies that the formula $\exists \varepsilon{>}0\, A(\varepsilon)$ where $A(\varepsilon) \equiv \forall x\, (S(x) \to \dot{p} \geq \varepsilon)$ and the formula $B \equiv \forall x\, (S(x) \to \dot{p} > 0)$ are provably equivalent in first-order real arithmetic. This provable real arithmetic equivalence follows from the fact that the continuous polynomial function $\dot{p}$ is bounded below by its minima on the compact set characterized by $S(x)$ and this minima is strictly positive. The following derivation of SP$_c$ threads these two formulas through the use of rule SP$_b$. After Skolemizing $\exists \varepsilon{>}0\, A(\varepsilon)$ with ∃L, the resulting formula $A(\varepsilon)$ is constant for the ODE $x' = f(x)$ so it is kept as a constant assumption across the use of SP$_b$, leaving only the two premises of rule SP$_c$:

$$\text{cut}\ \dfrac{\exists\text{L}\ \dfrac{\text{SP}_b\ \dfrac{\Gamma \vdash [x' = f(x) \,\&\, \neg P]S \qquad \mathbb{R}\ \dfrac{*}{S, A(\varepsilon) \vdash \dot{p} \geq \varepsilon}}{\Gamma, \varepsilon > 0, A(\varepsilon) \vdash \langle x' = f(x)\rangle P}}{\Gamma, \exists \varepsilon{>}0\, A(\varepsilon) \vdash \langle x' = f(x)\rangle P} \qquad \mathbb{R}\ \dfrac{\forall\text{R},\ {\to}\text{R}\ \dfrac{S \vdash \dot{p} > 0}{\vdash B}}{\vdash \exists \varepsilon{>}0\, A(\varepsilon)}}{\Gamma \vdash \langle x' = f(x)\rangle P}$$

□

Proof of Corollary 17. Rule SLyap is derived from rule SP$_c$ with $S \equiv \neg P \land K$, since the intersection of a closed set (characterized by $\neg P$) with a compact set (characterized by K) is compact. The resulting right premise from using SP$_c$ is the right premise of SLyap:

$$\text{SP}_c\ \dfrac{\Gamma, p \succcurlyeq 0 \vdash [x' = f(x) \,\&\, \neg P](\neg P \land K) \qquad \neg P, K \vdash \dot{p} > 0}{\Gamma, p \succcurlyeq 0 \vdash \langle x' = f(x)\rangle P}$$

Continuing from the left premise, a monotonicity step with the premise $p \geq 0 \vdash K$ turns the postcondition to $p \succcurlyeq 0$. Rule Barr is used, which, along with the premise $p \geq 0 \vdash K$ results in the premises of rule SLyap:

$$\text{M}[{}']\ \dfrac{\mathbb{R}\ \dfrac{p \geq 0 \vdash K}{\neg P, p \succcurlyeq 0 \vdash \neg P \land K} \qquad \text{Barr}\ \dfrac{\text{cut}\ \dfrac{\neg P, K \vdash \dot{p} > 0 \qquad \mathbb{R}\ \dfrac{p \geq 0 \vdash K}{\neg P, p = 0 \vdash K}}{\neg P, p = 0 \vdash \dot{p} > 0}}{p \succcurlyeq 0 \vdash [x' = f(x) \,\&\, \neg P]p \succcurlyeq 0}}{\Gamma, p \succcurlyeq 0 \vdash [x' = f(x) \,\&\, \neg P](\neg P \land K)}$$

□

B.3. Proofs for liveness with domain constraints

Proof of Corollary 18. The derivation uses axiom COR choosing $R \equiv \mathit{true}$ and noting that $p \geq 0$ (resp. $p > 0$) characterizes a topologically closed (resp. open) set so the appropriate topological requirements of COR are satisfied. The resulting left premise is the left premise of dV$_{\succcurlyeq}$&:

$$\text{COR}\ \dfrac{\Gamma \vdash [x' = f(x) \,\&\, \neg(p \succcurlyeq 0)]Q \qquad \Gamma, \varepsilon() > 0 \vdash \langle x' = f(x)\rangle p \succcurlyeq 0}{\Gamma, \varepsilon() > 0, \neg(p \succcurlyeq 0) \vdash \langle x' = f(x) \,\&\, Q\rangle p \succcurlyeq 0}$$

The proof continues from the resulting right premise (after COR) identically to the derivation of dV$_{\succcurlyeq}$ until the step where dV$^{\Gamma}_{\succcurlyeq}$ is used. The steps are repeated briefly here.

$$\text{cut},\ \mathbb{R},\ \exists\text{L}\ \dfrac{\text{dGt}\ \dfrac{\text{cut},\ \text{GEx}\ \dfrac{\Gamma, p = p_0, t = 0, \langle x' = f(x), t' = 1\rangle\, p_0 + \varepsilon()t > 0 \vdash \langle x' = f(x), t' = 1\rangle p \succcurlyeq 0}{\Gamma, \varepsilon() > 0, p = p_0, i\varepsilon() = 1, t = 0 \vdash \langle x' = f(x), t' = 1\rangle p \succcurlyeq 0}}{\Gamma, \varepsilon() > 0, p = p_0, i\varepsilon() = 1 \vdash \langle x' = f(x)\rangle p \succcurlyeq 0}}{\Gamma, \varepsilon() > 0 \vdash \langle x' = f(x)\rangle p \succcurlyeq 0}$$

Like the derivation of $\mathrm{dV}^{\Gamma}_{\succcurlyeq}$, axiom $\mathrm{K}\langle\&\rangle$ is used with $G \equiv p_0() + \varepsilon()t > 0$. The key difference is an additional dC step, which adds Q to the domain constraint.[15] The proof of this differential cut uses the left premise of $\mathrm{dV}_{\succcurlyeq}\&$, it is labeled $\textcircled{1}$ and shown below.

$$\mathrm{K}\langle\&\rangle\;\dfrac{\mathrm{dC}\;\dfrac{\Gamma, p = p_0(), t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg(p \succcurlyeq 0) \wedge Q]\, p_0() + \varepsilon()t \le 0 \qquad \textcircled{1}}{\Gamma, p = p_0(), t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg(p \succcurlyeq 0)]\, p_0() + \varepsilon()t \le 0}}{\Gamma, p = p_0, t = 0, \langle x' = f(x), t' = 1\rangle p_0 + \varepsilon()t > 0 \vdash \langle x' = f(x), t' = 1\rangle p \succcurlyeq 0}$$

The derivation from the resulting left premise (after the cut) continues similarly to $\mathrm{dV}^{\Gamma}_{\succcurlyeq}$ using a monotonicity step $\mathrm{M}[']$ to rephrase the postcondition, followed by $\mathrm{dI}_{\succcurlyeq}$ which results in the right premise of $\mathrm{dV}_{\succcurlyeq}\&$:

$$\mathrm{M}[']\;\dfrac{\mathrm{dI}_{\succcurlyeq}\;\dfrac{\neg(p \succcurlyeq 0), Q \vdash \dot{p} \ge \varepsilon()}{\Gamma, p = p_0(), t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg(p \succcurlyeq 0) \wedge Q]\, p \ge p_0() + \varepsilon()t}}{\Gamma, p = p_0(), t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg(p \succcurlyeq 0) \wedge Q]\, p_0() + \varepsilon()t \le 0}$$

The derivation from $\textcircled{1}$ removes the time variable t using the inverse direction of rule dGt [Pla17a, Pla18, PT20]. Just as rule dGt allows introducing a *fresh* time variable t for the sake of proof, its inverse direction simply removes the variable t since it is irrelevant for the proof of the differential cut.

$$\mathrm{dGt}\;\dfrac{\Gamma \vdash [x' = f(x) \,\&\, \neg(p \succcurlyeq 0)]Q}{\Gamma, p = p_0(), t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg(p \succcurlyeq 0)]Q}$$

□

Proof of Corollary 19. The derivations of rules $\mathrm{dV}_{=}\&$, $\mathrm{dV}^{M}_{=}\&$ are similar to the derivations of rules $\mathrm{dV}_{=}$, $\mathrm{dV}^{M}_{=}$ respectively. Rule $\mathrm{dV}^{M}_{=}\&$ is derived from $\mathrm{dV}_{=}\&$ by monotonicity:

$$\mathrm{M}\langle'\rangle\;\dfrac{Q, p = 0 \vdash P \qquad \mathrm{dV}_{=}\&\;\dfrac{\Gamma \vdash [x' = f(x) \,\&\, p < 0]Q \qquad p < 0, Q \vdash \dot{p} \ge \varepsilon()}{\Gamma, \varepsilon() > 0, p \le 0, Q \vdash \langle x' = f(x) \,\&\, Q\rangle p = 0}}{\Gamma, \varepsilon() > 0, p \le 0, Q \vdash \langle x' = f(x) \,\&\, Q\rangle P}$$

The derivation of rule $\mathrm{dV}_{=}\&$ starts by using axiom $\mathrm{K}\langle\&\rangle$ with $G \equiv p \ge 0$. The resulting box modality (right) premise is abbreviated $\textcircled{1}$ and proved below. On the resulting left premise, a DX step adds the negated postcondition $p < 0$ as an assumption to the antecedents since the domain constraint Q is true initially. Following that, rule $\mathrm{dV}_{\succcurlyeq}\&$ is used (with $\succcurlyeq$ being $\ge$, since Q characterizes a closed set). This yields the two premises of $\mathrm{dV}_{=}\&$:

$$\mathrm{K}\langle\&\rangle\;\dfrac{\mathrm{DX}\;\dfrac{\mathrm{dV}_{\succcurlyeq}\&\;\dfrac{\Gamma \vdash [x' = f(x) \,\&\, p < 0]Q \qquad p < 0, Q \vdash \dot{p} \ge \varepsilon()}{\Gamma, \varepsilon() > 0, p < 0 \vdash \langle x' = f(x) \,\&\, Q\rangle p \ge 0}}{\Gamma, \varepsilon() > 0, Q \vdash \langle x' = f(x) \,\&\, Q\rangle p \ge 0} \qquad \textcircled{1}}{\Gamma, \varepsilon() > 0, p \le 0, Q \vdash \langle x' = f(x) \,\&\, Q\rangle p = 0}$$

From premise $\textcircled{1}$, the derivation is completed similarly to $\mathrm{dV}_{=}$ using DX and Barr:

$$\mathrm{DX}\;\dfrac{\mathrm{Barr}\;\dfrac{\mathbb{R}\;\dfrac{*}{p \ne 0, p = 0 \vdash \dot{p} < 0}}{p < 0 \vdash [x' = f(x) \,\&\, Q \wedge p \ne 0]p < 0}}{p \le 0 \vdash [x' = f(x) \,\&\, Q \wedge p \ne 0]p < 0}$$

□

Proof of Corollary 20. Rule $\mathrm{SLyap}^{M}\&$ is derived from $\mathrm{SLyap}\&$ by a $\mathrm{DR}\langle\cdot\rangle$ monotonicity step followed by dW on its resulting left premise and $\mathrm{SLyap}\&$ on its resulting right premise:

$$\mathrm{DR}\langle\cdot\rangle\;\dfrac{\mathrm{dW}\;\dfrac{p > 0 \vdash Q}{\Gamma, p > 0 \vdash [x' = f(x) \,\&\, p > 0]Q} \qquad \mathrm{SLyap}\&\;\dfrac{p \ge 0 \vdash K \qquad \neg P, K \vdash \dot{p} > 0}{\Gamma, p > 0 \vdash \langle x' = f(x) \,\&\, p > 0\rangle P}}{\Gamma, p > 0 \vdash \langle x' = f(x) \,\&\, Q\rangle P}$$

[15] Notably, the differential cuts proof support from Sect. 7.2 can add such a cut automatically.

The derivation of rule SLyap& starts by adding assumption $\neg P$ to the antecedents, because if both $p > 0$ (which is already in the antecedents) and P were true initially, then the liveness succedent is trivially true by DX. Next, axiom COR is used with $R \equiv \mathit{true}$, its topological restrictions are met since both formulas P and $p > 0$ characterize open sets. From the resulting right premise, rule SLyap yields the corresponding two premises of SLyap& because formula K (resp. P) characterizes a compact set (resp. open set):

$$\scriptstyle\text{DX}\dfrac{\scriptstyle\text{COR}\dfrac{\Gamma, p > 0 \vdash [x' = f(x) \,\&\, \neg P]p > 0 \qquad \scriptstyle\text{SLyap}\dfrac{p \geq 0 \vdash K \qquad \neg P, K \vdash \dot{p} > 0}{\Gamma, p > 0 \vdash \langle x' = f(x)\rangle P}}{\Gamma, p > 0, \neg P \vdash \langle x' = f(x) \,\&\, p > 0\rangle P}}{\Gamma, p > 0 \vdash \langle x' = f(x) \,\&\, p > 0\rangle P}$$

From the leftmost open premise after COR, rule Barr is used and the resulting $p = 0$ assumption is turned into K using the left premise of SLyap&. The resulting open premises are the premises of SLyap&:

$$\scriptstyle\text{Barr}\dfrac{\scriptstyle\text{cut}\dfrac{\neg P, K \vdash \dot{p} > 0 \qquad \scriptstyle\mathbb{R}\dfrac{p \geq 0 \vdash K}{p = 0 \vdash K}}{\neg P, p = 0 \vdash \dot{p} > 0}}{\Gamma, p > 0 \vdash [x' = f(x) \,\&\, \neg P]p > 0}$$

□

Proof of Corollary 21. The derivation starts by using axiom SAR which results in two premises. From the left premise after axiom SAR, a monotonicity step turns the postcondition into S, yielding the left premise and first conjunct of the right premise of SP&.

$$\scriptstyle\text{SAR}\dfrac{\scriptstyle\text{M[']}\dfrac{S \vdash Q \qquad \Gamma \vdash [x' = f(x) \,\&\, \neg(P \wedge Q)]S}{\Gamma \vdash [x' = f(x) \,\&\, \neg(P \wedge Q)]Q} \qquad \Gamma \vdash \langle x' = f(x)\rangle P}{\Gamma \vdash \langle x' = f(x) \,\&\, Q\rangle P}$$

From the right premise after axiom SAR, rule SP yields the remaining two premises of SP&:

$$\scriptstyle\text{SP}\dfrac{\scriptstyle\text{dW, DMP}\dfrac{\Gamma \vdash [x' = f(x) \,\&\, \neg(P \wedge Q)]S}{\Gamma \vdash [x' = f(x) \,\&\, \neg P]S} \qquad S \vdash p \leq 0 \wedge \dot{p} \geq \varepsilon()}{\Gamma \vdash \langle x' = f(x)\rangle P}$$

The dW, DMP step uses the propositional tautology $\neg P \rightarrow \neg(P \wedge Q)$ to weaken the domain constraint so that it matches the left premise of rule SP&. □

Proof of Corollary 22. The chimeric proof rule SP^k_c& amalgamates ideas behind the rules SP&, dV$^k_{\succcurlyeq}$, SP$_c$. It is therefore unsurprising that the derivation of SP^k_c& uses various steps from the derivations of those rules. The derivation of SP^k_c& starts similarly to SP& (following Corollary 21) using axiom SAR:

$$\scriptstyle\text{SAR}\dfrac{\Gamma \vdash [x' = f(x) \,\&\, \neg(P \wedge Q)]Q \qquad \Gamma \vdash \langle x' = f(x)\rangle P}{\Gamma \vdash \langle x' = f(x) \,\&\, Q\rangle P}$$

From the left premise after SAR, a monotonicity step turns the postcondition into S, yielding the left premise and first conjunct of the right premise of SP^k_c&.

$$\scriptstyle\text{M[']}\dfrac{\Gamma \vdash [x' = f(x) \,\&\, \neg(P \wedge Q)]S \qquad S \vdash Q}{\Gamma \vdash [x' = f(x) \,\&\, \neg(P \wedge Q)]Q}$$

From the right premise after SAR, the derivation continues using K⟨&⟩ with $G \equiv \neg S$, followed by dW, DMP. The resulting left premise is (again) the left premise of SP^k_c&, while the resulting right premise is abbreviated ① and continued below:

$$\scriptstyle\text{K}\langle\&\rangle\dfrac{\scriptstyle\text{dW, DMP}\dfrac{\Gamma \vdash [x' = f(x) \,\&\, \neg(P \wedge Q)]S}{\Gamma \vdash [x' = f(x) \,\&\, \neg P]S} \qquad \textcircled{1}}{\Gamma \vdash \langle x' = f(x)\rangle P}$$

The derivation continues from ① by intertwining proof ideas from Corollary 14 and Corollary 16. First, compactness of the set characterized by $S(x)$ implies that the formula $\exists\varepsilon{>}0\, A(\varepsilon)$ where $A(\varepsilon) \equiv \forall x\,(S(x) \rightarrow$

$\dot{p}^{(k)} \geq \varepsilon$) and the formula $B \equiv \forall x\,(S(x) \rightarrow \dot{p}^{(k)} > 0)$ are provably equivalent in first-order real arithmetic. These facts are added to the assumptions similarly to the derivation of SP$_c$. The resulting right open premise is the right conjunct of the right premise of SP$_c^k$&:

$$\text{cut}\,\dfrac{\text{∃L}\,\dfrac{\Gamma, \varepsilon > 0, A(\varepsilon) \vdash \langle x' = f(x) \rangle \neg S}{\Gamma, \exists \varepsilon{>}0\, A(\varepsilon) \vdash \langle x' = f(x) \rangle \neg S} \qquad \mathbb{R}\,\dfrac{\forall\text{R}, \rightarrow\text{R}\,\dfrac{S \vdash \dot{p}^{(k)} > 0}{\vdash B}}{\vdash \exists \varepsilon{>}0\, A(\varepsilon)}}{\Gamma \vdash \langle x' = f(x) \rangle \neg S}$$

From the left premise, recall the derivation from Corollary 14 which introduces fresh variables for the initial values of the Lie derivatives with cut, $\mathbb{R}$, ∃L. The derivation continues similarly here, with the resulting antecedents abbreviated $\Gamma_0 \equiv \big(\Gamma, p = p_0, \ldots, \dot{p}^{(k-1)} = \dot{p}_0^{(k-1)}\big)$. Rule dGt is also used to add time variable t to the system of equations with initial value $t = 0$.

$$\text{cut}, \mathbb{R}, \text{∃L}\,\dfrac{\text{dGt}\,\dfrac{\Gamma_0, \varepsilon > 0, A(\varepsilon), t = 0 \vdash \langle x' = f(x), t' = 1 \rangle \neg S}{\Gamma_0, \varepsilon > 0, A(\varepsilon) \vdash \langle x' = f(x) \rangle \neg S}}{\Gamma, \varepsilon > 0, A(\varepsilon) \vdash \langle x' = f(x) \rangle \neg S}$$

Recall from Corollary 16 that the formula $R(p_1) \equiv \forall x\,(S(x) \rightarrow p \leq p_1)$ can be added to the assumptions using cut, $\mathbb{R}$, ∃L, for some fresh variable p_1 symbolically representing the maximum value of p on the compact set characterized by S:

$$\text{cut}, \mathbb{R}, \text{∃L}\,\dfrac{\Gamma_0, \varepsilon > 0, A(\varepsilon), t = 0, R(p_1) \vdash \langle x' = f(x), t' = 1 \rangle \neg S}{\Gamma_0, \varepsilon > 0, A(\varepsilon), t = 0 \vdash \langle x' = f(x), t' = 1 \rangle \neg S}$$

One last arithmetic cut is needed to set up the sequence of differential cuts (35). Recall the polynomial $q(t)$ from (35) is eventually positive for sufficiently large values of t because its leading coefficient is strictly positive. The same applies to the polynomial $q(t) - p_1$ so cut, $\mathbb{R}$ (and Skolemizing with ∃L) adds the formula $\forall t > t_1\,(q(t) - p_1 > 0)$ to the assumptions:

$$\text{cut}, \mathbb{R}, \text{∃L}\,\dfrac{\Gamma_0, \varepsilon > 0, A(\varepsilon), t = 0, R(p_1), \forall t > t_1\, q(t) - p_1 > 0 \vdash \langle x' = f(x), t' = 1 \rangle \neg S}{\Gamma_0, \varepsilon > 0, A(\varepsilon), t = 0, R(p_1) \vdash \langle x' = f(x), t' = 1 \rangle \neg S}$$

Once all the arithmetic cuts are in place, an additional cut introduces a (bounded) sufficient duration assumption $\langle x' = f(x), t' = 1 \rangle (q(t) - p_1 > 0 \vee \neg S)$ (antecedents temporarily abbreviated with $\ldots$ for brevity). The cut premise, abbreviated $\textcircled{1}$, is proved further below:

$$\text{cut}\,\dfrac{\Gamma_0, \ldots, \langle x' = f(x), t' = 1 \rangle (q(t) - p_1 > 0 \vee \neg S) \vdash \langle x' = f(x), t' = 1 \rangle \neg S \quad \textcircled{1}}{\Gamma_0, \varepsilon > 0, A(\varepsilon), t = 0, R(p_1), \forall t > t_1\,(q(t) - p_1 > 0) \vdash \langle x' = f(x), t' = 1 \rangle \neg S}$$

From the open premise on the left, axiom K⟨&⟩ is used with $G \equiv q(t) - p_1 > 0 \vee \neg S$:

$$\text{K}\langle\&\rangle\,\dfrac{\Gamma_0, \varepsilon > 0, A(\varepsilon), t = 0, R(p_1) \vdash [x' = f(x), t' = 1 \,\&\, S](q(t) - p_1 \leq 0 \wedge S)}{\Gamma_0, \ldots, \langle x' = f(x), t' = 1 \rangle (q(t) - p_1 > 0 \vee \neg S) \vdash \langle x' = f(x), t' = 1 \rangle \neg S}$$

Next, a monotonicity step M['] simplifies the postcondition using the (constant) assumption $R(p_1)$ and the domain constraint S:

$$\text{M}[{}']\,\dfrac{\Gamma_0, t = 0, A(\varepsilon) \vdash [x' = f(x), t' = 1 \,\&\, S] p \geq q(t)}{\Gamma_0, \varepsilon > 0, A(\varepsilon), t = 0, R(p_1) \vdash [x' = f(x), t' = 1 \,\&\, S](q(t) - p_1 \leq 0 \wedge S)}$$

The derivation closes using the chain of differential cuts from (35). In the first dC step, the (constant) assumption $A(\varepsilon)$ is used, see the derivation labeled $\textcircled{\star}$ immediately below:

$$\text{dC}\,\dfrac{\Gamma_0, t = 0 \vdash [x' = f(x), t' = 1 \,\&\, S \wedge \dot{p}^{(k-1)} \geq \dot{p}_0^{(k-1)} + \varepsilon()t] p \geq q(t) \quad \textcircled{\star}}{\Gamma_0, t = 0, A(\varepsilon) \vdash [x' = f(x), t' = 1 \,\&\, S] p \geq q(t)}$$

From $\textcircled{\star}$:

$$\text{dI}_{\succcurlyeq}\,\frac{\mathbb{R}\,\dfrac{*}{A(\varepsilon), S \vdash \dot{p}^{(k)} \geq \varepsilon()}}{\Gamma_0, t = 0, A(\varepsilon) \vdash [x' = f(x), t' = 1 \,\&\, S]\dot{p}^{(k-1)} \geq \dot{p}_0^{(k-1)} + \varepsilon()t}$$

Subsequent dC, dI$_{\succcurlyeq}$ steps are similar to the derivation in Corollary 14:

$$\text{dC, dI}_{\succcurlyeq}\,\frac{\text{dC, dI}_{\succcurlyeq}\,\dfrac{\text{dI}_{\succcurlyeq}\,\dfrac{*}{\Gamma_0, t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \cdots \wedge \dot{p}^{(1)} \geq \dot{p}_0^{(1)} + \cdots + \varepsilon()\frac{t^{k-1}}{(k-1)!}]p \geq q(t)}}{\vdots}}{\Gamma_0, t = 0 \vdash [x' = f(x), t' = 1 \,\&\, S \wedge \dot{p}^{(k-1)} \geq \dot{p}_0^{(k-1)} + \varepsilon()t]p \geq q(t)}$$

From premise $\textcircled{1}$, a monotonicity step M$\langle'\rangle$ rephrases the postcondition of the cut using the assumption $\forall t > t_1\, (q(t) - p_1 > 0)$. Axiom BEx finishes the derivation since formula $S(x)$ characterizes a compact (and hence bounded) set:

$$\text{M}\langle'\rangle\,\frac{\text{BEx}\,\dfrac{*}{\vdash \langle x' = f(x), t' = 1\rangle(t > t_1 \vee \neg S)}}{\forall t > t_1\, (q(t) - p_1 > 0) \vdash \langle x' = f(x), t' = 1\rangle(q(t) - p_1 > 0 \vee \neg S)}$$

□

Proof of Corollary 23. Rule E$_c$& is derived from SP$_c^k$& with $S \equiv Q \wedge \neg P$ and $k = 1$ because formula $Q \wedge \neg P$ is assumed to characterize a compact set, as required by rule SP$_c^k$&:

$$\text{SP}_c\,\frac{\text{M}[']\,\dfrac{\Gamma \vdash [x' = f(x) \,\&\, \neg(P \wedge Q)]Q}{\Gamma \vdash [x' = f(x) \,\&\, \neg(P \wedge Q)](Q \wedge \neg P)} \qquad \dfrac{Q, \neg P \vdash \dot{p} > 0}{Q, \neg P \vdash Q \wedge \dot{p} > 0}}{\Gamma \vdash \langle x' = f(x) \,\&\, Q\rangle P}$$

The M['] step uses the propositional tautology $\neg(P \wedge Q) \wedge Q \rightarrow Q \wedge \neg P$. □

B.4. Proofs for ODE liveness proofs in practice

Proof of Corollary 24. The derivation starts with a cut of the sole premise of dV$^{\exists}_{\succcurlyeq}$ (the left premise below). The existentially bound variable is renamed to δ throughout the derivation for clarity. After Skolemizing (with $\exists$L), rule dV$_{\succcurlyeq}$ is used with $\varepsilon() = \delta$. The universally quantified antecedent is constant for the ODE $x' = f(x)$ so it is soundly kept across the application of dV$_{\succcurlyeq}$. This proof is completed propositionally $\forall$L, $\rightarrow$L.

$$\text{cut}\,\frac{\Gamma \vdash \exists \delta > 0\, \forall x\, \big(\neg(p \succcurlyeq 0) \rightarrow \dot{p} \geq \delta\big) \qquad \exists\text{L}, \wedge\text{L}\,\dfrac{\text{dV}_{\succcurlyeq}\,\dfrac{\forall\text{L}, \rightarrow\text{L}\,\dfrac{*}{\forall x\, \big(\neg(p \succcurlyeq 0) \rightarrow \dot{p} \geq \delta\big), \neg(p \succcurlyeq 0) \vdash \dot{p} \geq \delta}}{\delta > 0, \forall x\, \big(\neg(p \succcurlyeq 0) \rightarrow \dot{p} \geq \delta\big) \vdash \langle x' = f(x) \,\&\, Q\rangle p \succcurlyeq 0}}{\exists \delta > 0\, \forall x\, \big(\neg(p \succcurlyeq 0) \rightarrow \dot{p} \geq \delta\big) \vdash \langle x' = f(x) \,\&\, Q\rangle p \succcurlyeq 0}}{\Gamma \vdash \langle x' = f(x) \,\&\, Q\rangle p \succcurlyeq 0}$$

□

Proof of Corollary 25. Assume that formulas P, G_P are in normal form as in Corollary 25. Rule dV is derived first since rule dV$^{\exists}$ follows from dV as a corollary. The derivation of rule dV uses variable b as a symbolic lower bound on the initial values of all terms p_{ij}, q_{ij} appearing in formula P. The formula $\exists b \bigwedge_{i=0}^{M} \left(\bigwedge_{j=0}^{m(i)} p_{ij} \geq b \wedge \bigwedge_{j=0}^{n(i)} q_{ij} \geq b\right)$ is a valid formula of real arithmetic and is proved as a cut by $\mathbb{R}$ because P is a finite formula so there exists a lower bound b smaller than the value all of the terms p_{ij}, q_{ij}.

The derivation starts similarly to dV$_{\succcurlyeq}$ by introducing fresh variables b (for the bound above), and i representing the multiplicative inverse of $\varepsilon()$ using arithmetic cuts cut, $\mathbb{R}$. It then Skolemizes ($\exists$L) and uses dGt to introduce a fresh time variable to the system of differential equations:

$$\scriptstyle\text{cut, }\mathbb{R}\displaystyle\dfrac{\scriptstyle\exists\text{L}\displaystyle\dfrac{\scriptstyle\text{dGt}\displaystyle\dfrac{\Gamma, \varepsilon() > 0, \bigwedge_{i=0}^{M}\Big(\bigwedge_{j=0}^{m(i)} p_{ij} \geq b \wedge \bigwedge_{j=0}^{n(i)} q_{ij} \geq b\Big), i\varepsilon() = 1, t = 0 \vdash \langle x' = f(x), t' = 1\rangle P}{\Gamma, \varepsilon() > 0, \bigwedge_{i=0}^{M}\Big(\bigwedge_{j=0}^{m(i)} p_{ij} \geq b \wedge \bigwedge_{j=0}^{n(i)} q_{ij} \geq b\Big), i\varepsilon() = 1 \vdash \langle x' = f(x)\rangle P}}{\Gamma, \varepsilon() > 0, \exists b\, \bigwedge_{i=0}^{M}\Big(\bigwedge_{j=0}^{m(i)} p_{ij} \geq b \wedge \bigwedge_{j=0}^{n(i)} q_{ij} \geq b\Big), \exists i\, (i\varepsilon() = 1) \vdash \langle x' = f(x)\rangle P}}{\Gamma, \varepsilon() > 0 \vdash \langle x' = f(x)\rangle P}$$

Next, the refinement axiom K⟨&⟩ is used with $G \equiv (b + \varepsilon()t > 0)$. This yields two premises, the right of which is proved by GEx (after monotonic rephrasing with $\mathbb{R}$, M⟨′⟩) because the ODE $x' = f(x)$ is assumed to have provable global solutions. The left premise from K⟨&⟩ is abbreviated ① and continued below.

$$\scriptstyle\text{K}\langle\&\rangle\displaystyle\dfrac{\text{①} \qquad \scriptstyle\mathbb{R},\text{ M}\langle'\rangle\displaystyle\dfrac{\scriptstyle\text{GEx}\displaystyle\dfrac{*}{\Gamma \vdash \langle x' = f(x), t' = 1\rangle t > -ib}}{\Gamma, \varepsilon() > 0, i\varepsilon() = 1 \vdash \langle x' = f(x), t' = 1\rangle (b + \varepsilon()t > 0)}}{\Gamma, \varepsilon() > 0, \bigwedge_{i=0}^{M}\Big(\bigwedge_{j=0}^{m(i)} p_{ij} \geq b \wedge \bigwedge_{j=0}^{n(i)} q_{ij} \geq b\Big), i\varepsilon() = 1, t = 0 \vdash \langle x' = f(x), t' = 1\rangle P}$$

Continuing from premise ①, monotonicity strengthens the postcondition from $b + \varepsilon()t \leq 0$ to G_P under the domain constraint assumption $\neg P$. This strengthening works because, assuming that $\neg P$ and G_P are true in a given state, then propositionally, at least one of the following pairs (each pair listed horizontally) of sub-formulas of $\neg P$ and G_P for some indices i, j is true in that state:

$$\begin{array}{ll} p_{ij} < 0 & p_{ij} - (b + \varepsilon()t) \geq 0 \\[1em] q_{ij} \leq 0 & q_{ij} - (b + \varepsilon()t) \geq 0 \end{array}$$

Either pair of formulas imply that formula $b + \varepsilon()t \leq 0$ is also true in that state, so the strengthening is proved by M[′], $\mathbb{R}$. Next, a cut, $\mathbb{R}$ step adds the formula G_P to the antecedents using the assumptions $\bigwedge_{i=0}^{M}\Big(\bigwedge_{j=0}^{m(i)} p_{ij} \geq b \wedge \bigwedge_{j=0}^{n(i)} q_{ij} \geq b\Big)$ and $t = 0$. Rule sAI& yields the sole premise of rule dV because G_P characterizes a closed set [PT20].

$$\scriptstyle\text{M}[']\text{, }\mathbb{R}\displaystyle\dfrac{\scriptstyle\text{cut, }\mathbb{R}\displaystyle\dfrac{\scriptstyle\text{sAI\&}\displaystyle\dfrac{\neg P, \dot{(\neg P)}^{(*)}, G_P \vdash \dot{(G_P)}^{(*)}}{G_P \vdash [x' = f(x), t' = 1 \,\&\, \neg P]G_P}}{\Gamma, \bigwedge_{i=0}^{M}\Big(\bigwedge_{j=0}^{m(i)} p_{ij} \geq b \wedge \bigwedge_{j=0}^{n(i)} q_{ij} \geq b\Big), t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg P]G_P}}{\Gamma, \bigwedge_{i=0}^{M}\Big(\bigwedge_{j=0}^{m(i)} p_{ij} \geq b \wedge \bigwedge_{j=0}^{n(i)} q_{ij} \geq b\Big), t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg P]\big(b + \varepsilon()t \leq 0\big)}$$

Rule $\text{dV}^{\exists}$ is derived from rule dV similarly to the derivation of rule $\text{dV}^{\exists}_{\succcurlyeq}$ from rule $\text{dV}_{\succcurlyeq}$. The derivation starts with a cut of the sole premise of $\text{dV}^{\exists}$ (the left premise below). The existentially bound variable is renamed to δ throughout the derivation for clarity. The right premise is abbreviated ② and shown below.

$$\scriptstyle\text{cut}\displaystyle\dfrac{\Gamma \vdash \exists \delta > 0\, \forall b\, \forall t\, \forall x\, \big(\neg P \wedge \dot{(\neg P)}^{(*)} \wedge G_P \rightarrow \dot{(G_P)}^{(*)}\big) \qquad \text{②}}{\Gamma \vdash \langle x' = f(x) \,\&\, Q\rangle P}$$

From ②, after Skolemizing (with ∃L), rule dV is used with $\varepsilon() = \delta$. The universally quantified antecedent is constant for the ODE $x' = f(x)$ and the universal quantification over variables b, t ensure that those variables are fresh in the rest of the sequent so the antecedent is soundly kept across the application of rule dV. This proof is completed propositionally ∀L, →L, ∧L.

$$\scriptstyle\exists\text{L, }\wedge\text{L}\displaystyle\dfrac{\scriptstyle\text{dV}\displaystyle\dfrac{\scriptstyle\forall\text{L, }\rightarrow\text{L, }\wedge\text{L}\displaystyle\dfrac{*}{\forall b\, \forall t\, \forall x\, \big(\neg P \wedge \dot{(\neg P)}^{(*)} \wedge G_P \rightarrow \dot{(G_P)}^{(*)}\big), \neg P, \dot{(\neg P)}^{(*)}, G_P \vdash \dot{(G_P)}^{(*)}}}{\delta > 0, \forall b\, \forall t\, \forall x\, \big(\neg P \wedge \dot{(\neg P)}^{(*)} \wedge G_P \rightarrow \dot{(G_P)}^{(*)}\big) \vdash \langle x' = f(x) \,\&\, Q\rangle P}}{\exists \delta > 0\, \forall b\, \forall t\, \forall x\, \big(\neg P \wedge \dot{(\neg P)}^{(*)} \wedge G_P \rightarrow \dot{(G_P)}^{(*)}\big) \vdash \langle x' = f(x) \,\&\, Q\rangle P}$$

□

Proof of Corollary 27. The derivation of rule cR is seemingly straightforward using axiom CR followed by rule Enc on the resulting middle premise. There is a minor subtlety to address because the formula $Q^{>}_{\geq}$ (with strict inequalities replacing non-strict ones in Q) is only a syntactic *under-approximation* of the interior of the set characterized by Q, and so the axiom CR does *not* immediately apply as stated. For example, formula $x < x$ characterizes the empty set, while the formula $x \leq x$ characterizes the set of all states, whose interior is also the set of all states. However, since Q is a semialgebraic formula, there is a computable quantifier-free formula $\mathring{Q}$ that exactly characterizes its topological interior [BCR98] which can be used with CR in the syntactic derivation below.

The derivation starts with a cut of the formula Q which yields the leftmost premise of rule cR. This is followed with DX, which adds formula $\neg P$ to the antecedents because there is nothing to prove if both formulas Q and P are already true initially. The derivation then uses CR with the computable formula $\mathring{Q}$ characterizing the topological interior of formula Q. This yields two premises, the right of which corresponds to the rightmost premise of rule cR. From the resulting left premise (with postcondition $\mathring{Q}$), an M['], $\mathbb{R}$ monotonicity step strengthens the postcondition because $Q^{>}_{\geq} \rightarrow \mathring{Q}$ is a provable formula of real arithmetic. Rule Enc completes the derivation because formula $Q^{>}_{\geq}$ is formed from finite conjunctions and disjunctions of strict inequalities, and $(Q^{>}_{\geq})^{\geq}_{>}$ is syntactically equal to Q by definition.

$$\text{cut}\,\dfrac{\Gamma\vdash Q \qquad \text{DX}\,\dfrac{\text{CR}\,\dfrac{\text{M['],}\,\mathbb{R}\,\dfrac{\text{Enc}\,\dfrac{\Gamma\vdash[x'=f(x)\,\&\,R\wedge\neg P\wedge Q]Q^{>}_{\geq}}{\Gamma,Q\vdash[x'=f(x)\,\&\,R\wedge\neg P]Q^{>}_{\geq}}}{\Gamma,Q\vdash[x'=f(x)\,\&\,R\wedge\neg P]\mathring{Q}} \qquad \Gamma\vdash\langle x'=f(x)\,\&\,R\rangle P}{\Gamma,Q,\neg P\vdash\langle x'=f(x)\,\&\,Q\rangle P}}{\Gamma,Q\vdash\langle x'=f(x)\,\&\,Q\rangle P}}{\Gamma\vdash\langle x'=f(x)\,\&\,Q\rangle P}$$

□

C. Counterexamples

This appendix gives explicit counterexamples to illustrate the soundness errors identified in Sects. 5 and 6.

C.1. Finite-time blow up

The soundness errors identified in Sect. 5 all arise because of incorrect handling of the fact that solutions may blow up in finite time. This phenomenon is studied in detail in Sect. 4, and it is illustrated by α_n (2), see Fig. 1, or α_b (7), see Example 1. The following is a counterexample for the original presentation of $\mathrm{dV}_=$ (and $\mathrm{dV}^M_=$, $\mathrm{dV}_=\&$, $\mathrm{dV}^M_=\&$) [TT10]. Similar counterexamples can be constructed for [PR07, Remark 3.6] and for the original presentation of SLyap, SLyap& [RS10].

Counterexample 9. Consider rule $\mathrm{dV}_=$ *without* the restriction that the ODE has provable global solutions. This unrestricted rule, denoted $\mathrm{dV}_=\lightning$, is unsound as shown by the following derivation using it with $\varepsilon()$=1:

$$\mathrm{dV}_=\lightning\,\dfrac{\mathbb{R}\,\dfrac{*}{v-2<0\vdash 1\geq 1}}{v-2\leq 0\vdash\langle u'=u^2,v'=1\rangle v-2=0}$$

The conclusion of this derivation is not valid. Consider the initial state ω with values $\omega(u) = 1$ and $\omega(v) = 0$. The explicit solution of the ODE from ω is given by $u(t) = \frac{1}{1-t}, v(t) = t$ for $t \in [0, 1)$. This solution *does not exist* beyond the time interval $[0, 1)$ because the u-coordinate asymptotically approaches ∞, i.e., blows up, as time approaches $t = 1$. It is impossible to reach a state satisfying $v - 2 = 0$ from ω along this solution since at least 2 time units are required.

This counterexample further illustrates the difficulty in handling nonlinear ODEs. Neither the precondition $(v - 2 \leq 0)$ nor postcondition $(v - 2 = 0)$ mention the variable u, and the ODEs $u' = u^2, v' = 1$ do not depend on variables v, u respectively, so it is tempting to disregard the variable u entirely. Indeed, the liveness property $v-2 \le 0 \to \langle v'=1\rangle v-2=0$ is valid. Yet, for liveness questions about the (original) ODE, $u'=u^2, v'=1$, the two variables are inextricably linked through the time axis of solutions to the ODE.

C.2. Topological considerations

The soundness errors identified in Sect. 6 arise because of incorrect topological reasoning in subtle cases where the topological boundaries of the sets characterized by the domain constraint and desired liveness postcondition intersect. The original presentation of $\text{dV}_{\succcurlyeq}\&$ [Pla10] gives the following proof rule for atomic inequalities $p \succcurlyeq 0$. For simplicity, assume that the ODE $x'=f(x)$ is globally Lipschitz continuous so that solutions exist for all time.

$$\text{dV}_{\succcurlyeq}\&\lightning\ \frac{\Gamma \vdash [x'=f(x) \,\&\, p \le 0]Q \qquad \neg(p \succcurlyeq 0), Q \vdash \dot{p} \ge \varepsilon()}{\Gamma, \varepsilon()>0 \vdash \langle x'=f(x) \,\&\, Q\rangle p \succcurlyeq 0}$$

Compared to $\text{dV}_{\succcurlyeq}\&$, this omits the assumption $\neg(p \succcurlyeq 0)$, makes no topological assumptions on the domain constraint Q, and uses syntactic weak negation [Pla10] for the domain constraint of its left premise. The following two counterexamples show that the two assumptions are necessary.

Counterexample 10. Consider the following derivation using the unsound rule $\text{dV}_{\succcurlyeq}\&\lightning$ with $\varepsilon()=1$:

$$\text{dV}_{\succcurlyeq}\&\lightning\ \dfrac{\text{dW},\mathbb{R}\,\dfrac{*}{u>1 \vdash [u'=1 \,\&\, u \le 0]u \le 1} \qquad \mathbb{R}\,\dfrac{*}{u<0, u \le 1 \vdash 1 \ge 1}}{u>1 \vdash \langle u'=1 \,\&\, u \le 1\rangle u \ge 0}$$

The conclusion of this derivation is not valid. In states where $u>1$ is true initially, the domain constraint is violated immediately so the diamond modality in the succedent is trivially false in those states.

Counterexample 11 ([Sog16]). This counterexample is adapted from [Sog16, Example 142], which has a minor typographical error (the sign of an inequality is flipped). Consider the following derivation using the unsound rule $\text{dV}_{\succcurlyeq}\&\lightning$ with $\varepsilon()=1$:

$$\text{dV}_{\succcurlyeq}\&\lightning\ \dfrac{\text{dW},\mathbb{R}\,\dfrac{*}{\vdash [u'=1 \,\&\, u \le 1]u \le 1} \qquad \mathbb{R}\,\dfrac{*}{u \le 1, u \le 1 \vdash 1 \ge 1}}{\vdash \langle u'=1 \,\&\, u \le 1\rangle u > 1}$$

The conclusion of this derivation is not valid and, in fact, unsatisfiable. The domain constraint $u \le 1$ and postcondition $u>1$ are contradictory so no solution can reach a state satisfying both simultaneously.

The next two counterexamples are for the liveness arguments from [PR05, Corollary 1] and [PR07, Theorem 3.5]. For clarity, the original notation from [PR07, Theorem 3.5] is used. The following conjecture is quoted from [PR07, Theorem 3.5]:

Conjecture 30. *Consider the system $x'=f(x)$, with $f \in C(\mathbb{R}^n,\mathbb{R}^n)$. Let $\mathcal{X} \subset \mathbb{R}^n$, $\mathcal{X}_0 \subseteq \mathcal{X}$, and $\mathcal{X}_r \subseteq \mathcal{X}$ be bounded sets. If there exists a function $B \in C^1(\mathbb{R}^n)$ satisfying:*

$$B(x) \le 0 \qquad \forall x \in \mathcal{X}_0 \tag{36}$$

$$B(x) > 0 \qquad \forall x \in \overline{\partial\mathcal{X} \setminus \partial\mathcal{X}_r} \tag{37}$$

$$\frac{\partial B}{\partial x} f(x) < 0 \qquad \forall x \in \overline{\mathcal{X} \setminus \mathcal{X}_r} \tag{38}$$

Then the eventuality property holds, i.e., for all initial conditions $x_0 \in \mathcal{X}_0$, the trajectory $x(t)$ of the system starting at $x(0)=x_0$ satisfies $x(T) \in \mathcal{X}_r$ and $x(t) \in \mathcal{X}$ for all $t \in [0,T]$ for some $T \ge 0$. The notation $\overline{\mathcal{X}}$ (resp. $\partial\mathcal{X}$) denotes the topological closure (resp. boundary) of the set $\mathcal{X}$.

In [PR05, Corollary 1], stronger conditions are required. In particular, the sets $\mathcal{X}_0, \mathcal{X}_r, \mathcal{X}$ are additionally required to be topologically open, and the inequality in (36) is strict, i.e., $B(x)<0$ instead of $B(x) \le 0$.

The soundness errors in both of these liveness arguments stem from the condition (37) being too permissive. For example, notice that if the sets $\partial\mathcal{X}, \partial\mathcal{X}_r$ are equal then (37) is vacuously true. The first counterexample below applies for the requirements of [PR07, Theorem 3.5], while the second applies even for the more restrictive requirements of [PR05, Corollary 1].

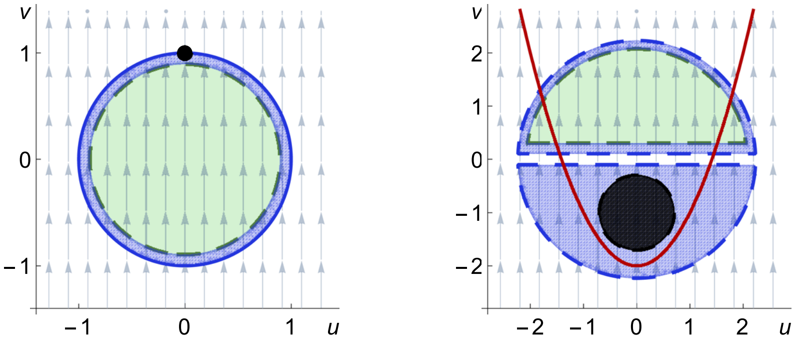


Fig. 6. (Left) Visualization of Counterexample 12. The solution from initial point $u = 0, v = 1$ ($\mathcal{X}_0$, in black) leaves the domain unit disk ($\mathcal{X}$, boundary in blue) immediately without ever reaching its interior ($\mathcal{X}_r$, in green with dashed boundary). The interior is slightly shrunk for clarity in the visualization: the blue and green boundaries should actually overlap exactly. **(Right)** Visualization of Counterexample 13. Solutions from the initial set ($\mathcal{X}_0$, in black with dashed boundary) eventually enter the goal region ($\mathcal{X}_r$, in green with dashed boundary). However, the domain ($\mathcal{X}$, in blue with dashed boundary) shares an (open) boundary with $\mathcal{X}_r$ at $v = 0$ which solutions are not allowed to cross. As before, the sets are slightly shrunk for clarity in the visualization: the blue and green boundaries should actually overlap exactly. The level curve $B = 0$ is plotted in red. All points above the curve satisfy $B < 0$, while all points below it satisfy $B > 0$.

Counterexample 12. Let the system $x' = f(x)$ be $u' = 0, v' = 1$. Let $\mathcal{X}_r$ be the open unit disk characterized by $u^2 + v^2 < 1$, $\mathcal{X}$ be the closed unit disk characterized by $u^2 + v^2 \leq 1$, and $\mathcal{X}_0$ be the single point characterized by $u = 0 \wedge v = 1$. All of these sets are bounded. Note that $\partial\mathcal{X} \setminus \partial\mathcal{X}_r = \emptyset$ since both topological boundaries are the unit circle $u^2 + v^2 = 1$. Let $B(u, v) = -v$, so that $\frac{\partial B}{\partial x} f(x) = \frac{\partial B}{\partial u} 0 + \frac{\partial B}{\partial v} 1 = -1 < 0$ and $B \leq 0$ on $\mathcal{X}_0$.

All conditions of [PR07, Theorem 3.5] are met but the eventuality property is false. The trajectory from $\mathcal{X}_0$ leaves $\mathcal{X}$ immediately and never enters $\mathcal{X}_r$. This is visualized in Fig. 6 (Left).

Counterexample 13. Let the system $x' = f(x)$ be $u' = 0, v' = 1$. Let $\mathcal{X}_r$ be the set characterized by the formula $u^2 + v^2 < 5 \wedge v > 0$, $\mathcal{X}$ be the set characterized by the formula $u^2 + v^2 < 5 \wedge v \neq 0$, and $\mathcal{X}_0$ be the set characterized by the formula $u^2 + (v + 1)^2 < \frac{1}{2}$. All of these sets are bounded and topologically open. Let $B(u, v) = -v + u^2 - 2$, so that $\frac{\partial B}{\partial x} f(x) = \frac{\partial B}{\partial u} 0 + \frac{\partial B}{\partial v} 1 = -1 < 0$, and $B < 0$ on $\mathcal{X}_0$. The set $\overline{\partial\mathcal{X} \setminus \partial\mathcal{X}_r}$ is characterized by formula $u^2 + v^2 = 5 \wedge v \leq 0$ and B is strictly positive on this set. These claims can be checked arithmetically, see Fig. 6 (Right) for a plot of the curve $B = 0$.

All conditions of [PR05, Corollary 1] are met but the eventuality property is false. Solutions starting in $\mathcal{X}_0$ eventually enter $\mathcal{X}_r$ but can only do so by leaving the domain constraint $\mathcal{X}$ at $v = 0$, see Fig. 6 (Right).

References

[ADBS09] Abate A, D'Innocenzo A, Di Benedetto MD, Sastry S(2009) Understanding deadlock and livelock behaviors in hybrid control systems. Nonlinear Anal Hybrid Syst 3(2):150–162. https://doi.org/10.1016/j.nahs.2008.12.005

[Alu15] Alur R (2015) Principles of cyber-physical systems. MIT Press, Cambridge

[BAB16] Butler MJ, Abrial J-R, Banach R (2016) Modelling and refining hybrid systems in Event-B and Rodin. In: Petre L, Sekerinski E (eds) From action systems to distributed systems—the refinement approach. Chapman and Hall/CRC, Boca Raton, pp 29–42. https://doi.org/10.1201/b20053

[BCR98] Bochnak J, Coste M, Roy M-F (1998) Real algebraic geometry. Springer, Heidelberg. https://doi.org/10.1007/978-3-662-03718-8

[BFP19] Bohrer B, Fernández M, Platzer A (2019) dL$_\iota$: Definite descriptions in differential dynamic logic. In: Fontaine P (ed) CADE, volume 11716 of LNCS. Springer, Cham, pp 94–110. https://doi.org/10.1007/978-3-030-29436-6_6

[BTM+19] Bohrer B, Tan YK, Mitsch S, Sogokon A, Platzer A (2019) A formal safety net for waypoint-following in ground robots. IEEE Robot Autom Lett 4(3):2910–2917. https://doi.org/10.1109/LRA.2019.2923099

[BvW98] Back R-J, von Wright J (1998) Refinement calculus—a systematic introduction. Springer, Berlin. https://doi.org/10.1007/978-1-4612-1674-2

[CÁS13] Chen X, Ábrahám E, Sankaranarayanan S (2013) Flow*: an analyzer for non-linear hybrid systems. In: Sharygina N, Veith H (eds) CAV, volume 8044 of LNCS. Springer, Heidelberg, pp 258–263. https://doi.org/10.1007/978-3-642-39799-8_18

[Chi06] Chicone C (2006) Ordinary differential equations with applications, 2nd ed. Springer, New York. https://doi.org/10.1007/0-387-35794-7

[DAPS19] Dupont G, Ameur Y, Pantel M, Singh NK (2019) Handling refinement of continuous behaviors: a proof based approach with Event-B. In: Méry D, Qin S (eds) TASE. IEEE, pp 9–16. https://doi.org/10.1109/TASE.2019.00-25

[DFPP18] Doyen L, Frehse G, Pappas GJ, Platzer A (2018) Verification of hybrid systems. In: Clarke EM, Henzinger TA, Veith H, Bloem R (eds) Handbook of model checking. Springer, Cham, pp 1047–1110. https://doi.org/10.1007/978-3-319-10575-8_30

[DM12] Duggirala PS, Mitra S (2012) Lyapunov abstractions for inevitability of hybrid systems. In: Dang T, Mitchell IM (eds) HSCC. ACM, New York, pp 115–124. https://doi.org/10.1145/2185632.2185652

[FGD$^+$11] Frehse G, Guernic CL, Donzé A, Cotton S, Ray R, Lebeltel O, Ripado R, Girard A, Dang T, Maler O (2011) SpaceEx: scalable verification of hybrid systems. In: Gopalakrishnan G, Qadeer S (eds) CAV, volume 6806 of LNCS. Springer, Heidelberg, pp 379–395. https://doi.org/10.1007/978-3-642-22110-1_30

[FMBP17] Fulton N, Mitsch S, Bohrer B, Platzer A (2017) Bellerophon: tactical theorem proving for hybrid systems. In: Ayala-Rincón M, Muñoz CA (eds) ITP, volume 10499 of LNCS. Springer, Cham, pp 207–224. https://doi.org/10.1007/978-3-319-66107-0_14

[FMQ$^+$15] Fulton N, Mitsch S, Quesel J-D, Völp M, Platzer A (2015) KeYmaera X: an axiomatic tactical theorem prover for hybrid systems. In: Felty AP, Middeldorp A (eds) CADE, volume 9195 of LNCS. Springer, Cham, pp 527–538. https://doi.org/10.1007/978-3-319-21401-6_36

[FyMS20] Foster S, y Munive JJH, Struth G(2020) Differential Hoare logics and refinement calculi for hybrid systems with Isabelle/HOL. In: Fahrenberg U, Jipsen P, Winter M (eds) RAMiCS, volume 12062 of LNCS. Springer, pp 169–186. https://doi.org/10.1007/978-3-030-43520-2_11

[GBC08] Graça DS, Buescu J, Campagnolo ML (2008) Boundedness of the domain of definition is undecidable for polynomial ODEs. Electron Notes Theor Comput Sci 202:49–57. https://doi.org/10.1016/j.entcs.2008.03.007

[GCB08] Graça DS, Campagnolo ML, Buescu J (2008) Computability with polynomial differential equations. Adv Appl Math 40(3):330–349. https://doi.org/10.1016/j.aam.2007.02.003

[GP14] Ghorbal K, Platzer A (2014) Characterizing algebraic invariants by differential radical invariants. In: Ábrahám E, Havelund K (eds) TACAS, volume 8413 of LNCS. Springer, Heidelberg, pp 279–294. https://doi.org/10.1007/978-3-642-54862-8_19

[GP17] Goubault E, Putot S (2017) Forward inner-approximated reachability of non-linear continuous systems. In: Frehse G, Mitra S (eds) HSCC. ACM, New York, pp 1–10. https://doi.org/10.1145/3049797.3049811

[Har79] Harel D (1979) First-order dynamic logic, volume 68 of LNCS. Springer. https://doi.org/10.1007/3-540-09237-4

[HC08] Haddad WM, Chellaboina V (2008) Nonlinear dynamical systems and control: a Lyapunov-based approach. Princeton University Press, Princeton

[Hen96] Henzinger TA (1996) The theory of hybrid automata. In: LICS. IEEE Computer Society, pp 278–292. https://doi.org/10.1109/LICS.1996.561342

[Kha92] Khalil HK (1992) Nonlinear systems. Macmillan Publishing Company, New York

[Koz97] Kozen D (1997) Kleene algebra with tests. ACM Trans Program Lang Syst 19(3):427–443. https://doi.org/10.1145/256167.256195

[LIC12] Logic in Computer Science (LICS) (2012) 27th Annual IEEE symposium on. Los Alamitos, IEEE

[LP16] Loos SM, Platzer A (2016) Differential refinement logic. In: Grohe M, Koskinen E, Shankar N (eds) LICS. ACM, pp 505–514. https://doi.org/10.1145/2933575.2934555

[LZZ11] Liu J, Zhan N, Zhao H (2011) Computing semi-algebraic invariants for polynomial dynamical systems. In: Chakraborty S, Jerraya A, Baruah SK, Fischmeister S (eds) EMSOFT. ACM, New York, pp 97–106. https://doi.org/10.1145/2038642.2038659

[MP92] Manna Z, Pnueli A (1992) The temporal logic of reactive and concurrent systems—specification. Springer, New York. https://doi.org/10.1007/978-1-4612-0931-7

[OL82] Owicki SS, Lamport L (1982) Proving liveness properties of concurrent programs. ACM Trans Program Lang Syst 4(3):455–495. https://doi.org/10.1145/357172.357178

[PJP07] Prajna S, Jadbabaie A, Pappas GJ (2007) A framework for worst-case and stochastic safety verification using barrier certificates. IEEE Trans Automat Control 52(8):1415–1428. https://doi.org/10.1109/TAC.2007.902736

[Pla10] Platzer A (2010) Differential-algebraic dynamic logic for differential-algebraic programs. J Log Comput 20(1):309–352. https://doi.org/10.1093/logcom/exn070

[Pla12a] Platzer A The complete proof theory of hybrid systems. In: LICS [LIC12]. pp 541–550. https://doi.org/10.1109/LICS.2012.64

[Pla12b] Platzer A Logics of dynamical systems. In: LICS [LIC12]. pp 13–24. https://doi.org/10.1109/LICS.2012.13

[Pla17a] Platzer A (2017) A complete uniform substitution calculus for differential dynamic logic. J Autom Reason 59(2):219–265. https://doi.org/10.1007/s10817-016-9385-1

[Pla17b] Platzer A (2017) Differential hybrid games. ACM Trans Comput Log 18(3):19:1–19:44. https://doi.org/10.1145/3091123

[Pla18] Platzer A (2018) Logical foundations of cyber-physical systems. Springer, Cham. https://doi.org/10.1007/978-3-319-63588-0

[PP02] Papachristodoulou A, Prajna S (2002) On the construction of Lyapunov functions using the sum of squares decomposition. In: CDC, vol 3. IEEE, pp 3482–3487. https://doi.org/10.1109/CDC.2002.1184414

[PQ08] Platzer A, Quesel J-D (2008) KeYmaera: a hybrid theorem prover for hybrid systems (system description). In: Armando A, Baumgartner P, Dowek G (eds) IJCAR, volume 5195 of LNCS. Springer, pp 171–178. https://doi.org/10.1007/978-3-540-71070-7_15

[PR05] Prajna S, Rantzer A (2005) Primal-dual tests for safety and reachability. In: Morari M, Thiele L (eds) HSCC, volume 3414 of LNCS. Springer, Heidelberg, pp 542–556. https://doi.org/10.1007/978-3-540-31954-2_35

[PR07] Prajna S, Rantzer A (2007) Convex programs for temporal verification of nonlinear dynamical systems. SIAM J Control Optim 46(3):999–1021. https://doi.org/10.1137/050645178

[PT20] Platzer A, Tan YK (2020) Differential equation invariance axiomatization. J ACM 67(1). https://doi.org/10.1145/3380825

[PW06] Podelski A, Wagner S (2006) Model checking of hybrid systems: from reachability towards stability. In: Hespanha JP, Tiwari A (eds) HSCC, volume 3927 of LNCS. Springer, Heidelberg, pp 507–521. https://doi.org/10.1007/11730637_38

[RRS03] Rönkkö M, Ravn AP, Sere K (2003) Hybrid action systems. Theor Comput Sci 290(1):937–973. https://doi.org/10.1016/S0304-3975(02)00547-9

[RS10] Ratschan S, She Z (2010) 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. https://doi.org/10.1137/090749955

[Rud76] Rudin W (1976) Principles of mathematical analysis, 3rd edn. McGraw-Hill, New York

[SJ15] Sogokon A, Jackson PB (2015) Direct formal verification of liveness properties in continuous and hybrid dynamical systems. In Bjørner N, de Boer FS (eds) FM, volume 9109 of LNCS. Springer, Cham, pp 514–531. https://doi.org/10.1007/978-3-319-19249-9_32

[SJJ19] Sogokon A, Jackson PB, Johnson TT (2019) Verifying safety and persistence in hybrid systems using flowpipes and continuous invariants. J Autom Reason 63(4):1005–1029. https://doi.org/10.1007/s10817-018-9497-x

[Sog16] Sogokon A (2016) Direct methods for deductive verification of temporal properties in continuous dynamical systems. PhD thesis, Laboratory for Foundations of Computer Science, School of Informatics, University of Edinburgh

[TP19] Tan YK, Platzer A (2019) An axiomatic approach to liveness for differential equations. In: ter Beek MH, McIver A, Oliveira JN (eds) FM, volume 11800 of LNCS. Springer, Cham, pp 371–388. https://doi.org/10.1007/978-3-030-30942-8_23

[TT10] Taly A, Tiwari A (2010) Switching logic synthesis for reachability. In: Carloni LP, Tripakis S (eds) EMSOFT. ACM, New York, pp 19–28. https://doi.org/10.1145/1879021.1879025

[Wal98] Walter W (1998) Ordinary differential equations. Springer, New York. https://doi.org/10.1007/978-1-4612-0601-9

[WZZ15] Wang S, Zhan N, Zou L (2015) An improved HHL prover: an interactive theorem prover for hybrid systems. In: Butler MJ, Conchon S, Zaïdi F (eds) ICFEM, volume 9407 of LNCS. Springer, Cham, pp 382–399. https://doi.org/10.1007/978-3-319-25423-4_25

[ZJLS01] Zhang J, Johansson KH, Lygeros J, Sastry S (2001) Zeno hybrid systems. Int J Robust Nonlinear Control 11(5):435–451. https://doi.org/10.1002/rnc.592

Received 12 April 2020

Accepted in revised form 7 November 2020 by Annabelle McIver, Maurice ter Beek and Cliff Jones

Published online 12 April 2021