An Axiomatic Approach to Liveness for Differential Equations

Yong Kiam Tan and André Platzer

Computer Science Department, Carnegie Mellon University, Pittsburgh, USA
{yongkiat|aplatzer}@cs.cmu.edu

Abstract. This paper presents an approach for deductive liveness verification for ordinary differential equations (ODEs) with differential dynamic logic. Numerous subtleties complicate the generalization of well-known 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. Our approach handles these subtleties by successively refining ODE liveness properties using ODE invariance properties which have a well-understood deductive proof theory. This approach is widely applicable: we survey several liveness arguments in the literature and derive them all as special instances of our axiomatic refinement approach. We also correct several soundness errors in the surveyed arguments, which further highlights the subtlety of ODE liveness reasoning and the utility of our deductive approach. The library of common refinement steps identified through our approach enables both the sound development and justification of new ODE liveness proof rules from our axioms.

Keywords: differential equations, liveness, differential dynamic logic

1 Introduction

Hybrid systems are mathematical models describing discrete and continuous dynamics, and interactions thereof [6]. This flexibility makes them natural models of cyber-physical systems (CPSs) which feature interactions between discrete computational control and continuous real world physics [2,19]. 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 continuous dynamics is a key aspect of any such endeavor.

This paper focuses on deductive liveness verification for continuous dynamics described by ordinary differential equations (ODEs). We work with differential dynamic logic (dL) [16,17,19], a logic for *deductive verification* of hybrid systems, which compositionally lifts our results to the hybrid systems setting. Methods for proving liveness in the discrete setting are well-known: loop variants show that discrete loops eventually reach a desired goal, while temporal logic is used to specify and study liveness properties in concurrent and infinitary settings [12,13]. In the continuous setting, *liveness* for an ODE means that its solutions eventually enter a desired goal region in finite time without leaving the domain of

M. H. ter Beek et al. (Eds.): FM 2019, LNCS 11800, pp. 371–388, 2019.
DOI: 10.1007/978-3-030-30942-8_23

Table 1. Surveyed ODE liveness arguments with our corrections highlighted in blue. The referenced corollaries are our corresponding (corrected) derived proof rules.

Source	Without Domain Constraints		With Domain Constraints	
[15]	OK	(Cor. 5)	if open/closed, initially false	(Cor. 13)
[22,23]	[23, Remark 3.6] is incorrect		if conditions checked globally	(Cor. 19)
[24]	if compact	(Cor. 12)	if compact	(Cor. 15)
[25]	OK	(Cor. 9)	OK	(Cor. 16)
[27]	if globally Lipschitz	(Cor. 7)	if globally Lipschitz	(Cor. 14)

allowed (or safe) states.[1] Deduction of such ODE liveness properties is hampered by several difficulties: *i)* solutions of ODEs may converge towards a goal without ever reaching it, *ii)* solutions of (non-linear) 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 leaving the domain constraint. In contrast, *invariance* properties for ODEs are better understood [9,11] and have a complete dL axiomatization [20]. Motivated by the aforementioned difficulties, we present dL axioms enabling step-by-step refinement of ODE liveness properties with a sequence of ODE invariance properties. This brings the full deductive power of dL's ODE invariance proof rules to bear on liveness proofs. Our approach is a general framework for understanding ODE liveness arguments. We use it to survey several arguments from the literature and derive them all as (corrected) dL proof rules, see Table 1. This logical presentation has two key benefits:

- The proof rules are *derived* from sound axioms of dL, guaranteeing their correctness. Many of the surveyed arguments contain subtle soundness errors, see Table 1. 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 rather than ad hoc approaches.
- The approach identifies common refinement steps that form a basis for the surveyed liveness arguments. 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 8, 10, and 18 are examples of new ODE liveness proof rules that can be derived and justified using our uniform approach.

All proofs are in the companion report [28], together with counterexamples for the soundness errors listed in Table 1.

2 Background

This section reviews the syntax and semantics of dL, focusing on its continuous fragment which has a complete axiomatization for ODE invariants [20]. Full presentations of dL, including its discrete fragment, are available elsewhere [17,19].

[1] This property has also been called, e.g., *eventuality* [23,25] and *reachability* [27]. To minimize ambiguity, this paper refers to the property as *liveness*, with a precise formal definition in Section 2. Other advanced notions of liveness for ODEs are discussed in Section 6, although their formal deduction is left for future work.

2.1 Syntax

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

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

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

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

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. We focus 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 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 written as $x' = f(x)$.

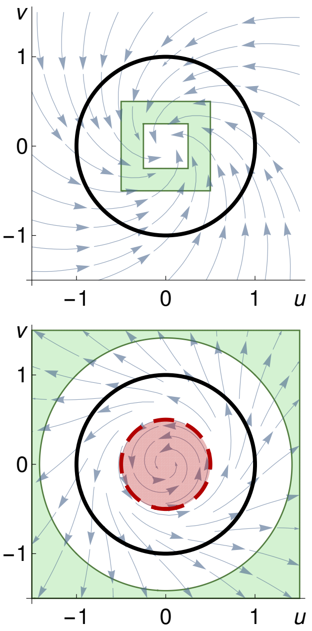


Fig. 1. Visualization of α_l (above) and α_n (below). Solutions of α_l globally spiral towards the origin. In contrast, solutions of α_n spiral inwards within the inner red disk (dashed boundary), but spiral outwards otherwise. For both ODEs, solutions starting on the black unit circle eventually enter their respective shaded green goal regions.

Two running example ODEs are visualized in Fig. 1 with directional arrows corresponding to their RHS evaluated at points on the plane. The first ODE, $\alpha_l \equiv u' = -v - u, v' = u - v$, is *linear* because its RHS depends linearly on u, v. The second ODE, $\alpha_n \equiv u' = -v - u(\frac{1}{4} - u^2 - v^2), v' = u - v(\frac{1}{4} - u^2 - v^2)$, is *non-linear*. The non-linearity of α_n results in more complex behavior for its solutions, e.g., the difference in spiraling behavior shown in Fig. 1. In fact, solutions of α_n blow up in finite time iff they start outside the disk characterized by $u^2 + v^2 \leq \frac{1}{4}$. Finite time blow up is impossible for linear ODEs like α_l [5,29].

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. These restrictions are always stated explicitly and are also indicated as arguments[2] to terms (or formulas), e.g., $p()$ means the term p does not mention any of $x_1, \ldots, x_n$ free, while $P(x)$ means the formula P may mention all of them.

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 formula ϕ is 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.[3] Let $\omega \in \mathbb{S}$ and $\boldsymbol{\varphi} : [0, T) \to \mathbb{S}$ (for some $0 < T \leq \infty$), be the unique, right-maximal solution [5,29] to the ODE $x' = f(x)$ with initial value $\boldsymbol{\varphi}(0) = \omega$:

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

Informally, $[x' = f(x) \,\&\, Q]\phi$ 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. For the running example, Fig. 1 suggests that formulas[4] $\langle\alpha_l\rangle\big(\frac{1}{4} \leq \|(u, v)\|_\infty \leq \frac{1}{2}\big)$ and $\langle\alpha_n\rangle u^2 + v^2 \geq 2$ are true for initial states ω on the unit circle. These liveness properties are rigorously proved in Examples 6 and 11 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 $x = (x_1, \ldots, x_n)$ change along the solution $\boldsymbol{\varphi}$ it may also be viewed geometrically as a trajectory in $\mathbb{R}^n$, dependent on the initial values of the constant *parameters* y. Similarly, the value of terms and formulas depends only on the values of their free variables [17]. Thus, terms (or formulas) whose free variables are all parameters for $x' = f(x)$ also have 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

[2] This understanding of variable dependencies is made precise using function and predicate symbols in dL's uniform substitution calculus [17].

[3] The semantics of dL formulas is defined compositionally elsewhere [17,19].

[4] Here, $\|(u, v)\|_\infty$ denotes the L^∞ norm. The inequality $\|(u, v)\|_\infty \leq \frac{1}{2}$ is expressible in first-order real arithmetic as $u^2 \leq \frac{1}{4} \land v^2 \leq \frac{1}{4}$ (similarly for $\frac{1}{4} \leq \|(u, v)\|_\infty$).

and proof rules in this paper. In the report [28], a more general definition of these side conditions is given for formulas ϕ that mention parameters y. These side conditions are decidable [3] when ϕ is a formula of first-order real arithmetic and there are simple syntactic criteria for checking if they hold [28].

Formula ϕ is valid iff $[\![\phi]\!] = \mathbb{S}$, i.e., ϕ is true in all states. In particular, if the formula $I \rightarrow [x' = f(x) \,\&\, Q]I$ 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.

2.3 Proof Calculus

All derivations are presented in a classical sequent calculus with usual rules for manipulating logical connectives and sequents. The semantics of *sequent* $\Gamma \vdash \phi$ is equivalent to the formula $(\bigwedge_{\psi \in \Gamma} \psi) \rightarrow \phi$ and 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 [3] so we assume such a decision procedure and label proof steps with $\mathbb{R}$ when they follow from real arithmetic. An axiom (schema) is *sound* iff all instances of the axiom 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 base dL axiomatization ensures that derived axioms and proof rules are sound [17,19,20].

The dL proof calculus (briefly recalled below) is *complete* for ODE invariants [20], i.e., any true ODE invariant expressible in first-order real arithmetic can be proved in the calculus. The proof rule $\text{dI}_{\succcurlyeq}$ (below) uses the *Lie derivative* of polynomial p with respect to the ODE $x' = f(x)$, which is defined as $\mathcal{L}_{f(x)}(p) \overset{\text{def}}{=} \sum_{x_i \in x} \frac{\partial p}{\partial x_i} f_i(x)$. 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. They are provably definable in dL using differentials [17]. 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 [17,19,20]). *The following are sound axioms and proof rules of* dL.

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

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

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

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

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

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 $\mathrm{dI}_{\succcurlyeq}$ says 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 says that if we 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; differential weakening dW says that postcondition P is always satisfied along solutions if it is already implied by the domain constraint. Liveness arguments are often based on analyzing the duration that solutions of the ODE are followed. Rule dGt is a special instance of the more general differential ghosts rule [17,19,20] which allows *new* auxiliary variables to be introduced for the purposes of proof. It augments the ODE $x' = f(x)$ with an additional differential equation, $t' = 1$, so that the (fresh) variable t, with initial value $t = 0$, tracks the progress of time. Using dW,K,$\langle\cdot\rangle$, the final two monotonicity proof rules M[$'$],M$\langle{}'\rangle$ for differential equations are derivable. They strengthen the postcondition from P to R, assuming domain constraint Q, for the box and diamond modalities respectively.

Throughout this paper, we present proof rules, e.g., dW, that discard all assumptions Γ on initial states when moving from conclusion to the premises. Intuitively, 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 [19]. These additional constant contexts are useful when working with assumptions on symbolic parameters e.g., $v() > 0$ to represent a (constant) positive velocity.

3 Liveness via Box Refinements

Suppose we already know an initial liveness property $\langle x' = f(x) \,\&\, Q_0\rangle P_0$ 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:

$$\langle x' = f(x) \,\&\, Q_0\rangle P_0 \rightarrow \langle x' = f(x) \,\&\, Q\rangle P \tag{1}$$

Proving implication (1) *refines* the initial liveness property to the desired one. Our approach is built on refinement axioms that conclude such implications from box modality formulas. The following are two basic derived refinement axioms:

Lemma 2 (Diamond refinement axioms). *The following $\langle\cdot\rangle$ refinement axioms are derivable in* dL.

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

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

In axiom K$\langle\&\rangle$, formula $[x' = f(x) \,\&\, Q \land \neg P]\neg G$ says the solution cannot get to G before getting to P as G never happens while $\neg P$ holds. In axiom DR$\langle\cdot\rangle$, formula $[x' = f(x) \,\&\, R]Q$ says that the ODE solution never leaves Q while staying in R, so the solution getting to P within R implies that it also gets to P within Q. These axioms prove implication (1) in just one refinement step. Logical implication is transitive though, so we can also chain a longer sequence of such steps to prove implication (1). This is shown in (2), with neighboring implications informally chained together for illustration:

$$\begin{aligned}\langle x' = f(x) \,\&\, Q_0\rangle P_0 \overbrace{\rightarrow}^{\text{DR}\langle\cdot\rangle \text{ with } [x'=f(x)\,\&\,Q_1]Q_0} \langle x' = f(x) \,\&\, Q_1\rangle P_0 \overbrace{\rightarrow}^{\text{K}\langle\&\rangle \text{ with } [x'=f(x)\,\&\,Q_1\land\neg P_1]\neg P_0} \langle x' = f(x) \,\&\, Q_1\rangle P_1 \\ \rightarrow \cdots \rightarrow \langle x' = f(x) \,\&\, Q\rangle P\end{aligned} \tag{2}$$

The chain of refinements (2) proves the desired implication (1), but to formally conclude the liveness property $\langle x' = f(x) \,\&\, Q\rangle P$, we still need to prove the hypothesis $\langle x' = f(x) \,\&\, Q_0\rangle P_0$ on the left of the implication. The following axioms provide a means of formally establishing such an initial liveness property:

Lemma 3 (Existence axioms). *The following existence axioms are sound. In both axioms, $p()$ is constant for the ODE $x' = f(x), t' = 1$. In axiom GEx, the ODE $x' = f(x)$ is globally Lipschitz continuous. In axiom BEx, the formula $B(x)$ characterizes a bounded set over variables x.*

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

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

Axioms GEx,BEx are stated for ODEs with an explicit time variable t, where $x' = f(x)$ does not mention t. Within proofs, these axioms can be accessed after using rule dGt to add a fresh time variable t. Solutions of globally Lipschitz ODEs exist for all time so axiom GEx says that along such solutions, the value of time variable t eventually exceeds that of the constant term $p()$.[5] This global Lipschitz continuity condition is satisfied e.g., by α_l, and more generally by linear ODEs of the form $x' = Ax$, where A is a matrix of (constant) parameters [5]. Global Lipschitz continuity is a strong requirement that does not hold even for simple non-linear ODEs like α_n, which only have short-lived solutions (see Fig. 1). This phenomenon, where the right-maximal ODE solution $\boldsymbol{\varphi}$ is only defined on a finite time interval $[0, T)$ with $T < \infty$, is known as *finite time blow up of solutions* [5]. Axiom BEx removes the global Lipschitz continuity requirement 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 $B(x)$.

Refinement with axiom DR$\langle\cdot\rangle$ requires proving the formula $[x' = f(x) \,\&\, R]Q$. Naïvely, we 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:

DR$\langle\cdot\rangle$↯ $[x' = f(x) \,\&\, R \land \neg P]Q \rightarrow \big(\langle x' = f(x) \,\&\, R\rangle P \rightarrow \langle x' = f(x) \,\&\, Q\rangle P\big)$

[5] It is important for soundness that $p()$ is constant for the ODE, e.g., instances of axiom GEx with postcondition $t > 2t$ are clearly not valid.

This conjectured axiom is unsound (indicated by $\lightning$) as the solution could sneak out of Q 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 refinement axioms). *The following topological $\langle\cdot\rangle$ refinement axioms are sound. In axiom COR, P, Q either both characterize topologically open or both characterize topologically closed sets over variables x.*

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

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

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 additional topological side conditions on formulas P, Q so it can only be used when these conditions are met. Axiom SAR applies more generally but only assumes the less informative formula $\neg(P \land Q)$ in the domain constraint for the box modality formula in the refinement. Its proof crucially relies on Q being a formula of real arithmetic so that the set it characterizes has tame topological behavior [3], see the proof in the report [28] for more details.[6]

4 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.

4.1 Differential Variants

A fundamental technique for verifying liveness of discrete loops is the identification of a loop variant, i.e., a quantity that decreases monotonically across each loop iteration. Differential variants [15] are their continuous analog:

Corollary 5 (Atomic differential variants [15]). *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 dV$_{\succcurlyeq}$, $x' = f(x)$ is globally Lipschitz continuous.*

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

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

[6] By topological considerations similar to COR, axiom SAR is also sound if it requires that the formula P (or resp. Q) characterizes a topologically closed (resp. open) set over the ODE variables x. These additional cases are also proved in the report [28] without relying on the fact that Q is a formula of real arithmetic.

Proof Sketch ([28]). Rule $\mathrm{dV}^*_{\succcurlyeq}$ derives by using axiom $\mathrm{K}\langle\&\rangle$ with the choice of formula $G \equiv p_0()+\varepsilon()t>0$:

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

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

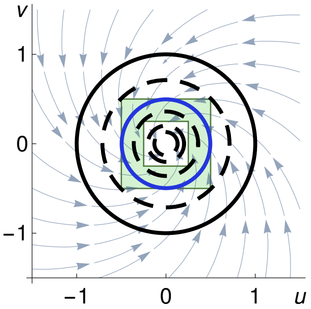
$$\mathrm{M}[']\ \dfrac{\mathrm{dI}_{\succcurlyeq}\ \dfrac{\neg(p \succcurlyeq 0) \vdash \dot{p} \ge \varepsilon()}{\Gamma, p = p_0(), t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg(p \succcurlyeq 0)]p \ge p_0() + \varepsilon()t}}{\Gamma, p = p_0(), t = 0 \vdash [x' = f(x), t' = 1 \,\&\, \neg(p \succcurlyeq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

Rule $\mathrm{dV}_{\succcurlyeq}$ is derived in the report [28] as a corollary of rule $\mathrm{dV}^*_{\succcurlyeq}$. It uses the global existence axiom GEx and rule dGt to introduce the time variable. □

The premises of both rules require a constant (positive) lower bound on the Lie derivative $\dot{p}$ which ensures that the value of p strictly increases along solutions to the ODE, eventually becoming non-negative. Soundness of both rules therefore crucially requires that ODE solutions exist for sufficiently long for p to become non-negative. This is usually left as a soundness-critical side condition in liveness proof rules [15,25], but such a side condition is antithetical to approaches for minimizing the soundness-critical core in implementations [17] because it requires checking the (semantic) condition that solutions exist for sufficient duration. The conclusion of rule $\mathrm{dV}^*_{\succcurlyeq}$ formalizes this side condition as an assumption while rule $\mathrm{dV}_{\succcurlyeq}$ uses global Lipschitz continuity of the ODEs to show it. All subsequent proof rules can also be presented with sufficient duration assumptions like $\mathrm{dV}^*_{\succcurlyeq}$ but these are omitted for brevity.

Example 6. Rule $\mathrm{dV}_{\succcurlyeq}$ enables a liveness proof for the linear ODE α_l as suggested by Fig. 1. 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 $u^2 + v^2 = \frac{1}{4}$ which is contained within the green goal region. 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 $u^2+v^2 \le \frac{1}{4}$ (see Corollary 7). The postcondition is rearranged before $\mathrm{dV}_{\succcurlyeq}$ is used with $\varepsilon() = \frac{1}{2}$. Its premise proves with $\mathbb{R}$ 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 $\frac{1}{2}$ with assumption $\frac{1}{4}{-}(u^2{+}v^2) < 0$.

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



The Lie derivative calculation shows that the value of u^2+v^2 decreases along solutions of α_l, as visualized by the shrinking (dashed) circles. However, the rate of shrinking converges to zero as solutions approach the origin, so solutions *never* reach the origin in finite time! This is why $\mathrm{dV}^*_{\succcurlyeq}$,$\mathrm{dV}_{\succcurlyeq}$ need a *constant* positive lower bound on the Lie derivative $\dot{p} \geq \varepsilon()$ instead of merely requiring $\dot{p} > 0$.

It is instructive to examine the chain of refinements (2) underlying the proof. The first $\mathrm{dV}_{\succcurlyeq}$ step refines the initial liveness property from GEx, i.e., that solutions exist globally (so, for at least $\frac{3}{4} / \frac{1}{2} = \frac{3}{2}$ time), to the property $u^2+v^2 \leq \frac{1}{4}$. Subsequent refinement steps can be read off from the proof steps above:

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

The latter two steps illustrate the idea behind the next two surveyed proof rules. In the original presentation [27], 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 the report [28] for counterexamples.

Corollary 7 (Equational differential variants [27]). *The following proof rules are derivable in* dL*. Term $\varepsilon()$ is constant for ODE $x' = f(x)$ and the ODE is globally Lipschitz continuous for both rules.*

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

The view of $\mathrm{dV}_{\succcurlyeq}$ as a refinement of GEx immediately yields generalizations to higher Lie derivatives. For example, it suffices that *any* higher Lie derivative $\dot{p}^{(k)}$ is bounded below by a positive constant rather than just the first:

Corollary 8 (Atomic higher differential variants). *The following proof rule (where $\succcurlyeq$ is either $\geq$ or $>$) is derivable in* dL*. Term $\varepsilon()$ is constant for ODE $x' = f(x)$ and the ODE is globally Lipschitz continuous.*

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

Proof Sketch ([28]). Since $\dot{p}^{(k)}$ is strictly positive, the (lower) Lie derivatives of p all eventually become positive. This derives using a sequence of dC,$\mathrm{dI}_{\succcurlyeq}$ steps. □

4.2 Staging Sets

The idea behind *staging sets* [25] is to use an intermediary staging set formula S that *can only be left by entering the goal region P*. This staging property is expressed by the box modality formula $[x' = f(x) \,\&\, \neg P]S$ and is formally justified as a refinement using axiom $\mathrm{K}\langle\&\rangle$ with $G \equiv \neg S$.

Corollary 9 (Staging sets [25]). *The following proof rule is derivable in* dL*. Term $\varepsilon()$ is constant for ODE $x' = f(x)$, which is globally Lipschitz continuous.*

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

In rule SP, the staging set formula S provides a choice of intermediary between the differential variant p and the desired postcondition P. Proof rules can be significantly simplified by choosing S with desirable topological properties. All proof rules derived so far either have an explicit sufficient duration assumption (like $\text{dV}^*_{\succcurlyeq}$) or use axiom GEx by assuming that ODEs are globally Lipschitz. To make use of axiom BEx, an alternative is to choose staging set formulas $S(x)$ that characterize a bounded (or even compact) set over the variables x.

Corollary 10 (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.*

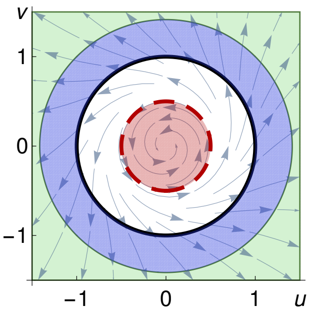
$$\text{SP}_b\,\frac{\Gamma \vdash [x' = f(x)\,\&\,\neg P]S \quad S \vdash \dot{p} \geq \varepsilon()}{\Gamma, \varepsilon() > 0 \vdash \langle x' = f(x)\rangle P} \qquad \text{SP}_c\,\frac{\Gamma \vdash [x' = f(x)\,\&\,\neg P]S \quad S \vdash \dot{p} > 0}{\Gamma \vdash \langle x' = f(x)\rangle P}$$

Proof Sketch ([28]). Rule SP$_b$ derives using BEx and 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 a compact domain attain their extrema. □

Example 11. Liveness for the non-linear ODE α_n (as suggested by Fig. 1) is proved using rule SP$_c$ by choosing the staging set formula $S \equiv 1 \leq u^2 + v^2 \leq 2$ (blue annulus) and the differential variant $p = u^2 + v^2$. 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 (abbreviated ①) 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 $u^2+v^2 \geq 2$. Its (elided) invariance proof is easy [20].

$$\text{SP}_c\,\dfrac{\text{①} \qquad {}^{\mathbb{R}}\dfrac{*}{S \vdash \dot{p} > 0}}{u^2+v^2=1 \vdash \langle\alpha_n\rangle u^2+v^2 \geq 2}$$

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



There are two subtleties to highlight in this proof. First, S characterizes a compact, hence bounded, set (as required by rule SP$_c$). Solutions of α_n can blow up in finite time which necessitates the use of BEx for proving its liveness properties. Second, S is cleverly chosen to *exclude* the red disk (dashed boundary) characterized by $u^2+v^2 \leq \frac{1}{4}$. As mentioned earlier, 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 (2) behind this proof can be seen from the derivation of rules SP$_b$,SP$_c$ in the report [28]. It starts from the initial liveness property BEx (with time bound $1 \,/\, \frac{3}{2} = \frac{2}{3}$) and uses two K⟨&⟩ refinement steps, first showing that the staging set is left ($\langle\alpha_n\rangle\neg S$), then showing the desired liveness property:

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

The use of axiom BEx is subtle and is sometimes overlooked in surveyed liveness arguments. For example, [23, Remark 3.6] incorrectly claims that their liveness argument works without assuming that the relevant sets are bounded. The following proof rule derives from SP_c and adapts ideas from [24, Theorem 2.4, Corollary 2.5], but formula K in the original presentation is only assumed to characterize a closed rather than compact set; the proofs (correctly) use the fact that the set is bounded but this assumption is not made explicit [24].

Corollary 12 (Set Lyapunov functions [24]). *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.*

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

5 Liveness With Domain Constraints

This section presents proof rules for liveness properties $x' = f(x) \,\&\, Q$ with domain constraint Q. Axiom $\mathrm{DR}\langle\cdot\rangle$ provides direct generalizations of the proof rules from Section 4 with the following derivation choosing $R \equiv \mathit{true}$:

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

This extends all chains of refinements (2) from Section 4 with an additional step:

$$\cdots \rightarrow \langle x' = f(x)\rangle P \overset{\mathrm{DR}\langle\cdot\rangle}{\rightarrow} \langle x' = f(x) \,\&\, Q\rangle P$$

Liveness arguments become much more intricate when attempting to generalize beyond $\mathrm{DR}\langle\cdot\rangle$, e.g., recall the unsound conjecture $\mathrm{DR}\langle\cdot\rangle\lightning$. Indeed, unlike the technical glitches of Section 4, our survey uncovers subtle soundness-critical errors here. With our deductive approach, these intricacies are isolated to the topological axioms (Lemma 4) which have been proved sound once and for all. As before, errors and omissions in the surveyed techniques are highlighted in blue.

5.1 Topological Proof Rules

The first proof rule generalizes differential variants to handle domain constraints:

Corollary 13 (Atomic differential variants with domains [15]). *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 is globally Lipschitz continuous. Formula Q characterizes a closed (resp. open) set when $\succcurlyeq$ is $\geq$ (resp. $>$).*

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

Proof Sketch ([28]). 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:

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

The right premise follows similarly to $\mathrm{dV}_{\succcurlyeq}$ although it uses an intervening dC step to add Q to the antecedents. □

The original presentation of rule $\mathrm{dV}^{*}_{\succcurlyeq}$ [15] omits the highlighted assumption $\neg(p \succcurlyeq 0)$. This premise is needed for the COR step and the rule is unsound without it. In addition, it uses a form of syntactic weak negation [15], which is also unsound for open postconditions, as pointed out earlier [25]. See the report [28] for counterexamples. Our presentation of $\mathrm{dV}_{\succcurlyeq}\&$ recovers soundness by adding topological restrictions on the domain constraint Q.

The next two corollaries similarly make use of COR to derive the proof rule $\mathrm{dV}^{M}_{=}\&$ [27] and the adapted rule SLyap& [24]. They respectively generalize $\mathrm{dV}^{M}_{=}$ and SLyap from Section 4 to handle domain constraints. The technical glitches in their original presentations [24,27], which were identified in Section 4, remain highlighted here:

Corollary 14 (Equational differential variants with domains [27]). *The following proof rules are derivable in* dL. *Term* $\varepsilon()$ *is constant for the ODE* $x' = f(x)$ *and the ODE is globally Lipschitz continuous in both rules. Formula* Q *characterizes a closed set over variables* x.

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

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

Corollary 15 (Set Lyapunov functions with domains [24]). *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.*

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

The staging sets with domain constraints proof rule SP& [25] uses axiom SAR:

Corollary 16 (Staging sets with domains [25]). *The following proof rule is derivable in* dL. *Term* $\varepsilon()$ *is constant for ODE* $x' = f(x)$ *and the ODE is globally Lipschitz continuous.*

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

The rules derived in Corollaries 13–16 demonstrate the flexibility of our refinement approach for deriving surveyed liveness arguments as proof rules. Our approach is not limited to these surveyed arguments because refinement steps can be freely mixed-and-matched for specific liveness questions.

Example 17. The liveness property $u^2+v^2=1 \rightarrow \langle\alpha_n\rangle u^2+v^2 \geq 2$ was proved in Example 11 using the staging set formula $S \equiv 1 \leq u^2+v^2 \leq 2$. Since S and $u^2+v^2 \geq 2$ both characterize closed sets, axiom COR extends the chain of refinements (2) from Example 11 to show a stronger liveness property for α_n:

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

Formula $\widetilde{S} \equiv 1 \leq u^2+v^2 < 2$ also proves Example 11 but does *not* characterize a closed set. Thankfully, the careful topological restriction of COR prevents us from unsoundly concluding the property $u^2+v^2=1 \rightarrow \langle\alpha_n \,\&\, \widetilde{S}\rangle u^2+v^2 \geq 2$. This latter property is unsatisfiable because $\widetilde{S}$ does not overlap with $u^2+v^2 \geq 2$.

The refinement approach also enables discovery of new, general liveness proof rules by combining refinement steps in alternative ways. As an example, the following chimeric proof rule combines ideas from Corollaries 8, 10, and 16:

Corollary 18 (Combination proof rule). *The following proof rule is derivable in* dL*. Formula S characterizes a compact set over variables x.*

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

Our logical approach derives even complicated proof rules like $\mathrm{SP}^k_c\&$ from a small set of sound logical axioms, which ensures their correctness. The proof rule $\mathrm{E}_c\&$ below derives from $\mathrm{SP}^k_c\&$ (for $k=1$) and is an adapted version of the liveness argument from [23, Theorem 3.5]. In the original presentation, additional restrictions are imposed on the sets characterized by Γ, P, Q, and different conditions are given compared to the left premise of $\mathrm{E}_c\&$ (highlighted below). These original conditions are overly permissive as they are checked on a smaller set than necessary for soundness. See the report [28] for counterexamples.

Corollary 19 (Compact eventuality [23]). *The following proof rule is derivable in* dL*. Formula $Q \land \neg P$ characterizes a compact set over variables x.*

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

6 Related Work

Liveness Proof Rules. The liveness arguments surveyed in this paper were originally presented in various notations, ranging from proof rules [15,25,27] to other mathematical notation [22,23,24,25]. All of them were justified directly through semantical (or mathematical) means. We unify (and correct) all of these arguments and present them as dL proof rules which are syntactically derived with our refinement-based approach from dL axioms.

Other Liveness Properties. The liveness property studied in this paper is the continuous analog of *eventually* [12] or *eventuality* [23,25] from temporal logics. In discrete settings, temporal logic specifications give rise to a zoo of liveness properties [12]. In continuous settings, *weak eventuality* (requiring *almost all* initial states to reach the goal region) and *eventuality-safety* have been studied [22,23]. In (continuous) adversarial settings, *differential game variants* [18] enable proofs of (Angelic) 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) [5,24]. For hybrid systems, various authors have proposed generalizations of classical asymptotic stability, such as *persistence* [26], *stability* [21], and *inevitability* [7]. *Controlled* versions of these properties are also of interest, e.g., *(controlled) reachability and attractivity* [1,27]. Eventuality(-like) properties are fundamental to all of these advanced liveness properties. The formal understanding of eventuality in this paper is therefore a key step towards enabling formal analysis of more advanced liveness properties.

Automated Liveness Proofs. Automated reachability analysis tools [4,8] can also be used for liveness verification. 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 [26] (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 $\mathcal{U}$ [10] (if $\mathcal{U}$ is non-empty). Neither approach handles domain constraints directly [10,26] 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 automated. Lyapunov functions guaranteeing (asymptotic) stability can be found by sum-of-squares (SOS) optimization [14]. Liveness arguments can be similarly combined with SOS optimization to find suitable differential variants [22,23]. Other approaches are possible, e.g., a constraint solving-based approach can be used for finding so-called *set Lyapunov functions* [24]. Crucially, automated approaches must be based on sound liveness arguments. The correct justification of these arguments is precisely what our approach enables.

7 Conclusion

This paper presents a refinement-based approach for proving liveness for ODEs. Exploration of new ODE liveness proof rules is enabled by piecing together refinement steps identified through our approach. Given its wide applicability and correctness guarantees, our approach is a suitable framework for justifying ODE liveness arguments, even for readers less interested in the logical aspects.

Acknowledgments. We thank Katherine Cordwell, Frank Pfenning, Andrew Sogokon, and the anonymous reviewers for their feedback on this paper. 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.

References

1. Abate, A., D'Innocenzo, A., Benedetto, M.D.D., Sastry, S.: Understanding deadlock and livelock behaviors in hybrid control systems. Nonlinear Anal. Hybrid Syst. **3**(2), 150 – 162 (2009). https://doi.org/10.1016/j.nahs.2008.12.005
2. Alur, R.: Principles of Cyber-Physical Systems. MIT Press (2015)
3. Bochnak, J., Coste, M., Roy, M.F.: Real Algebraic Geometry. Springer, Heidelberg (1998). https://doi.org/10.1007/978-3-662-03718-8
4. Chen, X., Ábrahám, E., Sankaranarayanan, S.: Flow*: An analyzer for non-linear hybrid systems. In: Sharygina, N., Veith, H. (eds.) CAV. LNCS, vol. 8044, pp. 258–263. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39799-8_18
5. Chicone, C.: Ordinary Differential Equations with Applications. Springer, New York, second edn. (2006). https://doi.org/10.1007/0-387-35794-7
6. Doyen, L., Frehse, G., Pappas, G.J., Platzer, A.: Verification of hybrid systems. In: Clarke, E.M., Henzinger, T.A., Veith, H., Bloem, R. (eds.) Handbook of Model Checking, pp. 1047–1110. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-10575-8_30
7. Duggirala, P.S., Mitra, S.: Lyapunov abstractions for inevitability of hybrid systems. In: Dang, T., Mitchell, I.M. (eds.) HSCC. pp. 115–124. ACM, New York (2012). https://doi.org/10.1145/2185632.2185652
8. Frehse, G., Guernic, C.L., Donzé, A., Cotton, S., Ray, R., Lebeltel, O., Ripado, R., Girard, A., Dang, T., Maler, O.: SpaceEx: Scalable verification of hybrid systems. In: Gopalakrishnan, G., Qadeer, S. (eds.) CAV. LNCS, vol. 6806, pp. 379–395. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-22110-1_30
9. Ghorbal, K., Platzer, A.: Characterizing algebraic invariants by differential radical invariants. In: Ábrahám, E., Havelund, K. (eds.) TACAS. LNCS, vol. 8413, pp. 279–294. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54862-8_19
10. Goubault, E., Putot, S.: Forward inner-approximated reachability of non-linear continuous systems. In: Frehse, G., Mitra, S. (eds.) HSCC. pp. 1–10. ACM, New York (2017). https://doi.org/10.1145/3049797.3049811
11. Liu, J., Zhan, N., Zhao, H.: Computing semi-algebraic invariants for polynomial dynamical systems. In: Chakraborty, S., Jerraya, A., Baruah, S.K., Fischmeister, S. (eds.) EMSOFT. pp. 97–106. ACM, New York (2011). https://doi.org/10.1145/2038642.2038659
12. Manna, Z., Pnueli, A.: The Temporal Logic of Reactive and Concurrent Systems - Specification. Springer, New York (1992). https://doi.org/10.1007/978-1-4612-0931-7
13. Owicki, S.S., Lamport, L.: Proving liveness properties of concurrent programs. ACM Trans. Program. Lang. Syst. **4**(3), 455–495 (1982). https://doi.org/10.1145/357172.357178
14. Papachristodoulou, A., Prajna, S.: On the construction of Lyapunov functions using the sum of squares decomposition. In: CDC. vol. 3, pp. 3482–3487. IEEE (2002). https://doi.org/10.1109/CDC.2002.1184414
15. Platzer, A.: Differential-algebraic dynamic logic for differential-algebraic programs. J. Log. Comput. **20**(1), 309–352 (2010). https://doi.org/10.1093/logcom/exn070
16. Platzer, A.: Logics of dynamical systems. In: LICS. pp. 13–24. IEEE (2012). https://doi.org/10.1109/LICS.2012.13
17. Platzer, A.: A complete uniform substitution calculus for differential dynamic logic. J. Autom. Reas. **59**(2), 219–265 (2017). https://doi.org/10.1007/s10817-016-9385-1

18. Platzer, A.: Differential hybrid games. ACM Trans. Comput. Log. **18**(3), 19:1–19:44 (2017). https://doi.org/10.1145/3091123
19. Platzer, A.: Logical Foundations of Cyber-Physical Systems. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-63588-0
20. Platzer, A., Tan, Y.K.: Differential equation axiomatization: The impressive power of differential ghosts. In: Dawar, A., Grädel, E. (eds.) LICS. pp. 819–828. ACM, New York (2018). https://doi.org/10.1145/3209108.3209147
21. Podelski, A., Wagner, S.: Model checking of hybrid systems: From reachability towards stability. In: Hespanha, J.P., Tiwari, A. (eds.) HSCC. LNCS, vol. 3927, pp. 507–521. Springer, Heidelberg (2006). https://doi.org/10.1007/11730637_38
22. Prajna, S., Rantzer, A.: Primal-dual tests for safety and reachability. In: Morari, M., Thiele, L. (eds.) HSCC. LNCS, vol. 3414, pp. 542–556. Springer, Heidelberg (2005). https://doi.org/10.1007/978-3-540-31954-2_35
23. Prajna, S., Rantzer, A.: Convex programs for temporal verification of nonlinear dynamical systems. SIAM J. Control Optim. **46**(3), 999–1021 (2007). https://doi.org/10.1137/050645178
24. Ratschan, S., She, Z.: Providing a basin of attraction to a target region of polynomial systems by computation of Lyapunov-like functions. SIAM J. Control Optim. **48**(7), 4377–4394 (2010). https://doi.org/10.1137/090749955
25. Sogokon, A., Jackson, P.B.: Direct formal verification of liveness properties in continuous and hybrid dynamical systems. In: Bjørner, N., de Boer, F.S. (eds.) FM. LNCS, vol. 9109, pp. 514–531. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-19249-9_32
26. Sogokon, A., Jackson, P.B., Johnson, T.T.: Verifying safety and persistence in hybrid systems using flowpipes and continuous invariants. J. Autom. Reas. (to appear). https://doi.org/10.1007/s10817-018-9497-x
27. Taly, A., Tiwari, A.: Switching logic synthesis for reachability. In: Carloni, L.P., Tripakis, S. (eds.) EMSOFT. pp. 19–28. ACM, New York (2010). https://doi.org/10.1145/1879021.1879025
28. Tan, Y.K., Platzer, A.: An axiomatic approach to liveness for differential equations. CoRR **abs/1904.07984** (2019)
29. Walter, W.: Ordinary Differential Equations. Springer, New York (1998). https://doi.org/10.1007/978-1-4612-0601-9