Axiomatization of Compact Initial Value Problems: Open Properties

ANDRÉ PLATZER, Informatics Department, Karlsruhe Institute of Technology, Karlsruhe, Germany
LONG QIAN, Mathematical Sciences, Carnegie Mellon University, Pittsburgh, United States

This article proves the completeness of an axiomatization for *initial value problems (IVPs)* with compact initial conditions and compact time horizons for bounded open safety, open liveness and existence properties. Completeness systematically reduces the proofs of these properties to a complete axiomatization for differential equation invariants. This result unifies symbolic logic and numerical analysis by a computable procedure that generates symbolic proofs with differential invariants for rigorous error bounds of numerical solutions to polynomial initial value problems. The procedure is modular and works for all polynomial IVPs with rational coefficients and initial conditions and symbolic parameters constrained to compact sets. Furthermore, this article discusses generalizations to IVPs with initial conditions/symbolic parameters that are not necessarily constrained to compact sets, achieved through the derivation of fully symbolic axioms/proof-rules based on the axiomatization.

CCS Concepts: • **Mathematics of computing** → **Ordinary differential equations**; • **Theory of computation** → **Timed and hybrid models**; *Proof theory*; **Modal and temporal logics**; *Programming logic;*

Additional Key Words and Phrases: Differential equation axiomatization, invariants, differential dynamic logic

ACM Reference Format:
André Platzer and Long Qian. 2025. Axiomatization of Compact Initial Value Problems: Open Properties. *J. ACM* 72, 6, Article 41 (November 2025), 51 pages. https://doi.org/10.1145/3763228

1 Introduction

Differential equations and their analysis play a fundamental role in **cyber-physical systems** (**CPS**) correctness [3, 42]. Classically, the descriptive power of differential equations exceeds the analytic power of differential equations [45], since solutions of differential equations are usually significantly more complicated, not computable in closed form or less analyzable than the differential equations themselves. That is why Henri Poincaré in 1881 called for the qualitative theory of differential equations [46], i.e., the study of differential equations directly via their differential equations rather than indirectly via their solutions. The logical foundations of the qualitative theory of differential equation invariants have been discovered in a complete axiomatization of differential equation invariants [45]. In that axiomatization, every true (semialgebraic) invariant of a (polynomial)

Funding has been provided by an Alexander von Humboldt Professorship and the National Science Foundation under Grant No. CCF 2220311.

Authors' Contact Information: André Platzer, Informatics Department, Karlsruhe Institute of Technology, Karlsruhe, Germany; e-mail: platzer@kit.edu; Long Qian, Mathematical Sciences, Carnegie Mellon University, Pittsburgh, Pennsylvania, United States; e-mail: longq@andrew.cmu.edu.

ACM 0004-5411/2025/11-ART41
https://doi.org/10.1145/3763228

differential equation system can be proved effectively in differential dynamic logic dL [40, 41], and every false invariant can be disproved, thereby leading to a purely logic-based proof-producing decision procedure. But in CPS applications, even just finding invariants is challenging. A CPS starts at an initial state within an initial region and follows a differential equation, where the question is whether it then always stays safe, which may still be far from an invariance question if the initial and safe region are very different.

This article, thus, studies the logical foundations of *(compact)* ***Initial Value Problems*** (***IVPs***). In a (compact) IVP a (polynomial) differential equation on a compact time interval (with rational endpoints) starts from some initial value in a compact semialgebraic set. The (semi)algebraic shape of those syntactic expressions ensures that the required concepts are definable in first-order logic of real arithmetic ($\mathsf{FOL}_{\mathbb{R}}$). IVPs are one of the most fundamental problems studied in numerical analysis [34]. Unlike in numerical algorithms for classical IVPs [24], however, the initial state is not given numerically as a single concrete vector of numbers such as $(0, 4.2, -6)$, because those are typically not known when analyzing *all* possible behavior of a CPS. Instead, *compact IVPs* generalize classical IVPs by supporting a compact initial region from which the symbolic initial state is selected nondeterministically.

This article proves the completeness of dL's axiomatization [41, 45, 52] for bounded open safety, open liveness and existence properties of compact IVPs such that *every* true such property can be proved. Moreover, these completeness theorems are effective, i.e., a direct computable procedure produces the dL proofs based on dL's effective axiomatization of differential equation invariants [45]. In order to achieve completeness and thereby complete Henri Poincaré's qualitative theory of differential equations for these properties of compact IVPs, this article will do something superficially frivolous: the completeness proofs will use solutions of IVPs, but ultimately of symbolic IVPs and only to guide the proofs of the required invariance properties of the IVPs. Besides, these solutions used for the guidance of the proofs will be approximate solutions only, not true solutions. And, indeed, Henri Poincaré was still correct that both the true solution and their approximations are more complicated than the IVP, and that the indirect symbolic invariance proofs that this article's procedure constructs are both simpler and the key to the complete theory of IVPs. In fact, one of the hard parts will be the need to prove that sufficient control can be exerted over the accumulating approximation errors to provide rigorous symbolic proofs with sufficiently small errors to justify *every* true bounded open safety, open liveness and existence property of a compact IVP.

While this article and its results are proof-theoretical in nature, they can also be viewed through a practically motivated angle. The problem of reachability analysis for ODEs and hybrid dynamical systems over a compact time horizon is an important area of study in the safety verification of CPS [3, 42], particularly for bounded model checking [25]. Consequently, practical tools [15, 16, 31] have been developed to tackle this problem, essentially computing interval enclosures of compact IVPs. Such procedures are all inherently based on numerical approximation techniques in contrast to the deductive, symbolic proof approach offered by dL.

In safety-critical applications however, the trustworthiness of such numerical approaches is challenging to justify rigorously. Even when the numerical approximations computed by such numerical procedures are mathematically rigorous (which is itself difficult to fully justify in a trustworthy fashion), subtle errors can still arise in the implementation of such algorithms. Even the verification of floating-point arithmetic has proven to be intricate and non-trivial [9].

Deductive approaches based on symbolic proofs in contrast are much more trustworthy. Properties of dynamical systems are proved by applying a sequence of sound proof rules based on a small set of sound axioms [23]. Certifying the correctness of such proofs only relies upon a small trusted core of the proof checker [8]. Such deductive approaches are more symbolic in nature, seemingly orthogonal to numerical approximations and less capable in verifying inherently numerical properties of compact IVPs. On the contrary, this article crucially shows that this is not the case, numerical approximations and symbolic logic can be harmoniously integrated to obtain the best of both worlds—symbolically proving properties of dynamical systems using numerical approximations. Thus, the desired properties can be proven deductively in a trustworthy manner accompanied by a certifying proof, while not losing the computational capabilities of using numerical approximations. This article thereby unifies computation and deduction for compact IVPs.

All in all, this article explores the *proof theory* of compact IVPs, providing *complete* reasoning principles for bounded open safety, open liveness and existence properties for compact IVPs by drawing upon both numerical algorithms and deductive verification techniques.

The following presents an overview of the main results established in this article, first defining the basic notions needed. Let

$$x' = f(x)$$
$$x(0) \in [\![C]\!] \subset \mathbb{R}^n$$

be an arbitrary IVP on a compact time horizon $[t_0, T]$ with rational endpoints, each component of $f(x) = (f_1(x), \ldots, f_n(x))$ is a rational polynomial in the (n-dimensional vectorial) variable x and $[\![C]\!]$ is a non-empty compact subset of $\mathbb{R}^n$ defined via the $\mathsf{FOL}_{\mathbb{R}}$ formula $C(x)$ (i.e., $[\![C]\!] = \{x \in \mathbb{R}^n \mid \mathbb{R} \models C(x)\}$). The main contributions of the article concern the completeness of fragments of dL, a brief explanation of the necessary fragment is given here and a more complete account of dL is provided in Section 3.1.

The fragments this article is concerned with comprises of dL formulas [38] of the following form, where $P, Q \in \mathsf{FOL}_{\mathbb{R}}$ and $t_0, T \in \mathbb{Q}$.

$$\mathsf{SAFETY}(P,Q) \equiv (P \land t = t_0 \rightarrow [x' = f(x), t' = 1 \& t \leq T]Q)$$
$$\mathsf{LIVENESS}(P,Q) \equiv (P \land t = t_0 \rightarrow \langle x' = f(x), t' = 1 \& t \leq T\rangle Q)$$

where the modal connectives $[x' = f(x), t' = 1 \& t \leq T]Q$ and $\langle x' = f(x), t' = 1 \& t \leq T\rangle Q$ are extensions of the classic modal operators $\Box Q, \Diamond Q$ to ODEs. Intuitively, $[x' = f(x), t' = 1 \& t \leq T]Q$ means "for every initial value, for all times $t \in [0, T]$ following the vector field $x' = f(x), t' = 1$, Q is true" and likewise for the diamond modality. Such modal formulas express safety/liveness properties of the flow induced by the differential equation $x' = f(x)$. If $\varphi(x,t)$ denotes the corresponding flow function[1] starting at $t = t_0$ (i.e., $\varphi(x, t_0) = x$), then the formulas above correspond exactly to the following formulas that quantify over times along the flow:

$$\mathsf{SAFETY}(P,Q) \iff \big(P(x) \rightarrow \forall t \in [t_0, T]\ Q(\varphi(x,t))\big)$$
$$\mathsf{LIVENESS}(P,Q) \iff \big(P(x) \rightarrow \exists t \in [t_0, T]\ Q(\varphi(x,t))\big)$$

i.e., the first formula expresses the safety property that every trajectory starting in the set characterized by P evolving on the time horizon $[t_0, T]$ remains in the safety region characterized by Q. Dually, the second formula expresses the liveness property that every trajectory starting in P can reach the target set Q by evolving on $[t_0, T]$. This article primarily concerns open properties where the post-condition Q defines an open subset (i.e., $[\![Q]\!]$ is topologically open). It is worth noting that liveness classically corresponds to the negated safety of the complement, i.e., the following holds

$$\neg\mathsf{SAFETY}(P, \neg Q) \iff \mathsf{LIVENESS}(P,Q)$$

Thus, (unconditional) completeness of safety properties is equivalent to the (unconditional) completeness of liveness properties. However, this equivalence does not hold between open properties

[1] The flow is assumed to be well-defined here for brevity, the complication of finite time blow-up is treated in Section 5.

(i.e., Q is topologically open) as the complement of a non-trivial open set is no longer open. The following main results are established in this article:

(1) **Completeness for convergence**: Suppose the (compact) IVP admits a solution/flow $\varphi(x,t)$ on the domain $[\![C]\!] \times [t_0,T]$ (i.e., $\varphi(x,t_0)=x, \varphi'(x,t)=f(\varphi(x,t))$ for all $(x,t)\in[\![C]\!]\times[t_0,T]$), let $(p_n)_n \in C^0([\![C]\!]\times[t_0,T],\mathbb{R}^n)$ be any sequence of definable approximants[2] that converges uniformly to $\varphi(x,t)$ in the space $C^0([\![C]\!]\times[t_0,T],\mathbb{R}^n)$. For all $\varepsilon\in\mathbb{Q}^+$, one can computably find some $k\in\mathbb{N}$ such that

$$C(x)\wedge x=x_0\wedge t=t_0 \rightarrow [x'=f(x),t'=1\&t\le T]\ \|x-p_k(x_0,t)\|^2\le\varepsilon^2$$

is a valid formula of dL where x, x_0, t are *symbolic variables.* In fact, we will show that this can be syntactically derived in dL's axiomatization. This formula is equivalent to the following sentence involving the true flow φ of the IVP as a function symbol

$$\forall x_{\ 0}\in[\![C]\!]\ \forall t\ \in[t_0,T]\ \left(\|\varphi(x_0,t)-p_k(x_0,t)\|^2\le\varepsilon^2\right)$$

i.e., p_k is an approximant of *uniform error* at most ε for the true flow $\varphi(x,t)$ on $[\![C]\!]\times[t_0,T]$. In other words, this formula along with its syntactic derivation provides a *proof* of the accuracy of the approximant p_k. This establishes that dL is *complete for convergence.* i.e., if a sequence $(p_n)_n \xrightarrow{n\to\infty} \varphi$ converges in $C^0([\![C]\!]\times[t_0,T],\mathbb{R}^n)$, then this convergence is provable in dL, succinctly denoted as the following:

$$\vDash (p_n)_n \xrightarrow{n\to\infty} \varphi \qquad\Longrightarrow\qquad \vdash (p_n)_n \xrightarrow{n\to\infty} \varphi$$

In particular, the definable approximants can be taken to be outputs of numerical solvers applied on the IVP, obtained via standard interpolation procedures (e.g., polynomials, splines). The above result shows that dL is capable of *symbolically proving* the accuracy of numerical solvers. In contrast to ODE solvers that rely upon rigorous numerics using one specific formally verified algorithm [31, 32], this result rather gives a procedure that decides if *any* such numerical algorithm is correct from its *outputs*, along with supporting formal proofs. Crucially this procedure does not rely on any particular ODE solver to be correct, it rather takes outputs of ODE solvers as inputs (represented by the sequence of approximants) and returns a certificate of correctness for the accuracy of the approximants in the form of a proof in dL.

(2) **Completeness of (compact) IVPs**: This article proves completeness of dL's axiomatization for bounded open safety, open liveness and existence properties of compact IVPs:

- **Completeness for bounded open safety**: Let $O(x)$ be a $\mathsf{FOL}_\mathbb{R}$ formula that characterizes a bounded open subset of $\mathbb{R}^n$. dL is complete for formulas of the form

$$C(x)\wedge t=t_0\rightarrow[x'=f(x),t'=1\&t\le T]O(x)$$

  i.e., if all flows of the IVP starting anywhere in $[\![C]\!]$ always remains within the set of safe states characterized by $O(x)$ on the time horizon $[t_0,T]$, then this is provable in dL.
- **Completeness for open liveness**: Let $O(x)$ be a $\mathsf{FOL}_\mathbb{R}$ formula that characterizes an open subset of $\mathbb{R}^n$ (not necessarily bounded as stronger assumptions are placed on the flow instead), and suppose that the true flow $\varphi:[\![C]\!]\times[t_0,T]\rightarrow\mathbb{R}^n$ is well-defined (i.e., does not exhibit finite time blow-up on $[t_0,T]$)[3]. Then dL is complete for formulas of the form

$$C(x)\wedge t=t_0\rightarrow\langle x'=f(x),t'=1\&t\le T\rangle O(x)$$

[2] Definable functions in $\mathsf{FOL}_\mathbb{R}$, which is exactly when each p_n is a semialgebraic function over $\mathbb{Q}$. In particular, this includes polynomials in $\mathbb{Q}[x,t]$, see Definition 4.5 for details.

[3] Such an assumption also suffices for arbitrary open safety properties.

i.e., if a target state characterized by $O(x)$ is reachable from starting anywhere in $[\![C]\!]$ in the time horizon $[t_0, T]$ by following the IVP, then this is provable in dL.

— **Completeness for existence**: dL is complete for formulas of the form

$$C(x) \wedge t = t_0 \longrightarrow \langle x' = f(x), t' = 1\rangle t \geq T$$

i.e., if the solution exists for time at least $t \geq T$ for all initial conditions from $[\![C]\!]$, then this is provable in dL.

By considering the case where $C(x) \equiv x = x_0$ defines a singleton, corresponding completeness results for IVPs with fixed initial conditions are obtained as a special case.

(3) **Axioms/proof-rules for symbolic IVPs**: In proving completeness of existence for IVPs, fundamental *symbolic* axioms/proof-rules (Theorem 5.7) are derived for deductive verification of symbolic IVPs on compact time horizons without placing constraints on the initial conditions. Establishing symbolic derivations of the classical Picard-Lindelöf theorem, the intermediate value theorem and the property that the solution to an IVP exists on some time horizon if and only if the solution has no finite time blow-up on that time horizon. Due to the fundamental nature of such axioms/proof-rules [54], their derivations are of independent interest.

2 Related Work

The results presented in this article build upon the proof theory of dynamical systems using the framework of ***differential dynamic logic*** (**dL**) [40, 45, 50, 52]. This article establishes the first complete axiomatization for compact IVPs, showing that all true (bounded) open properties can be deduced completely from symbolic axioms/proof rules, in the spirit of Poincaré's qualitative theory of differential equations [46]. Consequently, it is possible to deductively prove properties of compact IVPs with trustworthy symbolic logic whilst retaining the computational capabilities of numerical techniques. The restriction to open properties is motivated by the fact that general properties of solutions to IVPs quickly lead to deep open problems such as the decidability of the real exponential field [36] ($x' = x, x(0) = 1$ defines the exponential function), the bounded Skolem problem as discussed below, or are undecidable in general [14, 26].

Computability of compact IVPs: The computability of IVPs have been studied extensively [11–13, 27, 47], including the computability of the flow of compact IVPs [29] and deep results establishing the universality of ODEs with polynomial vector fields [14], highlighting the rich complexity of polynomial IVPs. More recent works have also shown interesting connections between computable ordinals and the solutions of discontinuous IVPs [10].

In the specific case of (continuous) linear dynamical systems, many deep and fundamental results have been established in earlier works [1, 17, 18, 20] concerning the (non-)computability of various properties such as: invariant synthesis, hyperplane reachability, recurrent reachability, and so on. The computability of these properties are challenging and often rely upon open problems in number theory, highlighting their intricacy.

In the context of IVP verification, such computability results can be viewed as the theoretical foundation of numerical techniques. Indeed, the statement that arbitrarily accurate numerical approximations can be computed for compact IVPs is a restatement of the result that solutions to compact IVPs are type-two computable (see Section 3.2 for details). However, the trustworthiness of such approaches is much more delicate and it is difficult to formalize requirements on the trustworthiness of numerical algorithms purely on the computability level. Such questions are more naturally expressed as *provability* questions, which is exactly what this article addresses.

In the same way that computability is the theoretical foundation for numerical techniques, provability is the theoretical foundation for symbolic deductive techniques. Such provability properties are generally more fine-grained and delicate compared with computability properties. As dL is computably axiomatized, any property it is complete for is trivially computably enumerable by searching through all possible proofs, while the logical completeness of computably enumerable properties is far from trivial. For example, the decidability of differential invariants was first established [35] and its complete axiomatization was only discovered [44, 45] later. Numerical techniques are often viewed to be more scalable than deductive techniques for IVPs, but symbolic proofs enjoy a higher level of rigor and reliability.

Nonetheless, the completeness results presented in this article precisely bridge this gap, showing that in the context of (open) properties of compact IVPs, provability and computability notions "coincide" - numerical approximations can be carried out entirely deductively in dL with symbolic proofs. There is no fundamental distinction between numerical and symbolic computations for compact IVPs. Properties that can be verified by numerical techniques with direct computations can also be verified deductively with logic, resulting in trustworthy proofs of such properties while enjoying the generality of numerical techniques. Furthermore, building upon works on the computability of IVPs [26], this article establishes a direct computable correspondence between valid (open) properties of compact IVPs and their proofs in dL.

Proof theory of compact IVPs: The completeness results presented in this article applies to all (open) properties for compact IVPs, and does so in a computable fashion. In contrast to the results established in this article, earlier works either only prove relative completeness with some non-computable oracle [39, 40], exact completeness that cannot handle compact IVPs which are sensitive to their initial conditions [45], or does not achieve general completeness results [50, 52]. To the best of our knowledge, this is the first result that establishes the provability of such properties of compact IVPs.

Concerning relative completeness, dL has been shown to be complete relative to its continuous fragment [38] and the continuous fragment of dL has been shown to be complete relative to its discrete fragment by leveraging additional axioms on Euler discretizations [39]. However, since the discrete fragment of dL is non-computable, such results do not yield exact and computable completeness results.

For exact (and computable) completeness, earlier works on the proof theory of ODEs have identified a complete axiomatization for differential invariants [44, 45], i.e., a semialgebraic region is invariant under the flow of the given ODE if and only if it is provably invariant in the logic dL. However, in the verification of safety properties of IVPs, appropriate invariants still need to be found. The synthesis of suitable invariants to prove safety properties of continuous dynamical systems is a challenging problem in general [51], even in the linear case this is intimately related to open problems in transcendental number theory [1]. This article in particular also establishes a reduction of "continuous dependence on initial conditions" of flows to a suitable differential invariant (Lemma 4.11), which could be viewed as an invariant synthesis result. Generalizing upon this, a complete axiomatization is then established for general safety properties of IVPs (Theorem 5.11) under topological assumptions which does not assume the existence of some suitable invariant. Furthermore, this article also prove completeness results for liveness (Theorem 5.13) and existence (Theorem 5.12) properties.

In addition, this article also provides novel syntactic derivations of classical theorems in dL that are fundamental to the study of IVPs, allowing for the deductive verification of general symbolic IVPs beyond compact IVPs. In contrast with earlier works [50, 52], these axioms/proof rules focus on the case where the IVP is considered on a compact time horizon and crucially does not assume global existence of solutions. This situation is much more delicate as solutions of IVPs might exhibit finite time blow-ups. The derivations themselves are of independent interest. Not only are the axioms/proof rules themselves fundamental in the study of IVPs, such derivations also improve upon earlier works (e.g., for IVT [43]) where soundness was proven but no derivation was known.

The Continuous Skolem Problem and limitations: The Continuous Skolem Problem is a central problem in the theory of continuous dynamical systems [5]. Given an IVP $x' = f(x)$ with $x(0) = x_0 \in \mathbb{Q}^n$ and a vector $u \in \mathbb{Q}^n$, the Continuous Skolem Problem asks if the solution $x(t)$ reaches the hyperplane defined by u. i.e., if there exists some $t \geq 0$ such that $u^T x(t) = 0$. The Bounded Continuous Skolem problem [5, Open Problem 17] asks if such a t exists in some pre-determined interval $[0, T]$ with $T \in \mathbb{Q}^+$. The decidability of both problems have been long-standing open problems, with partial progress being made in the case where the ODE is linear, i.e., $x' = Ax$ for $A \in \mathbb{Q}^{n\times n}$ [18]. In the linear case, the Bounded Continuous Skolem problem was shown to be decidable assuming Schanuel's conjecture [18, Theorem 7], a unifying conjecture in number theory which implies the decidability of the real exponential field [36]. Such problems have also been studied when $f(x)$ is allowed to be a polynomial [29]. In this setting, the decidability of the Bounded Continuous Skolem problem remains open. In the context of this article, such problems place inherent restrictions on possible generalizations of the new results presented here. The results established can be viewed as the form of "(compact, (bounded) open)", where the initial condition is required to come from a compact set and the post-condition is required to be (bounded) open. A natural generalization is to consider "(compact, compact)" where post-conditions are compact semialgebraic sets. However, such completeness results (if possible) are at least as hard as the Bounded Continuous Skolem problem for polynomial dynamical systems. This is because the Bounded Continuous Skolem problem is co-computably enumerable (co-c.e.):

$$\exists t \in [0, T]\ u^T x(t) = 0 \iff \min_{t\in[0,T]} |u^T x(t)| = 0$$

and minima of computable functions over compact sets are computable (Theorem 3.9), therefore the second relation is co-c.e. At the same time, reachability can be naturally formulated in dL via:

$$x = x_0 \land t = 0 \rightarrow \langle x' = f(x), t' = 1 \& t \leq T\rangle u^T x = 0$$

Thus, if completeness results of the form "(compact, compact)" hold, then the Bounded Continuous Skolem problem would also be c.e. by searching through all possible proofs in dL (as dL is computably axiomatized [39]) while bounding the hyperplane[4], implying the decidability of the Bounded Continuous Skolem problem (independent of Schanuel's conjecture). Hence, generalizations of the results in this article by relaxing the topological constraints on the post-conditions are likely challenging.

Reachability computation of dynamical systems: The problem of computing interval enclosures for hybrid/continuous dynamical systems shows up frequently in the safety verification of CPS. Practical implementations [15, 16, 21, 31, 32] exist to carry out such computations, based on numerical approximations. The correctness of these depends on both the correctness of the underlying mathematical theory of such approximations and the correctness of the implementation, both of which are prone to errors. Attempts in improving the reliability of such procedures focus on the formal verification of such algorithms (e.g., [31, 32, 37] in the continuous case), where the numerical algorithm implemented is formally verified to be mathematically sound. These formal verifications are inherently dependent on the specific algorithm used, and modifications to the algorithm require corresponding complex modifications to the proof of correctness, in addition to the possibility of implementation errors. The lack of compositionality [56, Page 325] implies that it is non-trivial to combine different algorithms harmoniously. This is in particular highlighted by the fact that, to the best of our knowledge, current algorithms for computing the interval enclosure of hybrid dynamical systems [2, 7, 19] are in theory mathematically rigorous but have

[4] While $u^T x = 0$ does not define a compact set, it can be modified to the compact set $u^T x = 0 \land \|x\|^2 \leq R$ for $R \in \mathbb{Q}^+$. If the former holds, then the latter holds for all sufficiently large R, resulting in a c.e. procedure by searching through all $R \in \mathbb{Q}^+$.

not been formally verified. More fundamentally, such approaches are providing formal verifications of the *algorithm* used to compute the approximations, inducing potential error when transforming from the abstract algorithm verified to the actual implementation executed. This is in contrast to logic-based deductive approaches where every verified property has a certifying *syntactic proof* which can be independently checked.

The results presented in this article provide a complementary possibility through dL: Such verifications can *all* be carried out deductively with sound axioms/proof rules, therefore the correctness of the approximations can be trusted as certified by their corresponding symbolic proofs. Numerical approximations can be computed deductively, ending up with compositional proofs in dL that can be used in symbolic proofs of safety of the overall hybrid dynamical system. In particular, the completeness results (e.g., Theorem 4.21) are agnostic to how the numerical approximants were computed. Therefore potentially unreliable approximation algorithms can be used in computations as the computed approximants can always be symbolically proven to be accurate if they truly are accurate. In contrast with the formal verification of numerical algorithms, the deductive approach certifies the correctness of outputs with corresponding *proofs* that can be checked with proof checkers such as KeYmaera X [8, 23]. The aim of the article is not to argue for the superiority of symbolic techniques over numerical ones, but rather that such approaches are in fact intimately related and it is possible to simultaneously achieve the strengths of both approaches at once as shown by the completeness results.

3 Preliminaries

We give a self-contained overview of the computable analysis and differential dynamic logic (dL) needed for the article. More details on computable analysis, computability theory [49, 55] and dL [38] can be found in the corresponding references.

3.1 Differential Dynamic Logic

This section provides a brief review of dL and its axiomatization, fixing some notational conventions along the way. This article focuses on the continuous fragment of dL. Intuitively, dL extends classical dynamic logic (which itself extends modal logic) where every ODE $x' = f(x)$ has corresponding modal operators $\langle x' = f(x)\rangle$, $[x' = f(x)]$. The modal formula $\langle x' = f(x)\rangle\varphi$ indicates that by flowing along the ODE $x' = f(x)$, there *exists* some time for which φ is true. Similarly, $[x' = f(x)]\varphi$ indicates that φ is *always* true following the flow of $x' = f(x)$.

3.1.1 Syntax. Terms in dL are formed by the following grammar, where $\mathbb{V}$ denotes the set of all variables, $x \in \mathbb{V}$ is a variable and $c \in \mathbb{Q}$ is a rational constant. Equivalently, terms are polynomials over $\mathbb{V}$ with rational coefficients [5].

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

dL formulas have the following grammar, where $\sim \in \{=, \neq, \geq, >, \leq, <\}$ is a comparison relation and α is a system of differential equations (dL allows for α to be from the more general class of *hybrid programs* [38], which is not needed here)

$$\begin{aligned}\varphi, \psi &::= p \sim q \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid \neg\varphi \mid \forall x \varphi \mid \exists x \varphi \mid \langle\alpha\rangle\varphi \mid [\alpha]\varphi \\ \alpha &::= \cdots \mid x' = f(x) \& Q\end{aligned}$$

[5] Prior works [45] make it possible to consider dL with an expanded language that includes familiar mathematical functions such as exp, sin, cos. Such expansions will not be considered in this article due to the subtle concerns regarding computability of such expanded functions.

In this article, we will only be dealing with the case $\alpha \equiv x' = f(x) \& Q$, where $x' = f(x)$ represents an autonomous system of ODEs $x_1' = f_1(x), \ldots, x_n' = f_n(x)$ and $x = (x_1, \ldots, x_n)$ is understood to be vectorial. Q here refers to some dL formula known as the *domain constraint*. Intuitively, this restricts the region for which the ODE $x' = f(x)$ is allowed to evolve. In contrast with some of the earlier works [45, 52], the domain constraint Q is in general allowed to be any dL formula, resulting in "rich-test" dL [38, 40, 41], but is usually a formula of real arithmetic ($\mathsf{FOL}_{\mathbb{R}}$).

The following conventions are used throughout this article. For terms and formulas that appear in contexts involving ODEs $x' = f(x)$, it is sometimes needed to restrict the variables that they can refer to. Such free variables will be indicated by explicitly writing them as arguments. For example, $p()$ means that the term p cannot refer to any bound variable of the ODE $x' = f(x)$. In contrast, $P(x)$ (or just P) indicates that all the variables may be referred to as free variables. Such variable dependencies can be made formal and rigorous through dL's uniform substitution calculus [41].

3.1.2 Semantics. A state ω is a mapping $\omega : \mathbb{V} \to \mathbb{R}$ that assigns a value to every variable. We denote $\mathbb{S}$ as the set of all such states. For a term p, its semantics in state $\omega \in \mathbb{S}$ written as $[\![p]\!]$ is the real value obtained by evaluating the polynomial p at the state ω. For a dL formula φ, its semantics $[\![\varphi]\!]$ is defined to be the set of all states $\omega \in \mathbb{S}$ such that $\omega \models \varphi$, i.e the formula φ is true in ω. The semantics of first-logical connectives are defined as expected, e.g., $[\![\varphi \vee \psi]\!] = [\![\varphi]\!] \cup [\![\psi]\!]$. For $\alpha \equiv x' = f(x) \& Q$, the semantics for $[\alpha]\varphi$ and $\langle\alpha\rangle\varphi$ are defined as follows. For the given ODE $x' = f(x)$ with domain constraint Q and any state $\omega \in \mathbb{S}$, let $\Psi_\omega : [0, T) \to \mathbb{S}$ be the solution to $x' = f(x)$ extended maximally to the right with $0 < T \leq \infty$ and $\Psi_\omega(0) = \omega$. We then have:

$$\omega \in [\![[\alpha]\varphi]\!] \text{ iff for all } 0 \leq \tau < T \text{ such that } \Psi_\omega(\xi) \models Q \text{ for all } 0 \leq \xi \leq \tau, \text{ we have } \Psi_\omega(\tau) \models \varphi$$

$$\omega \in [\![\langle\alpha\rangle\varphi]\!] \text{ iff there exists some } 0 \leq \tau < T \text{ such that } \Psi_\omega(\xi) \models Q \text{ for all } 0 \leq \xi \leq \tau \text{ and } \Psi_\omega(\tau) \models \varphi$$

Intuitively, the formula $[\alpha]\varphi$ expresses a *safety* property, that φ holds along all flows of the ODE $x' = f(x)$ that remain inside the domain constraint defined by the dL formula Q. Similarly, the formula $\langle\alpha\rangle\varphi$ expresses a *liveness* property, that there is some flow along $x' = f(x)$ staying within Q eventually reaching a state where φ is true.

Finally, a formula φ is said to be valid if $[\![\varphi]\!] = \mathbb{S}$, i.e., it is true in all states. For $\mathsf{FOL}_{\mathbb{R}}$ formulas[6] I and Q, we say I is a *differential invariant* of the ODE $x' = f(x) \& Q$ if the formula $I \to [x' = f(x) \& Q]I$ is valid, which is equivalent to $[\![I]\!] \subseteq [\![[x' = f(x) \& Q]I]\!]$ as sets of states. i.e., Starting from any state $\omega \in [\![I]\!]$ and evolving along the ODE $x' = f(x)$ while remaining within the domain constraint Q necessarily implies that the state remains in I, thus I is an *invariant* of the system $x' = f(x) \& Q$. One important fact used throughout this article is that dL is (effectively) complete for differential invariants in $\mathsf{FOL}_{\mathbb{R}}$ [45]. In other words, if I is a differential invariant of $x' = f(x) \& Q$, then one can effectively find a syntactic proof of $I \to [x' = f(x) \& Q]I$ (Theorem 3.2).

Example 3.1 (Differential Invariant). The $\mathsf{FOL}_{\mathbb{R}}$ formula $I(x, y) \equiv x^2 + y^2 = 1$ is a differential invariant of the ODE $x' = -y, y' = x$ representing circular motion. i.e., the following dL formula is valid

$$x^2 + y^2 = 1 \to [x' = -y, y' = x]x^2 + y^2 = 1$$

By Theorem 3.2, it then follows that this formula is furthermore provable in dL.

3.1.3 Proof Calculus. The derivations in this article are presented in a standard, classical sequent calculus with the usual rules for manipulating logical connectives and sequents. The semantics of a *sequent* $\Gamma \vdash \varphi$ is equivalent to the formula $(\bigwedge_{\psi \in \Gamma} \psi) \to \varphi$, and the sequent is called valid if

[6] This definition extends to general dL formulas, but computable completeness of differential invariance is restricted to $\mathsf{FOL}_{\mathbb{R}}$.

its corresponding formula is valid. For a sequent $\Gamma \vdash \varphi$, formulas Γ are called antecedents, and φ the succedent. Completed proof branches are marked with $*$ in a sequent proof, and since $\mathbb{R}$ has a decidable theory via quantifier elimination [53], statements that follow from real arithmetic are proven with the rule $\mathbb{R}$. An axiom (schema) is called *sound* iff all of its instances are valid, and a proof rule is sound if the validity of all its premises entail the validity of its conclusion. Axioms and proof rules are *derivable* if they can be proven from dL axioms and proof rules via the aforementioned sequent calculus. Derivable axioms are automatically sound due to the soundness of dL's axiomatization [38, 45].

This article uses a fragment of the base axiomatization of dL [40] (focusing on the continuous case) along with an extended axiomatization developed in prior works used to handle ODE invariants and liveness properties [45, 52]. A complete list of the axioms used is provided in Appendix A.

An important feature of the axiomatization used is that it is complete for all differential invariants [45]. Since this will be used extensively throughout the article, this fact is explicitly stated below.

Theorem 3.2 (Completeness of Differential Invariants [45]). dL *is complete for differential invariants. For all* $\mathrm{FOL}_{\mathbb{R}}$ *formulas* I, Q *and ODE* $x' = f(x)$, *if the* dL *formula*

$$I \rightarrow [x' = f(x) \& Q] I$$

is valid, then one can effectively find a proof of it in dL. *We will make use of this result with the following derived proof rule:*

$$\text{dInv}\quad \frac{*}{\vdash I \rightarrow [x' = f(x)\&Q]I} \qquad\qquad (\text{If } I \rightarrow [x' = f(x)\&Q]I \text{ is valid})$$

Theorem 3.2 will be utilized frequently to obtain syntactic proofs by first reducing the goals down to some differential invariant, and then proving the validity of this invariant semantically. This completeness is effective, so computability properties are preserved by appealing to Theorem 3.2.

3.2 Computability and Computable Analysis

The completeness properties established in this article are *effective*. Not only are valid formulas provable, there is a direct (computable) correspondence between the valid formulas and their proofs. i.e., there is a computable algorithm taking valid formulas as inputs and outputting corresponding proofs in dL.[7] To achieve the desired completeness results effectively, it is necessary to utilize the computability-theoretic properties of IVPs, which are framed in the language of *computable analysis*. The following provides the required background on computable analysis, under the standard framework of *Type Two Theory of Effectivity* (TTE) [55].

Definition 3.3 (Name). Let $x \in \mathbb{R}$ be any real number, a *name* for x is a sequence of rationals $(q_i)_i \subseteq \mathbb{Q}$ such that

$$\forall i \in \mathbb{N}\ (|q_i - x| < 2^{-i})$$

This definition naturally extends to $\mathbb{R}^n$ by requiring names to reside in $\mathbb{Q}^n$ and using the standard Euclidean norm. For $x \in \mathbb{R}^n$, we denote the set of all names of x as $\Gamma(x)$.

For a fixed real number $x \in \mathbb{R}^n$, one should think of its names as the "descriptions" of x. We then define x to be computable if it exhibits a computable description.

Definition 3.4 (Type-Two Computable Number). Let $x \in \mathbb{R}^n$ be any real number, x is *Type-Two computable* if it has a computable name. i.e., there is some computable sequence $(q_i)_i \subseteq \mathbb{Q}^n$ that is a name for x.

[7] As dL's axiomatization is effective, completeness automatically implies such an algorithm by searching through all proofs. However, this article establishes a direct correspondence rather than resorting to the brute-force search.

Intuitively, this means that a real $x \in \mathbb{R}^n$ is (Type-Two)computable if and only if it can be computably approximated by a sequence of vectors of rational numbers. From now on, whenever we refer to the computability of numbers in $\mathbb{R}^n$, we mean Type-Two computability.

Definition 3.5. An *oracle machine* M is a Turing machine that allows for an additional one-way read-only input tape that represents some input oracle used. The machine is allowed to read this input tape up to arbitrary, but finite, lengths.

One can think of oracle machines as regular Turing machines but with some access to outside information, namely the "oracle" input tape. The machine may use any finite amount of information on this tape. For an oracle machine M, and an infinite binary sequence $p \in 2^\omega$, M^p represents the oracle machine M with oracle p. By standard encoding, we do not differentiate between $\mathbb{Q}^\omega$ and 2^ω.

Having defined a notion of computability on individual elements of $\mathbb{R}^n$, the following definition provides a notion of computability on the closed subsets of $\mathbb{R}^n$.

Definition 3.6 ([55, Corollary 5.1.8]). A non-empty closed subset $E \subseteq \mathbb{R}^n$ is *computable* if its corresponding distance function $x \mapsto \inf_{y \in E} \|x - y\|$ is computable.

It can be easily seen that every $\mathsf{FOL}_{\mathbb{R}}$ definable closed set is computable.

Theorem 3.7. *If $E \subseteq \mathbb{R}^n$ is a closed subset defined by the $FOL_{\mathbb{R}}$ formula $\varphi(x)$, then it is a computable closed set and its distance function is computable uniformly in $\varphi(x)$.*

Proof. Let $d : \mathbb{R}^n \to \mathbb{R}$ denote the distance function for the closed set $E = [\![\varphi]\!]$ defined via

$$d(x) = \inf_{y \in E} \|x - y\|$$

It suffices to show that the relation $d(q) < r$ is uniformly decidable for $q \in \mathbb{Q}^n, r \in \mathbb{Q}^+$, which is true as this relation can be defined by the following $\mathsf{FOL}_{\mathbb{R}}$ formula :

$$\psi(q, r) \equiv \exists y(\varphi(y) \wedge \|y - q\|^2 < r^2)$$

hence decidability follows as $\mathbb{R}$ has a decidable theory, proving d to be computable. □

The following definition relates the use of oracle machines to computable functions in TTE.

Definition 3.8 (Computable Function). A function $f : E \subseteq \mathbb{R}^n \to \mathbb{R}^m$ with E a computable closed set is *computable* if there is some oracle machine M such that

$$\forall \in E \, \forall p \ \in \Gamma(x) \ ((M^p(i))_i \in \Gamma(f(x)))$$

i.e., M maps names of x to names of $f(x)$ for all $x \in E$.

Intuitively, this means that a function $f : \mathbb{R}^n \to \mathbb{R}^m$ is computable if and only if there is some computable algorithm such that for every $x \in \mathbb{R}^n$, the algorithm can output more and more accurate approximations of output $f(x)$ given more and more accurate approximations of input x. By this definition, any Type-Two computable function is necessarily continuous, since oracle machines can only read a finite amount of its oracle before producing an output. In other words, for all $x \in \mathbb{R}^n, i \in \mathbb{N}$, there is some corresponding $j \in \mathbb{N}$ such that if f is provided with an approximation of x accurate up to 2^{-j}, then the output is an approximation of $f(x)$ accurate up to 2^{-i}, therefore f is continuous. The standard functions $\sin(x), \cos(x), x^2, e^x, \cdots$ are all computable through their Taylor expansions.

A useful result of computable analysis is that the classical extreme value theorem holds computably [55, Corollary 6.2.5]. The following theorem states this for functions $f : K \subset \mathbb{R}^n \to \mathbb{R}^m$ with K a definable compact subset of $\mathbb{R}^n$, the proof is included for completeness.

Theorem 3.9 (Computable Extreme Value Theorem [55, Corollary 6.2.5]). *Let $f : K \to \mathbb{R}$ be a computable function on the compact set $K \subset \mathbb{R}^n$ defined by some $\mathrm{FOL}_{\mathbb{R}}$ formula $\varphi(x)$. Then* $\max_{x\in K}(f(x))$ *and* $\min_{x\in K}(f(x))$ *are uniformly computable in $f, \varphi(x)$.*

Proof. As K is definable and closed, it is a computable closed set. In addition, an upper bound on the radius of K can be computed from $\varphi(x)$: search for $R \in \mathbb{Q}^+$ such that the $\mathsf{FOL}_{\mathbb{R}}$ formula $\varphi(x) \to \|x\|^2 < R^2$ is valid, hence a representation of the compact set K [55, Remark 5.2.3] is computable from $\varphi(x)$. Consequently, a representation of the image of K under the computable function f, $f(K)$, is computable from $\varphi(x)$ as well. The computability of $\max_{x\in K} f(x)$ then follows from the computability of maximums on compact sets [55, Lemma 5.2.6] applied to $f(K)$. □

4 Completeness under Domain Constraints

This section establishes the completeness of dL's axiomatization for convergence with additional assumptions on domain constraints. To accomplish this, we will reduce the problem of proving error bounds for approximants of compact IVPs to differential invariance questions, which dL is effectively complete for [45]. Intuitively, this reduction is achieved by proving a syntactically provable version of "continuous dependence on initial data" for ODEs in dL. Establishing that the flow function induced by the ODE, if well-defined on a compact domain, is uniformly continuous. Consequently, if an approximant starts off close to the initial condition, then it will remain close to the true flow in the supremum norm for all times in the bounded interval. Thus, proofs of future error bounds of approximants provably reduce to arithmetic questions *at the initial time t_0*.

However, since polynomial vector fields are generally nonlinear and therefore do not exhibit global Lipschitz constants, it is tricky to obtain explicit and computable bounds in this reduction process. As such, this section will first assume the presence of some bounded domain constraint, which essentially reduces to the case of globally Lipschitz vector fields since polynomials are locally Lipschitz. Section 5.2 improves upon this, establishing that such assumptions are not necessary and can be removed, proving completeness for convergence without any additional assumptions.

4.1 Compact IVPs and Approximants

The following definitions fix standard notations that will be used throughout this article.

Definition 4.1 (Notation). The following notation will be used throughout the article.

- $\mathbb{R}^+, \mathbb{Q}^+$ denotes the set of positive real/rational numbers, respectively.
- x always denotes some vectorial variable $x = (x_1, \dots, x_n)$.
- For a ring R, denote its ring of polynomials in the variables $x_1, \dots, x_n$ as $R[x_1, \dots, x_n]$. This article only considers $R \in \{\mathbb{Q}, \mathbb{R}\}$. By a slight abuse of notation, elements $p(x) \in R[x]$ are also identified with the corresponding polynomial $p : R^n \to R$.
- By a *rational polynomial*, we mean some element of $\mathbb{Q}[x]$ where x is understood to be vectorial.
- $\|x\|$ for $x \in \mathbb{R}^n$ always refers to the Euclidean norm, and $\|f\|$ always refers to the sup norm for functions f. We sometimes write $\|f\|_A = \sup_{x\in A} \|f(x)\|$ to emphasize that the supremum norm of f is taken on the set A, which is $\mathsf{FOL}_{\mathbb{R}}$ definable when A is $\mathsf{FOL}_{\mathbb{R}}$ definable.
- $C^k([a,b], \mathbb{R}^n)$ for $k \in \mathbb{N}$ denotes the set of functions from the closed interval $[a,b]$ to $\mathbb{R}^n$ with k continuous derivatives on $[a,b]$. For K a compact Hausdorff space, $C^0(K, \mathbb{R}^n)$ denotes the space of continuous functions with the usual supremum norm $\|f\|_K = \sup_{x\in K} \|f(x)\|$. When the co-domain is clear, these are also abbreviated as $C^k([a,b]), C^0(K)$.
- $\mathbb{IQ}$ denotes the set of all compact intervals with rational endpoints, i.e.,

$$\mathbb{IQ} = \{[a,b] : a \le b, a, b \in \mathbb{Q}\}$$

- For $x \in \mathbb{R}^n, R \in \mathbb{R}^+$, write $B[x, R]$ for the closed ball of radius R around x, and $B(x, R)$ for the open ball. When x, R are definable in dL, $y \in B[x, R]$ and $y \in B(x, R)$ are definable via
$$y \in B[x, R] \iff \|y - x\|^2 \leq R^2$$
$$y \in B(x, R) \iff \|y - x\|^2 < R^2$$
For a set $A \subseteq \mathbb{R}^n$, write $B[A, R]$ (and similarly $B(A, R)$) for $\bigcup_{x \in A} B[x, R]$.
- $\mathsf{FOL}_{\mathbb{R}}$ denotes the set of all first-order formulas in the language of real closed fields. In this article, definable always refers to $\mathsf{FOL}_{\mathbb{R}}$ definable unless explicitly stated otherwise. As real closed fields admit quantifier elimination [53], we may assume without loss of generality that every element of $\mathsf{FOL}_{\mathbb{R}}$ is quantifier-free. Finally, for formulas $\varphi(x) \in \mathsf{FOL}_{\mathbb{R}}$, $[\![\varphi]\!]$ denotes the set defined by the formula in $\mathbb{R}$. i.e.,:
$$[\![\varphi]\!] = \{y \in \mathbb{R}^n \mid \mathbb{R} \models \varphi(y)\}$$
which coincides with the semantics of φ in dL.

Definition 4.2 (Compact IVP). A compact initial value problem (IVP) is a triple
$$(f(x), C(x), [t_0, T]) \in \mathbb{Q}^n[x] \times \mathsf{FOL}_{\mathbb{R}} \times \mathbb{IQ}$$
where $[\![C(x)]\!]$ is a non-empty compact set. The variable x is often suppressed for brevity, and $[\![C]\!]$ refers to $[\![C(x)]\!]$. Such a triple represents the following IVPs on $[t_0, T]$:
$$x' = f(x)$$
$$x(t_0) = x_0 \in [\![C]\!]$$

That is, the triple defines a collection of IVPs on some compact time horizon $[t_0, T]$ where the initial conditions are constrained to the compact set $[\![C]\!]$. The flow $\varphi : [\![C]\!] \times [t_0, T] \to \mathbb{R}^n$ of the compact IVP (if it exists) is the flow of the vector field $x' = f(x)$ starting at $t = t_0$. i.e., $\varphi(x, t_0) = x, \varphi'(x, t) = f(\varphi(x, t))$ for all $(x, t) \in [\![C]\!] \times [t_0, T]$.

Since singletons are compact, the standard notion of IVPs with a fixed initial condition $x(0) = x_0 \in \mathbb{Q}^n$ is a special case of Definition 4.2 where $C(x) \equiv x = x_0$.

Remark 4.3. In practice, many IVPs contain *parameters*. i.e., $x' = f(x, a)$, where the vectorial variable a denotes the parameters used. It is always possible to rewrite such IVPs into:
$$x' = f(x, a)$$
$$a' = 0$$
$$x(t_0) = x_0, a(t_0) = a$$
which forms a compact IVP when the parameters a are constrained to a compact set.

Example 4.4 (Moore–Greitzer Jet Engine Model). The Moore–Greitzer model of a jet engine [4, 48] for scalars u, v is given by
$$u' = -v - 1.5u^2 - 0.5u^3 - 0.5$$
$$v' = 3u - v$$
with initial conditions $u(0) \geq 0.6 \wedge v(0) \geq 0.9 \wedge u(0) + v(0) - 2 \leq 0$, where u, v measures the mass flow and the pressure rise respectively. Since the initial conditions define a (semialgebraic) compact subset of $\mathbb{R}^2$, for any $T \in \mathbb{Q}^+$, we may express this model on the time horizon $[0, T]$ as a compact IVP $(f(u, v), \Delta(u, v), [0, T])$ where:

- $f(u, v) = (-v - 1.5u^2 - 0.5u^3 - 0.5, 3u - v)$.
- $\Delta(u, v) \equiv u \geq 0.9 \wedge v \geq 0.9 \wedge u + v - 2 \leq 0$

This model will serve as a running example through this article, culminating in a proof of the error bound of a numerically computed approximation to the true flow in Example 5.4. All proofs concerning the Moore-Greitzer model have been verified using KeYmaera X[8].

The first step is to establish a suitable representation for approximants to solutions of compact IVPs. In this article, such approximants are taken to be functions definable in $\mathsf{FOL}_\mathbb{R}$, which are also the semialgebraic functions over $\mathbb{Q}$ [6]. The following definition restricts to the particular case of definable functions with domain being a subset of $\mathbb{R}^{n+1}$ and co-domain $\mathbb{R}^n$ for $n \geq 1$. This is because the approximants represent approximations to the flow induced by compact IVPs, as such, they will always be functions from $\mathbb{R}^{n+1}$ (n space variables, 1 time variable) to $\mathbb{R}^n$.

Definition 4.5 ($FOL_\mathbb{R}$ Definable Functions). A function $f : A \subseteq \mathbb{R}^{n+1} \longrightarrow \mathbb{R}^n$ with definable domain A is *definable* if there exists a $\mathsf{FOL}_\mathbb{R}$ formula $\eta(x, t, y)$ such that for all $x, y \in \mathbb{R}^n, t \in \mathbb{R}$

$$f(x,t) = y \iff \mathbb{R} \models \eta(x,t,y)$$

In this case, we say that $\eta(x, t, y)$ is a *representation* of f.

Remark 4.6. As dL strictly extends $\mathsf{FOL}_\mathbb{R}$ [40], $\mathsf{FOL}_\mathbb{R}$ definable functions are also dL definable.

The class of definable functions is very versatile. In particular, polynomials and splines with rational coefficients are definable in a natural way. As a consequence, one can always carry out spline/polynomial interpolation on a mesh-grid of points to arrive at a definable approximant.

Remark 4.7. While standard dL only allows for polynomials as terms (as opposed to dL's extensions with Noetherian functions [45]), definable functions in the sense of Definition 4.5 can be expressed as well using their representations. e.g., suppose $f : \mathbb{R}^{n+1} \longrightarrow \mathbb{R}^n$ has representation $\eta(x, t, y)$ and $u \in \mathbb{V}^n$ is some vectorial variable, $\|f(x,t) - u\|^2 \leq M^2$ can then be expressed by

$$\exists y (\eta(x,t,y) \land \|y - u\|^2 \leq M^2)$$

such abbreviations will be used throughout the article for formulas containing definable functions.

The following definition makes precise the notion of approximations used in this article.

Definition 4.8 (Local Definable Approximant). Let $(f(x), C(x), [t_0, T])$ be a compact IVP and $\varphi(x, t)$ be its corresponding flow function. A ***local definable approximant*** (**LDA**) for this compact IVP is a computable function $\Phi : \mathbb{N} \longrightarrow \mathsf{FOL}_\mathbb{R}$ such that the following holds:

(1) $\varphi(x,t) : [\![C]\!] \times [t_0, T] \longrightarrow \mathbb{R}^n$ is well-defined (i.e., does not exhibit finite time blow-up for time $t \in [t_0, T]$).
(2) For all $k \in \mathbb{N}$, $\Phi(k)$ defines a function $\Phi_k : [\![C]\!] \times [t_0, T] \longrightarrow \mathbb{R}^n$ (thus each Φ_k is a definable function with representation $\Phi(k)$).
(3) The sequence of functions $(\Phi_k)_k$ converges to φ in $C^0([\![C]\!] \times [t_0, T], \mathbb{R}^n)$.
(4) For all $k \in \mathbb{N}$, the function Φ_k is differentiable in its second (time) variable, and the sequence of time derivatives $(\Phi'_k)_k$ converges to φ' in $C^0([\![C]\!] \times [t_0, T], \mathbb{R}^n)$.

Example 4.9. For IVPs with polynomial vector fields, the sequence of Picard iterates [54] always form a LDA over a sufficiently small interval. i.e., For every IVP $x' = f(x), x(t_0) = x_0 \in \mathbb{Q}^n$, there always exists a sufficiently small $S > t_0$ such that the Picard iterates form a LDA for the compact IVP $(C(x) \equiv x = x_0, f(x), [t_0, S])$. To show this, recall that the Picard iterates $(\varphi_k)_k$ of the IVP $x' = f(x), x(t_0) = x_0$ are defined inductively by

- $\varphi_0(t) = x_0$.
- $\varphi_{k+1}(t) = x_0 + \int_{t_0}^{t} f(\varphi_k(s))ds$.

[8] https://github.com/LongQianQL/Compact_IVP_Example

By the Picard–Lindelöf theorem the iterates converge uniformly to the unique solution on some interval $[t_0, S]$ for some $S > t_0$. Furthermore, this sequence of iterates are simply polynomials in t with rational coefficients since integrals of rational polynomials are rational polynomials. As integrals of polynomials are computable, the sequence of iterates $(\varphi_k)_k$ and their representations are computable. It remains to show that the sequence $(\varphi'_k)_k$ converges to x' on $[t_0, S]$. Indeed, let $x(t) : [t_0, S] \to \mathbb{R}^n$ denote the unique solution that this sequence converges to. We have

$$|x'(t) - \varphi'_{k+1}(t)| = |f(x(t)) - f(\varphi_k(t))|$$

Note that $B[x([t_0, S]), 1]$ (the set of points of Euclidean distance at most 1 away from $x([t_0, S])$) is compact as x is continuous and $[t_0, S]$ is compact. Hence, as f is a polynomial vector field and therefore locally Lipschitz, there exists some $L > 0$ which is the Lipschitz constant of f on $B[x([t_0, T]), 1]$ (we can computably find such a value by computing the maximum of f's partial derivatives on $B[x([t_0, T]), 1]$, but this is *not required* to prove the iterates form a LDA). Since $(\varphi_k)_k$ converges to x on $[t_0, S]$, we have $\varphi_k([t_0, S]) \subseteq B[x([t_0, S]), 1]$ for all sufficiently large k. In other words, for all sufficiently large k, for all $t \in [t_0, S]$, we have:

$$|x'(t) - \varphi'_{k+1}(t)| = |f(x(t)) - f(\varphi_k(t))| \leq L \, \|x - \varphi_k\|_{[t_0,S]} \xrightarrow{k\to\infty} 0$$

The Picard–Lindelöf theorem says that $\varphi_k \to x$ uniformly i.e., in the supremum norm, and the above computation shows $(\varphi'_k)_k \to x'$ on $[t_0, S]$ under the sup-norm as well, therefore the sequence of Picard iterates $(\varphi_k)_k$ forms a LDA.

The example above shows that the Picard iterates will always be LDAs over sufficiently small intervals for IVPs with fixed initial values. The following theorem shows that for *any compact IVP*, a corresponding LDA can always be constructed effectively on the entire interval $[t_0, T]$ provided that the compact IVP does not exhibit finite time blow-up on $[t_0, T]$.

Theorem 4.10 (Computable LDA). *Let $(f(x), C(x), [t_0, T])$ be a n-dimensional compact IVP where the corresponding flow $\varphi(x, t)$ is well-defined on $[\![C]\!] \times [t_0, T]$. Then there exists a corresponding LDA Φ that is uniformly computable in the compact IVP such that for all $k \in \mathbb{N}$, every component of the function defined by $\Phi(k)$ is a rational polynomial in x, t. Furthermore, the LDA Φ satisfies $\|\varphi - \Phi_k\|_{[\![C]\!]\times[t_0,T]} < n2^{-k}$ and $\|\varphi' - \Phi'_k\|_{[\![C]\!]\times[t_0,T]} < n2^{-k}$ for all $k \in \mathbb{N}$.*

Proof. Since rational polynomials are $\mathsf{FOL}_{\mathbb{R}}$ definable, it suffices to computably construct a sequence of rational polynomials $(p^i_k)_{1\leq i\leq n, k\in\mathbb{N}} \subseteq \mathbb{Q}[x, t]$ such that the corresponding sequence $(p_k)_k \subseteq \mathbb{Q}^n[x, t]$ defined via $p_k = (p^1_k, \ldots, p^n_k)$ satisfies:

(1) The sequence $(p_k)_k$ converges to φ in $C^0([\![C]\!] \times [t_0, T], \mathbb{R}^n)$.
(2) The sequence $(p'_k)_k$ converges to φ' in $C^0([\![C]\!] \times [t_0, T], \mathbb{R}^n)$.

This is sufficient as one can then define the formulas:

$$\psi_k(x, y, t) \equiv \bigwedge_{1\leq i\leq n} y_i = p^i_k(x, t)$$

Properties (1), (2) then imply that the function $\Phi : \mathbb{N} \to \mathsf{FOL}_{\mathbb{R}}$ defined by $\Phi(k) = \psi_k$ forms a LDA for the compact IVP.

To construct the desired sequence $(p^i_k)_{1\leq i\leq n, k\in\mathbb{N}}$, first fix some $1 \leq i \leq n$, let $k \in \mathbb{N}$ be arbitrary and notice that it suffices to construct some $p^i_k \in \mathbb{Q}[x, t]$ satisfying the following:

(1) $\|\varphi_i - p^i_k\|_{C^0([\![C]\!]\times[t_0,T])} < 2^{-k}$ where φ_i denotes the ith component of φ.
(2) $\|(p^i_k)' - \varphi'_i\|_{C^0([\![C]\!]\times[t_0,T])} < 2^{-k}$ where the derivative is taken with respect to time variable.

As we may then carry out the same construction for arbitrary $1 \leq i \leq n$ and $k \in \mathbb{N}$ to obtain

$$\left\|(\varphi_1, \ldots, \varphi_n) - (p_k^1, \ldots, p_k^n)\right\|_{C^0(\llbracket C \rrbracket \times [t_0, T])} \leq \sum_{i=1}^{n} \left\|\varphi_i - p_k^i\right\|_{C^0(\llbracket C \rrbracket \times [t_0, T])} < n2^{-k}$$

which converges to 0 as $k \longrightarrow \infty$, likewise for $\left\|\varphi' - p_k'\right\|_{C^0(\llbracket C \rrbracket \times [t_0, T])}$. To carry out the construction for a fixed index $1 \leq i \leq n$ and $k \in \mathbb{N}$, first note that the flow function $\varphi(x, t) : \llbracket C \rrbracket \times [t_0, T] \longrightarrow \mathbb{R}^n$ is computable for compact IVPs [47] as $\llbracket C \rrbracket$ is a computably closed set by Theorem 3.7. Because $f \in \mathbb{Q}^n[x, t]$ is also computable, consequently the time-derivative of φ, $\varphi'(x, t) = f(\varphi(x, t))$ is also computable on $\llbracket C \rrbracket \times [t_0, T]$. The effective Stone-Weierstrass theorem [55, Theorem 6.1.10] then allows us to compute some $q_k^i \in \mathbb{Q}[x, t]$ such that

$$\left\|q_k^i - \varphi_i'\right\|_{C^0(\llbracket C \rrbracket \times [t_0, T])} < \frac{2^{-k-1}}{\max(T - t_0, 1)}$$

Define $p_k^i \in \mathbb{Q}[x, t]$ by

$$p_k^i(x, t) = x_i + \int_{t_0}^{t} q_k^i(x, s) ds$$

which is computable since q_k^i is a polynomial with rational coefficients, hence its integral in the time variable t can be directly computed symbolically using the elementary power rule. It remains to verify that conditions (1) and (2) are met:

(1) Direct computations for $(x_0, t) \in \llbracket C \rrbracket \times [t_0, T]$ yields:

$$|p_k^i(x_0, t) - \varphi_i(x_0, t)| \leq \int_{t_0}^{t} |q_i^k(x_0, s) - \varphi_i'(x_0, s)| \leq (T - t_0) \frac{2^{-k-1}}{\max(T - t_0, 1)} \leq 2^{-k-1} < 2^{-k}$$

(2) Noticing that the time derivative of p_k^i is q_k^i which is continuous in both variables, a similar computation to the above for any $(x_0, t) \in \llbracket C \rrbracket \times [t_0, T]$ yields:

$$|(p_k^i)'(x_0, t) - \varphi_i'(x_0, t)| = |q_k^i(x_0, t) - \varphi_i'(x_0, t)| \leq \left\|q_k^i - \varphi_i'\right\|_{C^0(\llbracket C \rrbracket \times [t_0, T])} < 2^{-k-1}$$

thereby condition (2) is also satisfied.

The construction is uniformly computable for all $1 \leq i \leq n$ and $k \in \mathbb{N}$, so the proof is complete. □

4.2 Provable IVP Approximants

The following technical lemma proves the validity of a class of differential invariants capturing the "continuous dependence on initial conditions" characteristic of flow functions. Such invariants are then used in proving the desired error bounds under the presence of a bounded domain constraint $B(x)$ containing the true flow of the compact IVP $(f(x), C(X), [t_0, T])$. Note that this domain constraint is an assumption on the $\mathrm{FOL}_{\mathbb{R}}$ formula $B(x)$ itself, rather than a constraint on the values of the variables.

Lemma 4.11 (Continuous Dependence on Initial Conditions). *Let $(f(x), C(x), [t_0, T])$ be a compact IVP and $B(x) \in FOL_{\mathbb{R}}$. Further assume that the following holds:*

(1) *The flow $\varphi(x, t)$ of the compact IVP is well-defined on $\llbracket C \rrbracket \times [t_0, T]$.*
(2) *$\llbracket B \rrbracket \subset \mathbb{R}^n$ is a bounded set containing $\varphi(\llbracket C \rrbracket, [t_0, T])$.*

Then for all $K \in \mathbb{Q}^+$ greater than or equal to the Lipschitz constant of $f(x)$ on $\llbracket B \rrbracket$, for all LDA Φ, for all positive rational $h \in \mathbb{Q}^+$, for all sufficiently large $k \in \mathbb{N}$, the following is a valid differential invariant in dL*:*

$$\psi_k(x_0, x, g, t) \longrightarrow [x' = f(x), g' = Kg, t' = 1 \& t \leq T \land B(x)]\psi_k(x_0, x, g, t)$$

With $\psi_k(x_0, x, g, t)$ defined as:

$$\psi_k(x_0, x, g, t) \equiv t \geq t_0 \wedge g \geq 1 \wedge C(x_0) \wedge \|x - \Phi_k(x_0, t)\|^2 \leq \varepsilon(g, t)^2$$
$$\varepsilon(g, t) \equiv h(1 + t - t_0)g - h$$

A corresponding witness k can also be computed uniformly from the compact IVP, $B(x)$, Φ and h.

Lemma 4.11 computes some k witnessing the validity of the differential invariant, but it proves the stronger assertion that there exists some $k_0 \in \mathbb{N}$ such that for all $k \geq k_0$, the differential invariant at index k is valid. Such a threshold k_0 is in general not computable, because LDAs are not required to have a computable rate of convergence to the true flow to allow for more general approximants. This is similar to the difference between computably enumerable real numbers, which have computable sequences of rationals converging to them, and computable real numbers, which have computable sequences of rationals converging to them with *computable rates of convergence.*

Remark 4.12. Intuitively, the idea of the proof of Lemma 4.11 is to find some $\mathsf{FOL}_{\mathbb{R}}$ formula $\mathrm{Small}(x, t)$ that captures the difference between the flow $\varphi(x, t)$ and the approximation $\Phi_k(x, t)$ being small. By the continuous dependence of φ on its initial conditions, the differential invariant

$$\mathrm{Small}(x, t) \rightarrow [x' = f(x), t' = 1 \& t \leq T]\mathrm{Small}(x, t)$$

is valid and by Theorem 3.2 rule dInv will give a syntactic proof. However, while the dependence of the flow $\varphi(x, t)$ on its initial conditions is continuous, the error rate may grow like e^{Lt} where L is the Lipschitz constant of the vector field f on $\varphi([\![C]\!], [t_0, T])$. Since the theory of real exponential fields is not known to be decidable [36] and e^x is not directly expressible in dL (without extended terms), we will have to encode it via an ODE. In the definition of $\psi_k(x_0, x, g, t)$, the variable g represents the exponential function, as indicated by its ODE $g' = Kg$. The error function $\varepsilon(g, t)$ represents this error rate being scaled by the exponential function g. Lastly, as $f(x)$ is in general only *locally* Lipschitz, the domain constraint $B(x)$ is needed in order to obtain a *fixed* upper bound on the Lipschitz constant.

The following integral form of Grönwall's inequality is needed to prove Lemma 4.11.

Lemma 4.13 (Grönwall's inequality [28, 54]). *Let $[a, b] \subset \mathbb{R}$ be an interval of the real line, $u \in C([a, b], \mathbb{R})$ and $\alpha, \beta \in \mathbb{R}$. Further suppose that for all $t \in [a, b]$, we have:*

$$u(t) \leq \alpha + \int_a^t \beta u(s) ds$$

Then the following inequality holds for all $t \in [a, b]$:

$$u(t) \leq \alpha e^{\beta(t-a)}$$

With the lemma above, we are now ready to prove Lemma 4.11.

Proof of Lemma 4.11. As the claim only concerns validity of the differential invariant and the ODE is autonomous, we may assume without loss of generality that $t_0 = 0$ by translating the starting time if needed. Suppose that $\psi_k(x_0, x, g, t)$ is satisfied at some initial state, that is, there is some $t_1, g_0 \in \mathbb{R}, y_0, y \in \mathbb{R}^n$ such that $\psi_k(y_0, y, g_0, t_1)$ holds, giving the following conditions:

$$\psi_k(y_0, y, g_0, t_1) \equiv t_1 \geq t_0 \wedge g_0 \geq 1 \wedge C(y_0) \wedge \|y - \Phi_k(y_0, t_1)\|^2 \leq \varepsilon(g_0, t_1)^2$$

If $t_1 > T$ then the domain constraint $t \leq T$ is trivially false, so further assume without loss of generality that $t_1 \leq T$. Let $\varphi(x, t)$ denote the flow of the compact IVP and $\psi(g_0, t)$ denote the flow of g along $g' = Kg$ with initial condition $\psi(g_0, 0) = g_0$. By definition at time $t \in [t_1, T]$ the variable

x has the value $\varphi(y, t - t_1)$. Define the following function for $(x_0, t) \in [\![C]\!] \times [0, T]$ recording the difference between the true solution and the approximant at time t with initial condition x_0:

$$R_k(x_0, t) = \Phi_k(x_0, t) - \varphi(x_0, t)$$

To establish the validity of the invariant, it suffices to show (recall $t_0 = 0$)

$$\|\Phi_k(y_0, t) - \varphi(y, t - t_1)\| \leq \varepsilon(\psi(g_0, t - t_1), t)$$

for all $t \in [t_1, T]$ such that the domain constraint is maintained. This is because g satisfies the ODE $g' = Kg$, thus $\psi(g_0, t - t_1) = g_0 e^{K(t-t_1)} \geq g_0 \geq 1$, hence $g \geq 1$ is always satisfied by the assumption of $K \in \mathbb{Q}^+$. The condition $t \geq t_0$ is also satisfied as the ODE $t' = 1$ is strictly increasing, therefore $t \geq t_1 \geq t_0$. Finally $C(y_0)$ remains true since y_0 does not change along the ODE. To handle the non-trivial inequality, notice that $t \geq t_1$, therefore:

$$\begin{aligned}\Phi_k(y_0, t) - \varphi(y, t - t_1) =& R_k(y_0, t) + \varphi(y_0, t) - \varphi(y, t - t_1)\\ =& R_k(y_0, t) + \varphi(\varphi(y_0, t_1), t - t_1) - \varphi(y, t - t_1)\\ =& R_k(y_0, t) + \varphi(y_0, t_1) + \int_0^{t-t_1} f(\varphi(\varphi(y_0, t_1), s))ds - y - \int_0^{t-t_1} f(\varphi(y, s))ds\end{aligned}$$

Applying the triangle inequality gives:

$$\|\Phi_k(y_0, t) - \varphi(y, t - t_1)\| \leq \|R_k(y_0, t) + \varphi(y_0, t_1) - y\| + \int_0^{t-t_1} \|f(\varphi(\varphi(y_0, t_1), s)) - f(\varphi(y, s))\| \, ds \tag{1}$$

Now we crucially use the fact that $B(x)$ is both a domain constraint and assumed to contain the flow $\varphi(x_0, t)$ for $(x_0, t) \in [\![C]\!] \times [0, T]$ to see that for $s \in [0, t - t_1]$, we will always have $B(\varphi(\varphi(y_0, t_1), s))$ and $B(\varphi(y, s))$ (i.e., $\varphi(y_0, t_1 + s)$, $\varphi(y, s)$ both belong to the bounded set $[\![B]\!]$). Letting L denote the Lipschitz constant of $f(x)$ on $[\![B]\!]$ (recall that such a constant always exists since $f(x)$ is locally Lipschitz), we have:

$$\int_0^{t-t_1} \|f(\varphi(\varphi(y_0, t_1), s)) - f(\varphi(y, s))\| \, ds \leq L \int_0^{t-t_1} \|\varphi(\varphi(y_0, t_1), s) - \varphi(y, s)\| \, ds \tag{2}$$

We will now establish the following bound:

$$\|\varphi(\varphi(y_0, t_1), s) - \varphi(y, s)\| \leq \|\varphi(y_0, t_1) - y\| \, e^{Ls} \tag{3}$$

To do this, define $E \in C^1([0, t - t_1], \mathbb{R}^n)$ by $E(s) = \varphi(\varphi(y_0, t_1), s) - \varphi(y, s)$. Direct manipulations yield:

$$\begin{aligned}\|E(s)\| = \left\|E(0) + \int_0^s E'(r)dr\right\| &\leq \|E(0)\| + \int_0^s \|E'(r)\| \, dr\\ &= \|\varphi(y_0, t_1) - y\| + \int_0^s \|f(\varphi(\varphi(y_0, t_1), r)) - f(\varphi(y, r))\| \, dr\\ &\leq \|\varphi(y_0, t_1) - y\| + L \int_0^s \|\varphi(\varphi(y_0, t_1), r) - \varphi(y, r)\| \, dr\\ &= \|\varphi(y_0, t_1) - y\| + L \int_0^s \|E(r)\| \, dr\end{aligned}$$

Note that in this derivation, we again utilized the assumption that $f(x)$ is Lipschitz on $[\![B]\!]$ with Lipschitz constant L in the second to last inequality. Applying Grönwall's inequality (Lemma 4.13) with $u(s) = \|E(s)\|, \alpha = \|\varphi(y_0, t_1) - y\|, \beta = L$ then gives the desired bound equation (3). Applying this to inequality (2) results in:

$$\int_0^{t-t_1} \|f(\varphi(\varphi(y_0, t_1), s)) - f(\varphi(y, s))\| \, ds \leq L \, \|\varphi(y_0, t_1) - y\| \int_0^{t-t_1} e^{Ls} ds$$
$$= \|\varphi(y_0, t_1) - y\| \left(e^{L(t-t_1)} - 1\right)$$

Substituting this back into inequality (1) gives:

$$\|\Phi_k(y_0, t) - \varphi(y, t - t_1)\| \leq \|R_k(y_0, t) + \varphi(y_0, t_1) - y\| + \|\varphi(y_0, t_1) - y\| \left(e^{L(t-t_1)} - 1\right)$$

Recalling $R_k(y_0, t) = \Phi_k(y_0, t) - \varphi(y_0, t)$ yields:

$$\|\Phi_k(y_0, t) - \varphi(y, t - t_1)\| \leq \|R_k(y_0, t) + \Phi_k(y_0, t_1) - R_k(y_0, t_1) - y\|$$
$$+ \|R_k(y_0, t_1) - \Phi_k(y_0, t_1) + y\| \left(e^{L(t-t_1)} - 1\right)$$

Utilizing the triangle inequality and rearranging, we arrive at:

$$\|\Phi_k(y_0, t) - \varphi(y, t - t_1)\| \leq \|\Phi_k(y_0, t_1) - y\| \, e^{L(t-t_1)} + \|R_k(y_0, t) - R_k(y_0, t_1)\| + \|R_k(y_0, t_1)\| \, (e^{L(t-t_1)} - 1)$$

Recall that we may choose k arbitrarily large and $\|R_k\|_{[\![C]\!] \times [0,T]} \xrightarrow{k \to \infty} 0$, hence assume that k is large enough to witness $\|R_k\|_{[\![C]\!] \times [0,T]} \leq h$. Also by assumption on g_0, y_0, y, t_1, the following holds:

$$\|\Phi_k(y_0, t_1) - y\| \leq \varepsilon(g_0, t_1)$$

Rearranging yields:

$$\|\Phi_k(y_0, t) - \varphi(y, t - t_1)\| \leq (\varepsilon(g_0, t_1) + h) e^{L(t-t_1)} + \|R_k(y_0, t) - R_k(y_0, t_1)\| - h$$

Expanding $\varepsilon(g_0, t_1) = h(1 + t_1) g_0 - h$ by construction and requiring $K \geq L$ yields:

$$\begin{aligned}
\|\Phi_k(y_0, t) - \varphi(y, t - t_1)\| &\leq h(1 + t_1) g_0 e^{L(t-t_1)} + \|R_k(y_0, t) - R_k(y_0, t_1)\| - h \\
&\leq h(1 + t_1 - t + t) g_0 e^{K(t-t_1)} + \|R_k(y_0, t) - R_k(y_0, t_1)\| - h \\
&= h(1 + t) g_0 e^{K(t-t_1)} - h + \|R_k(y_0, t) - R_k(y_0, t_1)\| - h g_0 e^{K(t-t_1)} (t - t_1) \\
&= \varepsilon(\psi(g_0, t - t_1), t) + \|R_k(y_0, t) - R_k(y_0, t_1)\| - h g_0 e^{K(t-t_1)} (t - t_1) \\
&\leq \varepsilon(\psi(g_0, t - t_1), t) + \|R_k(y_0, t) - R_k(y_0, t_1)\| - h(t - t_1)
\end{aligned}$$

where the second equality uses the fact that $\psi(g_0, t)$ is the flow of $g' = Kg$ starting at $g(0) = g_0$, thus $\psi(g_0, t - t_1) = g_0 e^{K(t-t_1)}$. The final inequality follows from $t \geq t_1$ and $g_0 \geq 1$. Now define

$$M_k = \max_{y_0 \in [\![C]\!], t \in [t_0, T]} \left\|R'_k(y_0, t)\right\|$$

which is well-defined as $R'_k \in C^0([\![C]\!] \times [0, T], \mathbb{R}^n)$. Since $(\Phi'_k)_k$ converges uniformly to φ' on $[\![C]\!] \times [0, T]$, $(M_k)_k$ will converge to 0. Thus, choose k large enough so that $M_k \leq h$, which allows us to deduce:

$$\begin{aligned}
\varepsilon(\psi(g_0, t - t_1), t) + \|R_k(y_0, t) - R_k(y_0, t_1)\| - h(t - t_1) &\leq \varepsilon(\psi(g_0, t - t_1), t) + M_k(t - t_1) - h(t - t_1) \\
&\leq \varepsilon(\psi(g_0, t - t_1), t)
\end{aligned}$$

exactly as desired. Thus, for any $h > 0$, choosing k large enough such that the following conditions are met will witness the validity of the differential invariant.

- $\max_{y_0 \in [\![C]\!], t \in [0,T]} \|R_k(y_0, t)\| \leq h$
- $\max_{y_0 \in [\![C]\!], t \in [0,T]} \left\|R'_k(y_0, t)\right\| \leq h$

Furthermore, since maximums of computable functions are computable by Theorem 3.9, a satisfying index k can be found computably. To see that K can be effectively computed and chosen to be a rational, note that we only require $K \geq L$ to hold, so one can search through all positive rationals $K \in \mathbb{Q}^+$ and halt when the following $\mathrm{FOL}_{\mathbb{R}}$ formula is decided to be true

$$\forall x \forall y \left(B(x) \land B(y) \to \|f(x) - f(y)\|^2 \leq K^2 \|x - y\|^2\right)$$

and since $\mathbb{R}$ has a computable theory by quantifier elimination [53], this search is computable. □

The "continuous dependence on initial conditions" property proven by Lemma 4.11 provides control on the errors induced by LDAs, and is crucial in establishing completeness for LDAs in Theorem 5.1. The following example gives a sense of how this can be achieved.

Example 4.14. Consider the simple compact IVP $x' = x$, $x(0) = 1$ over the interval $[0, 5]$ (i.e., $C(x) \equiv x = 1$), which has a solution of $x(t) = e^t$ (and therefore we know that $\max_{t \in [0,5]} x(t) = e^5 < 300$). In this case, the Picard iterates will form a LDA on the compact time horizon $[0, 5]$. The Picard iterates of this ODE are:

$$\varphi_0(t) = x_0$$

$$\varphi_{n+1}(t) = x_0 + \int_0^t \varphi_n(s) ds$$

Listing out the first few terms

$$\varphi_0(t) = 1, \varphi_1(t) = 1 + t, \varphi_2(t) = 1 + t + \frac{t^2}{2}, \varphi_3(t) = 1 + t + \frac{t^2}{2} + \frac{t^3}{6}$$

Where $\varphi_n(t)$ is just the nth Taylor approximate, and $\varphi_n'(t) = \varphi_{n-1}(t)$. By Taylor's theorem, the nth remainder term R_n will be bounded by

$$|R_n| \leq \frac{e^5 5^{n+1}}{(n+1)!}$$

And similarly, M_n, the nth error in the derivative, will be bounded by

$$|M_n| = |R_{n-1}| \leq \frac{e^5 5^n}{n!}$$

Suppose one wants to generate a proof witnessing that some Picard iterate is within 10^{-3} of the true solution. Picking $h = 10^{-6}$, one has (note that the Lipschitz constant is 1 here and $t \in [0, 5]$)

$$|\varepsilon(\psi(1, t), t)| \leq 10^{-6}(1 + 5)e^5 + 10^{-6} \approx 8 \times 10^{-4} < 10^{-3}$$

Thus, if $\varepsilon(g, t)$ gives a valid differential invariant in the sense of Lemma 4.11, then the error of the approximant is necessarily bounded by 10^{-3}. Per the proof of the Lemma 4.11, n just needs to be picked large enough so that

$$|R_{n-1}|, |R_n| \leq 10^{-6}$$

and the differential invariant corresponding to $\varepsilon(g, t)$ is valid. By the bound given above, we see that for $n = 28$, $|R_{27}|, |R_{28}| \leq 2 \times 10^{-7}$. Now consider the invariant:

$$\psi_{28} \to [x' = f(x), t' = 1 \& t \leq 5 \land \|x\|^2 \leq 300]\psi_{28}$$

Since Picard iterates always satisfy $\psi_k(1, x(0), 1, 0)$ as they have the correct values at $t = 0$, the invariant generated above is valid and witnesses an error bound of at most 10^{-3}. Furthermore, this differential invariant can be independently verified by a proof checker for dL [8, 22], taking advantage of the effective axiomatisation of differential invariants [45] which reduces the verification of differential invariants down to questions of real arithmetic. When combined with formally-verified decision procedures for real arithmetic [33], this gives a complete verification of the validity of the invariant, illustrating how Lemma 4.11 can be used to produce proofs of error bounds of approximants.

Example 4.15 (Invariant for Moore–Greitzer). Recall that the dynamics of the Moore–Greitzer jet engine model is given by

$$\begin{aligned} u' &= f_1(u,v) = -v - 1.5u^2 - 0.5u^3 - 0.5 \\ v' &= f_2(u,v) = 3u - v \end{aligned}$$

with compact initial conditions $\Delta(u,v) \equiv 0.9 \leq u \wedge 0.9 \leq v \wedge u + v \leq 2$. Motivated by prior works which numerically computes reachability enclosures of this system via successive iterations [48, Table 1] over many time steps without corresponding syntactic proofs, we compute a *provable approximant* to the flow over one such time step, corresponding to $T = 0.02$. The approximant $\Phi(u_0, v_0, t)$ for which we will prove its accuracy is given by (recall that $\Phi(u_0, v_0, t) = (\Phi_1(u_0, v_0, t), \Phi_2(u_0, v_0, t))$):

$$\begin{aligned} \Phi_1(u_0,v_0,t) &= u_0 + tc_u^1(u_0,v_0) + t^2c_u^2(u_0,v_0) + t^3c_u^3(u_0,v_0) \\ c_u^1(u_0,v_0) &= -\frac{u_0^3}{2} - \frac{3u_0^2}{2} - v_0 - 0.5 \\ c_u^2(u_0,v_0) &= \frac{3u_0^5}{8} + \frac{15u_0^4}{8} + \frac{9u_0^3}{4} + \frac{3u_0^2v_0}{4} + 0.375u_0^2 + \frac{3u_0v_0}{2} - 0.75u_0 + \frac{v_0}{2} \\ c_u^3(u_0,v_0) &= -\frac{5u_0^7}{16} - \frac{35u_0^6}{16} - \frac{39u_0^5}{8} - \frac{7u_0^4v_0}{8} - 3.8125u_0^4 - \frac{7u_0^3v_0}{2} - 0.75u_0^3 \\ &\quad - \frac{13u_0^2v_0}{4} + \frac{3u_0^2}{4} - \frac{u_0v_0^2}{2} - u_0v_0 + 0.375u_0 - \frac{v_0^2}{2} - \frac{v_0}{6} + 0.125 \\ \Phi_2(u_0,v_0,t) &= v_0 + tc_v^1(u_0,v_0) + t^2c_v^2(u_0,v_0) + t^3c_v^3(u_0,v_0) \\ c_v^1(u_0,v_0) &= -\frac{u_0^3}{2} - \frac{3u_0^2}{2} - v_0 - 0.5 \\ c_v^2(u_0,v_0) &= 3u_0 - v_0 \\ c_v^3(u_0,v_0) &= \frac{3u_0^5}{8} + \frac{15u_0^4}{8} + \frac{5u_0^3}{2} + \frac{3u_0^2v_0}{4} + 1.125u_0^2 + \frac{3u_0v_0}{2} - 0.25u_0 + \frac{5v_0}{6} + 0.25 \end{aligned}$$

Such an approximant was computed by Picard iteration with appropriate rounding on the coefficients. It is important to note that LDA approximants are not limited to be Picard iterates, and the proofs of accuracy only depends on the true errors. To apply Lemma 4.11, the following constructs are needed:

- $h \in \mathbb{Q}^+$, bounding the error of the approximant.
- $B(u,v) \in \mathsf{FOL}_{\mathbb{R}}$ characterizing a bounded set that contains the flow.
- $K \in \mathbb{Q}^+$ larger than or equal to the Lipschitz constant of $f(u,v)$ on $[\![B]\!]$.

These values can be computed numerically by any method of choice. For example by numerically sampling, we see that the choices $h = 4 \times 10^{-3}, K = 8$ and

$$B(u,v) \equiv 0.781 < u < 1.109 \wedge 0.891 < v < 1.199 \wedge u + v < 2.25$$

satisfy such requirements, therefore the invariant

$$\psi(u_0, v_0, u, v, g, t) \rightarrow [u' = f_1(u, v), v' = f_2(u, v), g' = 8g, t' = 1 \& t \leq 0.02 \land B(u, v)]\psi(u_0, v_0, u, v, g, t)$$

with

$$\psi(u_0, v_0, u, v, g, t) \equiv t \geq 0 \land g \geq 1 \land \Delta(u_0, v_0) \land \|(u - \Phi_1(u_0, v_0, t), v - \Phi_2(u_0, v_0, t))\|^2 \leq \varepsilon(g, t)^2$$
$$\varepsilon(g, t) \equiv 4 \times 10^{-3}((1 + t)g - 1)$$

is valid and provable by dInv. Crucially, while the approximation and $u, K, B(u, v)$ were all obtained *numerically*, the validity of the invariant is *deductively proven* with a *proof* in dL that can be independently verified by proof checkers such as KeYmaera X [23]. Later examples build off of this differential invariant and eventually prove that the approximant $\Phi(u_0, v_0, t)$ has an error of at most 5×10^{-3} on $[\![\Delta]\!] \times [0, 0.02]$.

Remark 4.16. While Lemma 4.11 above applies to all LDAs, it would be interesting to know if the conditions can be relaxed to allow for approximants that do not converge in derivative. The above result still holds when there is only a *subsequence* of approximants that converge in derivative to φ'. Hence, the result remains true if we just assume that the approximants have bounded first and second derivatives, as this allows us to construct a convergent subsequence using Arzelà–Ascoli [54]. Even though one cannot generally compute this convergent subsequence directly, since differential invariants can be effectively decided by Theorem 3.2, it suffices to perform an unbounded search across all approximants, halting whenever one of the desired invariants is decided to be valid.

Building on Lemma 4.11, the following theorem reduces the problem of proving convergence of LDAs to arithmetic questions involving the exponential function.

Theorem 4.17 (Derivable LDA). *Let $(C(x), f(x), [t_0, T])$ be a compact IVP with Φ a LDA, $B(x)$ a $FOL_{\mathbb{R}}$ formula, $c, K \in \mathbb{Q}^+$ rational constants. Assume that the following holds:*

1. *The flow $\varphi(x, t)$ of the compact IVP is well-defined on $[\![C]\!] \times [t_0, T]$.*
2. *$[\![B]\!] \subset \mathbb{R}^n$ is a bounded set containing $\varphi([\![C]\!], [t_0, T])$.*
3. *K is greater than or equal to the Lipschitz constant of $f(x)$ on $[\![B]\!]$.*
4. *$c > 1$.*

Then for all $M, \varepsilon \in \mathbb{Q}^+$, for all sufficiently large $k \in \mathbb{N}$, the following proof rule is syntactically derivable in dL*, where x, g, t, x_0 are symbolic variables.*

$$\text{LDA}\quad \frac{\vdash g = c \land t = t_0 \rightarrow [g' = Kg, t' = 1 \& t \leq T]g \leq M}{\vdash C(x) \land x = x_0 \land t = t_0 \rightarrow [x' = f(x), t' = 1 \& t \leq T \land B(x)]\ \|x - \Phi_k(x_0, t)\|^2 \leq M^2\varepsilon^2}$$

For each $\varepsilon \in \mathbb{Q}^+$, a corresponding k can be computed uniformly in the compact IVP, Φ, c and ε.

Theorem 4.17 gives an effective way of reducing rigorous proofs for error bounds of LDAs in dL under the presence of some bounded domain $B(x)$ to the problem of proving upper bounds of the exponential function over a bounded interval. Section 4.3 shows that proofs of such upper bounds are always possible even if decidability of the exponential field is a famous open problem [36]. In contrast to the rational constants t_0, T, c, K, M, the variables x, g, t, x_0 in the proof rule are *symbolic*.

Proof. The proof directly follows from Lemma 4.11. Pick $n \in \mathbb{N}$ large enough such that $2^{-n}(1 + T - t_0) \leq \varepsilon$ is satisfied. Since Φ is a LDA, taking k to be large enough such that $\|\Phi_k - \varphi\|_{[\![C]\!] \times [t_0, T]} \leq 2^{-n}(c - 1)$ and Lemma 4.11 holds with $h = 2^{-n}$ gives the following:

1. $\forall x_0 \in [\![C]\!]\ \|x_0 - \Phi_k(x_0, t_0)\| \leq 2^{-n}(c - 1)$.
2. The following differential invariant is valid for $h = 2^{-n}$ (thus provable in dL by Theorem 3.2):

$$\psi_k(x_0, x, g, t) \rightarrow [x' = f(x), g' = Kg, t' = 1 \& t \leq T \land B(x)]\psi_k(x_0, x, g, t)$$

The desired proof in dL can now be constructed via the steps below by cutting in the differential invariant. First abbreviate

$$\alpha \equiv x' = f(x), g' = Kg, t' = 1 \& t \leq T \wedge B(x)$$

$$\text{→R,DG,∃R}\,\dfrac{\text{cut,→L}\,\dfrac{\mathbb{R}\,\dfrac{*}{C(x), x = x_0, g = c, t = t_0 \vdash \psi_k(x_0, x, g, t)} \quad \text{dInv}\,\dfrac{*}{\psi_k(x_0, x, g, t) \vdash [\alpha]\psi_k(x_0, x, g, t)} \quad \dfrac{}{\textcircled{1}}}{C(x), x = x_0, t = t_0, g = c \vdash [x' = f(x), g' = Kg, t' = 1 \& t \leq T \wedge B(x)]\, \|x - \Phi_k(x_0, t)\|^2 \leq M^2\varepsilon^2}}{\vdash C(x) \wedge x = x_0 \wedge t = t_0 \rightarrow [x' = f(x), t' = 1 \& t \leq T \wedge B(x)]\, \|x - \Phi_k(x_0, t)\|^2 \leq M^2\varepsilon^2}$$

The left premise closes by $\mathbb{R}$ from item (1), the second premise closes by Lemma 4.11, and the final remaining premise is

$$\textcircled{1} \equiv C(x), x = x_0, t = t_0, g = c, [\alpha]\psi_k(x_0, x, g, t) \vdash [\alpha]\, \|x - \Phi_k(x_0, t)\|^2 \leq \varepsilon^2 M^2$$

Which can be handled with dW and cutting in the bound $[\alpha]g \leq M$ with dC. Crucially the application of DGi to remove $x' = f(x)$ is sound since $x \notin K, M$.

$$\text{dC,dW}\,\dfrac{\mathbb{R}\,\dfrac{*}{g \leq M, t \leq T, \psi_k(x_0, x, g, t) \vdash \|x - \Phi_k(x_0, t)\|^2 \leq \varepsilon^2 M^2} \quad \text{DGi}\,\dfrac{\textcircled{2}}{g = c, t = t_0 \vdash [\alpha]g \leq M}}{x = x_0, t = t_0, g = c, [\alpha]\psi_k(x_0, x, g, t) \vdash [\alpha]\, \|x - \Phi_k(x_0, t)\|^2 \leq \varepsilon^2 M^2}$$

where the remaining premise on the right is

$$\textcircled{2} \equiv g = c, t = t_0 \vdash [g' = Kg, t' = 1 \& t \leq T]g \leq M$$

For the left premise, notice that the following is a valid formula of $\mathsf{FOL}_{\mathbb{R}}$, and therefore provable:

$$t \leq T \wedge g \leq M \wedge \psi_k(x, x_0, g, t) \longrightarrow \|x - \Phi_k(x_0, t)\|^2 \leq (2^{-n}(1 + T - t_0)M)^2$$

thus, the left premise closes by our choice of $n \in \mathbb{N}$. The proof of the desired formula has now been reduced to an upper bound on the exponential function (premise ②), completing the derivation. Since k was only required to satisfy conditions (1), (2) and a satisfying witness for Lemma 4.11 can be computed, such a k can be computed as well, completing the proof of the theorem. □

Example 4.18 (Constrained Exponential bound for Moore-Greitzer). Theorem 4.17 applies to the Moore-Greitzer jet engine model introduced in Example 4.4 with its invariant established in Example 4.15. We apply proof rule LDA using

- $B(u, v) \equiv 0.781 < u < 1.109 \wedge 0.891 < v < 1.199 \wedge u + v < 2.25$
- $K = 8$
- $c = 1.1$
- $\varepsilon = 4 \times 10^{-3} \times (1 + 0.02)$
- $M = 1.2$

Using these values, LDA proves the following

$$\text{LDA}\,\dfrac{g = 1.1, t = 0 \vdash [g' = 8g, t' = 1 \& t \leq 0.02]g \leq 1.2}{\Delta(u_0, v_0), u = u_0, v = v_0, t = 0 \vdash [(u', v') = f(u, v) \& t \leq 0.02 \wedge B(u, v)]\, \|(u, v) - \Phi(u_0, v_0, t)\|^2 < (5 \times 10^{-3})^2}$$

where the constant 5 was chosen as

$$\varepsilon M = 4 \times 1.2 \times 1.02 \times 10^{-3} < 5 \times 10^{-3}$$

As the derivation shows, the proof rule LDA reduced the problem of proving an error bound of 5×10^{-3} to the problem of upper bounding exponentials on $[0, 0.02]$. Importantly, while all of the values were chosen numerically, the proof rule LDA is derived. Therefore the validity of the formula is backed up by a corresponding *syntactic proof*.

Theorem 4.17 still holds even if $(\Phi_k)_k$ does not converge in derivative, as long as it has bounded first and second time derivatives (implicitly requiring it to be twice differentiable), since Lemma 4.11 still holds in this case per Remark 4.16.

4.3 Provable Taylor Bounds on Exponentials

Theorem 4.17 reduced the proof of error bounds for LDAs to proving upper bounds for the exponential function on compact intervals. In this section, we show that dL is capable of proving arbitrarily accurate upper bounds on the exponential function via Taylor polynomials on the compact interval $[0, T]$.

Proposition 4.19 (provable Taylor approximants). *Let $K, T \in \mathbb{Q}^+$ be rational constants. For all sufficiently large $n \in \mathbb{N}$, there is a syntactic term $\theta_n \in \mathbb{Q}[t]$ such that the following is a valid differential invariant*

$$g \le \theta_n \rightarrow [g' = Kg, t' = 1 \& t \le T] g \le \theta_n$$

Furthermore, $\theta_n \rightarrow e^{Kt}$ on $[-T, T]$ as $n \rightarrow \infty$ where θ_n is treated as a function in t. Finally, for all $n \in \mathbb{N}$ we have $\theta_n(0) = 1$ and θ_n can be computed uniformly in K, T, n.

Proof. For $n \in \mathbb{N}$, let us denote $q_n(t)$ as the nth Taylor approximant of e^{Kt} i.e.,

$$q_n(t) = \sum_{i=0}^{n} \frac{K^i t^i}{i!}$$

Let

$$\theta_n(t) = q_n(t) + \frac{Mt^n}{n!} \qquad M = \frac{K^{n+1}T}{n - KT}$$

which is well-defined for all $n > KT$. By the Darboux inequality [45, Corollary 3.2], the validity of the invariant follows from the validity of $(\theta_n(t))' \ge K\theta_n(t)$. Computing $(\theta_n(t))'$ gives

$$(\theta_n(t))' = Kq_{n-1}(t) + \frac{Mt^{n-1}}{(n-1)!}$$

So we have

$$\begin{aligned} (\theta_n(t))' - K\theta_n(t) &= \frac{Mt^{n-1}}{(n-1)!} - \frac{K^{n+1}t^n}{n!} - \frac{KMt^n}{n!} \\ &\ge \frac{t^{n-1}}{n!}\left(nM - KMT - K^{n+1}T\right) = \frac{t^{n-1}}{n!}\left((n - KT)M - K^{n+1}T\right) = 0 \end{aligned}$$

Therefore the invariant is indeed valid for all $n > KT$. To witness the desired convergence, note

$$\frac{Mt^n}{n!} \xrightarrow{n \to \infty} 0$$

and $q_n \xrightarrow{n \to \infty} e^{Kt}$ on $[-T, T]$ by Taylor's theorem. The proof is therefore complete. □

It now follows that dL is capable of proving arbitrarily accurate upper bounds on the exponential function on bounded intervals.

Corollary 4.20 (bounded exponentials). *Let $c, K \in \mathbb{Q}^+$ be constants and $[t_0, T] \in \mathbb{IQ}$ be a rational interval. For all $M \in \mathbb{Q}^+$ that satisfy $ce^{K(T-t_0)} < M$, the following formula is provable in* dL*:*

$$g = c \land t = t_0 \rightarrow [g' = Kg, t' = 1 \& t \le T] g \le M$$

Proof. We first begin with standard reductions using DG and dInv, reducing the proof down to upper bounds on the standard exponential IVP $x' = Kx$ with initial condition $x(t_0) = 1$.

$$
{\scriptstyle\rightarrow\text{R,DG},\exists\text{R}}\,\dfrac{
 {\scriptstyle\text{K}}\,\dfrac{
  {\scriptstyle[\,]\wedge,\wedge\text{R}}\,\dfrac{
    {\scriptstyle\text{dInv}}\,\dfrac{*}{g = cx \vdash [g' = Kg, x' = Kx, t' = 1 \& t \le T]g = cx}
    \qquad
    {\scriptstyle\text{DGi}}\,\dfrac{\dfrac{\textcircled{1}}{x = 1, t = t_0 \vdash [x' = Kx, t' = 1 \& t \le T]x \le \frac{M}{c}}}{x = 1, t = t_0 \vdash [g' = Kg, x' = Kx, t' = 1 \& t \le T]x \le \frac{M}{c}}
  }{g = c, x = 1, t = t_0 \vdash [g' = Kg, x' = Kx, t' = 1 \& t \le T]\left(x \le \frac{M}{c} \wedge g = cx\right)}
 }{g = c, x = 1, t = t_0 \vdash [g' = Kg, x' = Kx, t' = 1 \& t \le T]g \le M}
}{\vdash g = c \wedge t = t_0 \rightarrow [g' = Kg, t' = 1 \& t \le T]g \le M}
$$

Where the left premise closes as it is a valid differential invariant. Theorem 4.19 now gives some $\theta(s) \in \mathbb{Q}[s]$ such that $c\,\|\theta\|_{[0,T-t_0]} \le M$, $\theta(0) = 1$, and the following differential invariant is valid:

$$x \le \theta(s) \rightarrow [x' = Kx, s' = 1 \& s \le T - t_0]x \le \theta(s)$$

Note that this is only possible by our assumption of $ce^{K(T-t_0)} < M$. Premise ① can now be handled by cutting in this invariant on $\theta(s)$.

$$
{\scriptstyle\text{DG},\exists\text{R}}\,\dfrac{
 {\scriptstyle\text{dC,dInv}}\,\dfrac{
  {\scriptstyle\text{dC}}\,\dfrac{
   {\scriptstyle\text{DGi}}\,\dfrac{
    {\scriptstyle\text{cut,dInv,K}}\,\dfrac{
     {\scriptstyle\mathbb{R}}\,\dfrac{*}{x = 1, s = 0, t = t_0 \vdash x \le \theta(s)}
     \qquad
     {\scriptstyle\text{dC,dInv}}\,\dfrac{
      {\scriptstyle\text{dW}}\,\dfrac{
       {\scriptstyle\mathbb{R}}\,\dfrac{*}{s \ge 0, s \le T - t_0 \vdash c\theta(s) \le M}
      }{s = 0 \vdash [x' = Kx, s' = 1 \& s \le T - t_0 \wedge s \ge 0]\left(x \le \theta(s) \rightarrow x \le \frac{M}{c}\right)}
     }{s = 0 \vdash [x' = Kx, s' = 1 \& s \le T - t_0]\left(x \le \theta(s) \rightarrow x \le \frac{M}{c}\right)}
    }{x = 1, s = 0, t = t_0 \vdash [x' = Kx, s' = 1 \& s \le T - t_0]x \le \frac{M}{c}}
   }{x = 1, s = 0, t = t_0 \vdash [x' = Kx, s' = 1, t' = 1 \& s \le T - t_0]x \le \frac{M}{c}}
  }{x = 1, s = 0, t = t_0 \vdash [x' = Kx, s' = 1, t' = 1 \& t \le T \wedge s = t - t_0]x \le \frac{M}{c}}
 }{x = 1, s = 0, t = t_0 \vdash [x' = Kx, s' = 1, t' = 1 \& t \le T]x \le \frac{M}{c}}
}{x = 1, t = t_0 \vdash [x' = Kx, t' = 1 \& t \le T]x \le \frac{M}{c}}
$$

Where the left premise closes as $\theta(0) = 1$, and the right premise closes since θ was constructed to satisfy $c\,\|\theta\|_{[0,T-t_0]} \le M$, which is therefore provable by $\mathbb{R}$. This completes the proof. □

Chaining up the results of Theorem 4.17 and Theorem 4.19 gives complete proofs for accuracy bounds of LDAs for compact IVPs. This has many important consequences regarding the proof theory of dL which are listed below. The first of which says that for any LDA, for any desired accuracy, one can derive a proof certifying this accuracy within dL assuming the presence of some domain constraint.

Theorem 4.21 (completeness for LDAs with Domain Constraints). *Let $(f(x), C(x), [t_0, T])$ be a compact IVP, Φ a LDA and $B(x)$ a FOL$_\mathbb{R}$ formula. Assume that the following holds:*

1. *The flow $\varphi(x, t)$ of the compact IVP is well defined on $[\![C]\!] \times [t_0, T]$.*
2. *$[\![B]\!] \subset \mathbb{R}^n$ is a bounded set containing $\varphi([\![C]\!], [t_0, T])$.*

Then for all $\varepsilon \in \mathbb{Q}^+$, for all sufficiently large $k \in \mathbb{N}$, the following formula is provable in dL.

$$C(x) \wedge x = x_0 \wedge t = t_0 \rightarrow [x' = f(x), t' = 1 \& t \le T \wedge B(x)]\,\|x - \Phi_k(x_0, t)\|^2 \le \varepsilon^2$$

For each $\varepsilon \in \mathbb{Q}^+$ a corresponding k can be computed uniformly from the compact IVP, Φ and ε.

Proof. Follows directly via Theorem 4.17 and Corollary 4.20. □

Example 4.22 (Constrained bound for Moore-Greitzer). Following Theorem 4.19, we prove

$$g = 1.1, t = 0 \vdash [g' = 8g, t' = 1 \& t \le 0.02]g \le 1.2$$

This derivation combined with Example 4.18 proves the validity of the following formula

$$\begin{aligned}&\Delta(u_0, v_0) \land t = 0 \land u = u_0 \land v = v_0 \rightarrow\\&[(u', v') = f(u, v), t' = 1 \& t \leq 0.02 \land B(u, v)]\ \|(u, v) - \Phi(u_0, v_0, t)\|^2 < (0.005)^2\end{aligned}$$

which is a particular instance of Theorem 4.21, syntactically proving an error bound of 0.005 for the approximation $\Phi(u_0, v_0, t)$ under the assumption of the domain constraint $B(u, v)$.

The following result syntactically proves the classical Stone–Weierstraß theorem in dL for flows of compact IVPs under the assumption of some bounded domain constraint. That is, flows of compact IVPs can be approximated up to arbitrary accuracy with (rational) polynomials.

Theorem 4.23 (Weierstrass Approximation with Domain Constraints). *For a given compact IVP $(f(x), C(x), [t_0, T])$ and $B(x)$ a FOL$_{\mathbb{R}}$ formula, suppose that the following holds:*

(1) *The flow $\varphi(x, t)$ of the compact IVP is well defined on $[\![C]\!] \times [t_0, T]$.*
(2) *$[\![B]\!] \subset \mathbb{R}^n$ is a bounded set containing $\varphi([\![C]\!], [t_0, T])$.*

Then there is a computable sequence $(\theta_k)_k \in \mathbb{Q}^n[x_0, t]$ of approximants such that the following formulas are provable for all $k \in \mathbb{N}$:

$$C(x) \land x = x_0 \land t = t_0 \rightarrow [x' = f(x), t' = 1 \& t \leq T \land B(x)]\ \|x - \theta_k(x_0, t)\|^2 \leq 2^{-2k}$$

Proof. Follows directly from Theorem 4.21 and Theorem 4.10. □

Theorem 4.21 and Theorem 4.23 proves that under the presence of some bounded domain constraint, flows of compact IVPs can be arbitrarily approximated by polynomials with provably accurate error bounds. As such, one can *always* prove desired (open) properties of flows of compact IVPs by transferring to the case of polynomials, where the properties can then be proven by quantifier elimination with the proof rule $\mathbb{R}$. The remaining sections handle the case where such domain constraints are not assumed to exist *a priori*.

5 Proving Domain Constraints and Bounded Completeness

A key assumption in the previous section is the existence of a FOL$_{\mathbb{R}}$ formula $B(x)$ that bounds the evolution of the flow induced by the ODE, acting as a domain constraint. Such an assumption was a natural consequence of the fact that non-linear polynomial vector fields are only locally Lipschitz, and therefore some *a priori* bound on the flow is required in order to computably utilize the continuity of the flow. In this section, we will first show how to eliminate such assumptions by proving them directly for compact IVPs and obtain a stronger version of Theorem 4.21. Utilizing this, we prove that dL's axiomatization [41, 45, 52] enjoys completeness properties over compact time horizons without assuming bounded domain constraints. And finally, we discuss methods of handling domain constraints symbolically. Along the way, the syntactic provability of several axioms within dL that synthesize fundamental mathematical properties of ODEs is established, which are of independent interest.

5.1 Error Bounds Without Domain Constraints

Our main goal is the following strengthening of Theorem 4.21, which *does not* assume the existence of a bounded domain constraint.

Theorem 5.1 (Completeness for LDAs). *Let $(f(x), C(x), [t_0, T])$ be a compact IVP with a well-defined flow $\varphi : [\![C]\!] \times [t_0, T] \rightarrow \mathbb{R}^n$ and Φ a LDA. Then for all $\varepsilon \in \mathbb{Q}^+$, for all sufficiently large $k \in \mathbb{N}$, the following formula is provable in* dL.

$$C(x) \land x = x_0 \land t = t_0 \rightarrow [x' = f(x), t' = 1 \& t \leq T]\ \|x - \Phi_k(x_0, t)\|^2 < \varepsilon^2$$

Furthermore, a satisfying k can be computed uniformly from the compact IVP, Φ and ε.

Remark 5.2. Theorem 5.1 can be understood as a "completeness for convergence of LDAs" result. In the sense that if a sequence of definable functions $(g_k)_k : [\![C]\!] \times [t_0, T] \to \mathbb{R}^n$ converges to the true flow $\varphi : [\![C]\!] \times [t_0, T] \to \mathbb{R}^n$ in the C^1 norm, then their convergence in the C^0 norm can be syntactically proven in dL. While this result assumes the existence of the flow for a sufficient duration, Theorem 5.12 shows that dL is complete for such existence properties as well. Corollary 5.6 further strengthens this theorem by weakening the assumption to C^0 convergence instead of C^1 convergence.

To prove Theorem 5.1, the following lemma is needed.

Lemma 5.3 (completeness for bounded flows). *Let $(f(x), C(x), [t_0, T])$ be a compact IVP, Φ a LDA and $R \in \mathbb{Q}^+$. Assume that the following holds:*

1. *The flow $\varphi(x, t)$ of the compact IVP is well-defined on $[\![C]\!] \times [t_0, T]$.*
2. *$\varphi([\![C]\!], [t_0, T]) \subseteq B(0, R)$, where $B(0, R)$ is the open ball of radius R in $\mathbb{R}^n$.*

Then the following formula is provable in dL*.*

$$C(x) \land t = t_0 \to [x' = f(x), t' = 1 \& t \le T] \, \|x\|^2 < R^2$$

Proof. First note that rule Enc reduces the problem to:

$$\text{Enc}\,\frac{C(x) \land t = t_0 \vdash [x' = f(x), t' = 1 \& t \le T \land \|x\|^2 \le R^2] \, \|x\|^2 < R^2}{C(x) \land t = t_0 \vdash [x' = f(x), t' = 1 \& t \le T] \, \|x\|^2 < R^2}$$

By Theorem 4.10, we may compute some LDA Φ for this compact IVP. Now do an a priori unbounded search on pairs $(\varepsilon, k) \in \mathbb{Q}^+ \times \mathbb{N}$ such that the following formulas are provable in dL.

$$C(x) \land x = x_0 \land t = t_0 \to [x' = f(x), t' = 1 \& t \le T \land \|x\|^2 \le R^2] \, \|x - \Phi_k(x_0, t)\|^2 \le \frac{\varepsilon}{2}$$

$$\forall x_0 \forall t \left(t_0 \le t \land t \le T \land C(x_0) \to \|\Phi_k(x_0, t)\|^2 < R^2 - \frac{\varepsilon}{2}\right)$$

In fact, such pairs necessarily exist and the search is bounded. To see this, note that $\varphi([\![C]\!], [t_0, T])$ is a compact subset of the open set $B(0, R)$ by assumption, so there exists some $\varepsilon \in \mathbb{Q}^+$ such that $B(\varphi([\![C]\!], [t_0, T]), \varepsilon) \subseteq B(0, R)$. By choosing this ε and $k \in \mathbb{N}$ sufficiently large, the first formula will be valid and therefore provable by Theorem 4.21. The second formula is true and therefore provable by $\mathbb{R}$ for all sufficiently large $k \in \mathbb{N}$ since Φ is a LDA. Hence, we can computably find a pair (ε, k) with corresponding proofs to the formulas above. Now applying axiom V (Lemma B.1) and dW shows that $t_0 \le t \le T$ and $C(x_0)$ are always satisfied during the evolution of the ODE in the first formula. As such, applying these axioms on the formulas together with V proves

$$\begin{aligned}&C(x) \land x = x_0 \land t = t_0 \to \\ &[x' = f(x), t' = 1 \& t \le T \land \|x\|^2 \le R^2] \left(\|x - \Phi_k(x_0, t)\|^2 \le \frac{\varepsilon}{2} \land \|\Phi_k(x_0, t)\|^2 < R^2 - \frac{\varepsilon}{2}\right)\end{aligned}$$

from which the remaining premise introduced by Enc follows. □

Theorem 5.1 can now be proven using Lemma 5.3 and Theorem 4.21.

Proof of Theorem 5.1. First note that for any positive rational $R \in \mathbb{Q}^+$, cutting in the domain constraint $\|x\|^2 < R^2$ with dC (and applications of $\exists$L to introduce the variable x_0) reduces the proof obligation to proving the following premises:

$$\vdash C(x) \land x = x_0 \land t = t_0 \to [x' = f(x), t' = 1 \& t \le T \land \|x\|^2 < R^2]\, \|x - \Phi_k(x_0, t)\|^2 < \varepsilon^2$$

$$\vdash C(x) \land t = t_0 \to [x' = f(x), t' = 1 \& t \le T]\, \|x\|^2 < R^2$$

Hence, we may do a bounded search on the pair $(R, k) \in \mathbb{Q}^+ \times \mathbb{N}$ such that the above are provable. This is a bounded search since $\varphi([\![C]\!], [t_0, T])$ is a compact set, so for all sufficiently large R we have $\varphi([\![C]\!], [t_0, T]) \subseteq B(0, R)$, from which the provability of the two premises follows from Theorem 4.21 and Lemma 5.3, respectively. Furthermore, this is a computable search as Theorem 4.21 and Lemma 5.3 both hold computably. Once such a pair (R, k) has been found with corresponding proofs, the premises are proven and therefore the proof is complete by applying axiom dC. □

Theorem 5.1 proves that for all compact IVPs, for all corresponding LDAs, for all $\varepsilon \in \mathbb{Q}^+$, one can find some corresponding proof in dL certifying the LDA to be at most ε away from the true solution. The following example applies this theorem to Moore–Greitzer's model of jet engines.

Example 5.4 (Unconstrained bound for Moore–Greitzer). Example 4.22 proved an error bound of 0.005 under the assumption of a domain constraint $B(u, v)$ given by

$$B(u, v) \equiv 0.781 < u < 1.109 \land 0.891 < v < 1.199 \land u + v < 2.25$$

Applying Theorem 5.1 and utilizing the constrained bound proven in Example 4.22 then proves an error bound of 0.005 without assuming domain constraints.

$$\Delta(u_0, v_0, t) \land t = 0 \land u = u_0 \land v = v_0 \to$$
$$[(u', v') = f(u, v), t' = 1 \& \le 0.02]\, \|(u, v) - \Phi(u_0, v_0, t)\|^2 < 0.005^2$$

As such, we have syntactically proven the accuracy of a numerical approximation using deductive logic reasoning.

The following theorem proves the Stone–Weierstraß theorem (Theorem 4.23) without domain constraints.

Theorem 5.5 (Stone-Weierstrass). *Let $(f(x), C(x), [t_0, T])$ be a compact IVP with well-defined flow $\varphi(x, t) : [\![C]\!] \times [t_0, T] \to \mathbb{R}^n$. Then there is a computable sequence $(\theta_k)_k \in \mathbb{Q}^n[x_0, t]$ of approximants such that the following formulas are provable for all $k \in \mathbb{N}$:*

$$C(x) \land x = x_0 \land t = t_0 \to [x' = f(x), t' = 1 \& t \le T]\, \|x - \theta_k(x_0, t)\|^2 \le 2^{-2k}$$

Proof. Follows directly by Theorem 4.10 and Theorem 5.1. □

Theorem 5.1 can also be viewed as a "completeness for convergence" result that requires C^1 convergence and proves C^0 convergence. By utilizing Theorem 4.10 to provably compute a correct LDA, it is possible to strengthen Theorem 5.1 and only require C^0 convergence.

Corollary 5.6 (Completeness for convergence). *Let $(f(x), C(x), [t_0, T])$ be a compact IVP with well-defined flow $\varphi : [\![C]\!] \times [t_0, T] \to \mathbb{R}^n$. Further suppose that $(f_k)_k$ is a sequence of $\mathrm{FOL}_{\mathbb{R}}$ definable functions with $f_k : [\![C]\!] \times [t_0, T] \to \mathbb{R}^n$. Then dL is complete for convergence:*

$$\vDash (f_k)_k \xrightarrow{n \to \infty} \varphi \qquad \Longrightarrow \qquad \vdash (f_k)_k \xrightarrow{n \to \infty} \varphi$$

i.e., if $(f_k)_k$ converges to φ in $C^0([\![C]\!] \times [t_0, T], \mathbb{R}^n)$, then for every $\varepsilon \in \mathbb{Q}^+$, for all sufficiently large $k \in \mathbb{N}$, the following formula is provable

$$C(x) \land x = x_0 \land t = t_0 \to [x' = f(x), t' = 1 \& t \le T]\, \|f_k(x_0, t) - x\|^2 < \varepsilon^2$$

Furthermore, a satisfying k can be computed uniformly from the compact IVP, ε and $(f_k)_k$.

Proof. Let Φ be some LDA of the compact IVP computed by Theorem 4.10, $\varepsilon \in \mathbb{Q}^+$ be the desired accuracy. Let k be large enough such that Theorem 5.1 holds with an accuracy of $\frac{\varepsilon}{3}$ and $\|f_k - \varphi\|_{[\![C]\!]\times[t_0,T]} < \frac{\varepsilon}{3}$ is satisfied. It suffices to show that the formula

$$C(x) \wedge x = x_0 \wedge t = t_0 \rightarrow [x' = f(x), t' = 1 \& t \leq T]\, \|f_k(x_0, t) - x\|^2 < \varepsilon^2$$

is provable. Indeed, Theorem 5.1 and the choice of k imply that the following formula is provable

$$C(x) \wedge x = x_0 \wedge t = t_0 \rightarrow [x' = f(x), t' = 1 \& t \leq T]\, \|\Phi_k(x_0, t) - x\|^2 < \left(\frac{\varepsilon}{3}\right)^2$$

By construction and $\mathbb{R}$, it is also provable that $\|\Phi_k - f_k\|_{[\![C]\!]\times[t_0,T]} < \frac{2\varepsilon}{3}$. Hence an application of axiom K implies that the following is provable, completing the proof. □

$$C(x) \wedge x = x_0 \wedge t = t_0 \rightarrow [x' = f(x), t' = 1 \& t \leq T]\, \|f_k(x_0, t) - x\|^2 < \left(\frac{\varepsilon}{3} + \frac{2\varepsilon}{3}\right)^2$$

5.2 Symbolic Domain Constraints and Completeness on Compact Time Horizons

This section establishes completeness properties of dL over compact time horizons for compact IVPs. The main proof strategy is to utilize our results in previous sections which show that dL is complete for LDAs of compact IVPs, thereby reducing properties of such compact IVPs to decidable sentences in real arithmetic. This section also explores to what extent such results can be applied to IVPs with symbolic initial conditions that are not constrained to compact sets. The main technical results can be encapsulated in the following theorem, which asserts the provability of various axioms and proof rules in dL.

Theorem 5.7. *The following axioms and rules are syntactically derivable in* dL*, thus sound. Where* $M, R > 0$ *are symbolic variables, and* $B(x), Q, \Gamma_1, \Gamma_2, P_1, P_2$ *are* $FOL_{\mathbb{R}}$ *formulas with* $B(x)$ *characterizing a bounded set.*

$$\text{StepDual}_{\rightarrow} \quad t \leq \tau \wedge [x' = f(x), t' = 1 \& t \leq \tau]B(x) \rightarrow \langle x' = f(x), t' = 1 \& B(x)\rangle t = \tau$$

$$\text{StepDual}_{\leftarrow} \quad \langle x' = f(x), t' = 1 \& Q\rangle t \geq \tau \rightarrow [x' = f(x), t' = 1 \& t \leq \tau]Q$$

$$\text{StepEx} \quad \begin{array}{l} \forall y \left(y \in B[x_0, R] \rightarrow \|f(y)\|^2 \leq M^2\right) \rightarrow \\ \left(x = x_0 \wedge t = t_0 \rightarrow \langle x' = f(x), t' = 1 \& x \in B[x_0, R]\rangle t \geq t_0 + \dfrac{R}{M}\right) \end{array}$$

$$\text{StepExt} \quad \dfrac{\begin{array}{c} t = t_0, P_1 \vdash \Gamma_2 \\ \Gamma_1 \vdash [x' = f(x), t' = 1 \& t \leq t_0]P_1 \\ \Gamma_2 \vdash [x' = f(x), t' = 1 \& t \leq t_0 + t_1]P_2 \end{array}}{t \leq t_0, \Gamma_1 \vdash [x' = f(x), t' = 1 \& t \leq t_0 + t_1]((t \leq t_0 \rightarrow P_1) \wedge (t > t_0 \rightarrow P_2))}$$

Remark 5.8. These axioms are capable of symbolically simulating a basic algorithm for certifying existence of ODEs, which essentially mimics the classical proof [30], such an algorithm has also been presented explicitly in more recent work [27]. Example 5.10 shows how this can be done.

The following provides some intuitive explanation for the axioms/proof rules in Theorem 5.7.

- Axioms StepDual$_{\rightarrow}$, StepDual$_{\leftarrow}$ provide a duality between box and diamond modalities on compact time horizons for ODEs. These axioms are useful in proving that the flow is bounded within some bounded set over a fixed time interval. It is also worth noting that while axiom StepDual$_{\rightarrow}$ requires a bounded set, axiom StepDual$_{\leftarrow}$ places no requirements on the domain constraint Q as it follows from the uniqueness of flows for ODEs.

- Axiom StepEx is a quantitative version of the classical Picard-Lindelöf theorem presented in the language of dL, allowing one to symbolically prove that the solution exists for a duration of $\frac{R}{M}$, which is a lower-bound on how long it takes for the solution to escape the ball $B[x_0, R]$.
- Proof rule StepExt provides a way of concatenating information proven for different time steps together over the entire time step. Similar to the proof of computability of solutions to IVPs [27] which iteratively chains up Picard iterations at various time steps.

All of the above axioms/proof rules are syntactically derivable using just dL's axiomatization [45, 52]. It is important to note that the axioms in Theorem 5.7 hold *symbolically* and are *not* limited to compact IVPs (e.g., x_0, τ, t, T, M, R are symbolic variables).

In order to prove Theorem 5.7, the following lemma is needed, which establishes the provability of many fundamental properties of ODEs, and is therefore of independent interest.

Lemma 5.9. *The following axioms are derivable in* dL*, where Q, Q_1, Q_2 are $FOL_{\mathbb{R}}$ formulas and e is a term.*

$$\text{Rev}\quad P\rightarrow[x' = f(x)\&Q]\langle x' = -f(x)\&Q\rangle P$$

$$\text{Stuck}\quad t = t_0\rightarrow([x' = f(x), t' = 1\&t \leq t_0]P \leftrightarrow P)$$

$$\text{Idem}\quad \langle x' = f(x)\&Q\rangle P\rightarrow\langle x' = f(x)\&Q \land \langle x' = f(x)\&Q\rangle P\rangle P$$

$$\text{Uniq'}\quad \begin{array}{l}\langle x'=f(x)\&Q_1\rangle P_1 \land \langle x'=f(x)\&Q_2\rangle P_2\rightarrow\\ \langle x'=f(x)\&Q_1\land Q_2\rangle\ (P_1\land\langle x'=f(x)\&Q_2\rangle P_2)\lor\langle x'=f(x)\&Q_1\land Q_2\rangle\ (P_2\land\langle x'=f(x)\&Q_1\rangle P_1)\end{array}$$

$$\text{IVT}\quad \begin{array}{l}e \leq 0 \land \langle x' = f(x), t' = 1\&Q\rangle\ (t = \tau \land e > 0)\rightarrow\\ \langle x' = f(x), t' = 1\&Q \land t < \tau \land e \leq 0\rangle e = 0\end{array}$$

While Lemma 5.9's purpose in this article is solely to prove Theorem 5.7, they also convey helpful properties of ODEs that are useful for other purposes. The following provides some intuition for these axioms.

- Axiom Rev says that if a property P is true, then after flowing along some ODE one can always flow back to a state where P is true. A sort of "there and back" quantification that says the current state can always be reached by reversing the ODE flow. This axiom (and its proof) has already been implemented in KeYmaera X's tactics library, but we reproduce a proof here for completeness.
- Axiom Stuck expresses that the ODE $t' = 1$ is strictly monotone, and therefore does not have any fixed points. Thus, if the current state has $t = t_0$ and the domain constraint includes $t \leq t_0$, then the overall dynamical system is stuck and necessarily cannot evolve, resulting in the RHS of the axiom.
- Axiom Idem expresses an "idempotence" property of diamond modalities. If the current state can flow along some ODE to a target region, then every state along this flow can also flow to the target region. One can also view this as a statement on the uniqueness of flows [45].
- Axiom Uniq' is a more fine-grained version of dL's uniqueness axiom [45] that deals with two potentially distinct target regions. While the implication looks complicated, it just says that if the flow along the same ODE can reach two regions P_1, P_2 under the domain constraints Q_1, Q_2 respectively, then by uniqueness of flows one flow will be the prefix of the other.
- Axiom IVT internalizes the classical intermediate value theorem within dL, saying if the term e is initially non-positive and becomes positive along some flow, then it necessarily reaches $e = 0$ along the way and will do so while remaining in $e \leq 0$.

Proofs of Lemma 5.9 and Theorem 5.7 are provided in Appendix B.

The main use of Theorem 5.7 in this article is to establish completeness results for compact IVPs. However, as the axioms/proof rules in Theorem 5.7 are fully symbolic, they also enable deductive reasoning for general symbolic IVPs which is of independent interest, one such example is given below.

Example 5.10 (Symbolic Maximal Interval of Existence). Consider the simple uni-variate ODE $x' = x^2 + 1$ with symbolic initial condition $x(0) = x_0$. Its exact solution is

$$x(t) \equiv \tan(\arctan(x_0) + t)$$

Thus, the (right) maximal interval of existence of the corresponding solution is $[0, \frac{\pi}{2} - \arctan(x_0))$, note that x_0 is a *symbolic variable* rather than a fixed constant. This example shows how dL can essentially prove this symbolic interval of existence. Since $\arctan(x_0)$ is not expressible in dL, we approximate $\arctan(x)$ (and $\frac{\pi}{2} - \arctan(x)$) informally via its series expansion at infinity

$$\arctan(x) \sim \frac{\pi}{2} - \frac{1}{x} + \frac{1}{3x^3} + o\left(\frac{1}{x^4}\right)$$
$$\frac{\pi}{2} - \arctan(x) \sim \frac{1}{x} - \frac{1}{3x^3} + o\left(\frac{1}{x^4}\right)$$

With Theorem 5.7, it can be shown that for all $\varepsilon \in \mathbb{Q}^+$ however small, the following formula (parametrized by ε) is derivable in dL[9] (the same technique in this example also works for higher-order bounds)

$$x = x_0 \land t = 0 \land x_0 > 0 \to \langle x' = x^2 + 1, t' = 1\rangle t \geq (1 - \varepsilon)\left(\frac{1}{x_0} - \frac{1}{3x_0^3}\right)$$

In other words, for every $\varepsilon > 0$, one can *symbolically prove* that the (right) maximal interval of existence is at least $(1 - \varepsilon)(\frac{1}{x} - \frac{1}{3x^3})$. Importantly, such a bound is interesting because x_0 is symbolic and can be unbounded, hence the provability of this formula does not directly follow from the completeness results for compact IVPs. Indeed, for x_0 sufficiently small the bound tends to $-\infty$, which is trivially satisfied. The assumption of $x_0 > 0$ is added for clarity in derivations only, and an identical formula can also be derived for $x_0 < 0$.

A complete proof of this example is provided in Appendix B. The main idea is to derive a numerical approximation purely symbolically using StepEx. For a symbolic initial value x_0, bounding the maximum derivative in $B(x_0, x_0)$ gives some positive duration of existence. Running this procedure iteratively for n steps gives rise to n such values, adding these up with axiom StepExt gives a lower-bound on the duration of existence while remaining in the region $B(x_0, nx_0)$. By picking $n \in \mathbb{N}$ large enough (independent of x_0), this procedure proves the desired lower-bound.

With Theorem 5.7, various completeness properties of dL for compact IVPs can now be proven. The following theorem states that all true safety properties of compact IVPs can be proven provided that the safety set is open.

Theorem 5.11 (Completeness for Bounded Safety). *Let $(f(x), C(x), [t_0, T])$ be a compact IVP and $O(x)$ a $FOL_{\mathbb{R}}$ formula characterizing a bounded open set. Then* dL *is complete for formulas of the form*

$$C(x) \land t = t_0 \to [x' = f(x), t' = 1 \& t \leq T]O(x)$$

i.e., the following equivalence holds

$$\models C(x) \land t = t_0 \to [x' = f(x), t' = 1 \& t \leq T]O(x) \iff$$
$$\vdash C(x) \land t = t_0 \to [x' = f(x), t' = 1 \& t \leq T]O(x)$$

[9] Since $x_0 \neq 0$ is enforced, the value $\frac{1}{x_0}$ is defined uniquely as some c such that $cx_0 = 1$.

Proof. The $\Longleftarrow$ implication is soundness and follows by soundness of dL's axiomatization [38, 45, 52], so it remains to prove the $\Longrightarrow$ implication. To this end, let us assume the validity of such a formula. Since $O(x)$ is a bounded set, this implies that the flow $\varphi : [\![C]\!] \times [t_0, T] \to \mathbb{R}^n$ of the compact IVP is well-defined as it does not exhibit finite time blow-up. By validity of the formula, we have $\varphi([\![C]\!], [t_0, T]) \subseteq O(x)$. Since $O(x)$ is open and $\varphi([\![C]\!], [t_0, T])$ is compact, there necessarily exists some $\varepsilon \in \mathbb{Q}^+$ such that $B(\varphi([\![C]\!], [t_0, T]), \varepsilon) \subseteq [\![O]\!]$. For each $n \in \mathbb{N}$, denote by θ_n the (vectorial) polynomial of error at most 2^{-n} as computed by Theorem 5.5. Now note that for all sufficiently large $n \in \mathbb{N}$, the following formulas will be valid

$$C(x) \land x = x_0 \land t = t_0 \to [x' = f(x), t' = 1 \& t \leq T] \, \|x - \theta_n(x_0, t)\|^2 \leq 2^{-2n}$$
$$\forall x_0 \forall t (C(x_0) \land t_0 \leq t \land t \leq T \to B[\theta_n(x_0, t), 2^{-n}] \subseteq [\![O]\!])$$

Furthermore, they are both provable via Theorem 5.5 and $\mathbb{R}$ respectively. Thus, doing a bounded search on $n \in \mathbb{N}$ will find one where the two formulas above are provable. From this applications of V,dW on the first formula proves

$$C(x) \land x{=}x_0 \land t{=}t_0 \to [x'{=}f(x), t'{=}1 \& t \leq T] \left(t_0 \leq t \land t \leq T \land C(x_0) \land \|x - \theta_n(x_0, t)\|^2 \leq 2^{-2n}\right)$$

Another application of V (Lemma B.1) brings the second formula in, proving

$$C(x) \land x{=}x_0 \land t{=}t_0 \to [x'{=}f(x), t'{=}1 \& t \leq T] \left(B[\theta_n(x_0, t), 2^{-n}] \subseteq [\![O]\!] \land \|x - \theta_n(x_0, t)\|^2 \leq 2^{-2n}\right)$$

The desired formula of $C(x) \land t = t_0 \to [x' = f(x), t' = 1 \& t \leq T] O(x)$ then follows by applying K and $\mathbb{R}$, completing the proof. □

Beyond safety properties, the following theorem establishes that dL is also complete for durations of existence. If the flow of a compact IVP exists on the time interval $[0, T]$, then it *provably* exists.

Theorem 5.12 (Completeness for Bounded Existence). *Let $(f(x), C(x), [t_0, T])$ be a compact IVP.* dL *is complete for formulas of the form*

$$C(x) \land t = t_0 \to \langle x' = f(x), t' = 1 \rangle t \geq T$$

Where $T \in \mathbb{Q}^+$ is a rational constant. i.e., the following equivalence holds

$$\models C(x) \land t = t_0 \to \langle x' = f(x), t' = 1 \rangle t \geq T \iff$$
$$\vdash C(x) \land t = t_0 \to \langle x' = f(x), t' = 1 \rangle t \geq T$$

Proof. Again $\Longleftarrow$ follows from dL's soundness [41, 45, 52], so it suffices to prove $\Longrightarrow$. Assuming that such a formula is valid, the flow $\varphi : [\![C]\!] \times [t_0, T] \to \mathbb{R}^n$ of the compact IVP is necessarily well-defined and therefore does not exhibit finite time blow-up on the time interval $[t_0, T]$. Thus, for all sufficiently large $R \in \mathbb{Q}^+$, the following formula will be valid

$$C(x) \land t = t_0 \to [x' = f(x), t' = 1 \& t \leq T] \, \|x\|^2 < R^2$$

By Theorem 5.11, this will furthermore be provable in dL because $\|x\|^2 < R^2$ is open. Thus, we may do a search for $R \in \mathbb{Q}^+$ until we find a value for which the formula above is provable. Once such a value is found, the desired formula can be proven via the following derivation

$$\dfrac{\dfrac{*}{\vdash C(x) \land t = t_0 \to [x' = f(x), t' = 1 \& t \leq T] \, \|x\|^2 < R^2}}{\vdash C(x) \land t = t_0 \to \langle x' = f(x), t' = 1 \rangle t \geq T} \ \text{StepDual}_{\to}\text{,dRW}\langle\cdot\rangle$$

where the premise is proven by application of Lemma 5.3. This completes the proof. □

Theorem 5.11 and Theorem 5.12 do *not* require the flow of the compact IVP to be well-defined a priori, as dL is capable of proving this from the validity of the formulas in question.

There is a natural dual part to Theorem 5.11, involving liveness formulas of the form

$$\vdash C(x) \land t = t_0 \to \langle x' = f(x), t' = 1 \& t \le T \rangle O(x)$$

dL is indeed also complete for formulas of this form, and the requirements on $O(x)$ can even be slightly relaxed in comparison with the earlier theorems to just characterizing an open set that is not necessarily bounded.

Theorem 5.13 (Completeness for liveness). *Let $(f(x), C(x), [t_0, T])$ be a compact IVP with well-defined flow $\varphi : [\![C]\!] \times [t_0, T] \to \mathbb{R}^n$ and $O(x)$ a $FOL_{\mathbb{R}}$ formula characterizing an open set. Then* dL *is complete for formulas of the form*

$$C(x) \land t = t_0 \to \langle x' = f(x), t' = 1 \& t \le T \rangle O(x)$$

i.e., the following equivalence holds

$$\models C(x) \land t = t_0 \to \langle x' = f(x), t' = 1 \& t \le T \rangle O(x) \iff$$
$$\vdash C(x) \land t = t_0 \to \langle x' = f(x), t' = 1 \& t \le T \rangle O(x)$$

Proof. As $\Longleftarrow$ is soundness, we only handle $\Longrightarrow$, so suppose that the formula is valid. Similar to the proof of Theorem 5.11, denote by θ_n the (vectorial) polynomial of error at most 2^{-n} as computed by Theorem 5.5 for each $n \in \mathbb{N}$. Now (computably) search for some $n \in \mathbb{N}$ such that the following formulas are valid (note that the first formula is always valid by construction of θ_n)

$$C(x) \land x = x_0 \land t = t_0 \to [x' = f(x), t' = 1 \& t \le T] \, \|\theta_n(x_0, t) - x\|^2 \le 2^{-2n}$$
$$\forall x_0 \in [\![C]\!] \, \exists t \, (t_0 \le t \land t \le T \land B[\theta_n(x_0, t), 2^{-n}] \subseteq [\![O]\!])$$

For this to be a well-defined procedure, we prove that such an $n \in \mathbb{N}$ necessarily exists. Suppose for the sake of contradiction that this is false, then for all $n \in \mathbb{N}$, the following hold:

(1) $\|\theta_n - \varphi\|_{C^0([\![C]\!] \times [t_0, T])} \le 2^{-n}$
(2) There exists some $z_n \in [\![C]\!]$ such that for all $t \in [t_0, T]$, $B[\theta_n(z_n, t), 2^{-n}] \nsubseteq [\![O]\!]$.

Since $[\![C]\!]$ is compact, we may assume without loss of generality (by re-indexing if necessary), that the sequence $z_n \to z \in [\![C]\!]$ converges to some z. To achieve a contradiction, it suffices to show that $\varphi(z, t) \notin [\![O]\!]$ for all $t \in [t_0, T]$. Let $t \in [t_0, T]$ be arbitrary and denote $d : \mathbb{R}^n \to \mathbb{R}$ as the distance function associated to the closed set $[\![O]\!]^C$. For all $n \in \mathbb{N}$, we have

$$\begin{aligned}
d(\varphi(z, t)) &\le d(\theta_n(z_n, t)) + \|\theta_n(z_n, t) - \varphi(z, t)\| \\
&\le 2^{-n} + \|\theta_n(z_n, t) - \varphi(z, t)\| \qquad \text{(by choice of } z_n \text{ in (2))} \\
&\le 2^{-n} + \|\theta_n(z, t) - \varphi(z, t)\| + \|\theta_n(z_n, t) - \theta_n(z, t)\| \\
&\le 2^{-n} + \|\theta_n - \varphi\|_{C^0([\![C]\!] \times [t_0, T])} + \|\theta_n(z_n, t) - \varphi(z_n, t)\| + \|\varphi(z_n, t) - \theta_n(z, t)\| \\
&\le 2^{-n+1} + \|\theta_n - \varphi\|_{C^0([\![C]\!] \times [t_0, T])} + \|\varphi(z_n, t) - \varphi(z, t)\| + \|\varphi(z, t) - \theta_n(z, t)\| \\
&\le 2^{-n+2} + \|\varphi(z_n, t) - \varphi(z, t)\| \xrightarrow{n \to \infty} 0
\end{aligned}$$

where the final convergence uses the fact that φ is continuous. Since the argument above holds for all $t \in [t_0, T]$, this shows $\varphi(z, [t_0, T]) \cap [\![O]\!] = \emptyset$, a contradiction. Thus, there necessarily exists some n such that both formulas are valid and therefore provable via Theorem 5.5 and $\mathbb{R}$. To continue, first note that the following is provable

$$C(x) \land x = x_0 \land t = t_0 \to \langle t' = 1 \& t \le T \rangle B[\theta_n(x_0, t), 2^{-n}] \subseteq [\![O]\!]$$

with derivation

$$\rightarrow\mathrm{R}\;\dfrac{\langle\&\rangle,\exists\mathrm{R}\;\dfrac{K\langle\cdot\rangle\;\dfrac{\langle{}'\rangle,\mathbb{R}\;\dfrac{\mathbb{R}\;\dfrac{*}{C(x), x = x_0 \vdash \exists t\,(t_0 \le t \land t \le T \land B[\theta_n(x_0,t), 2^{-n}] \subseteq \llbracket O \rrbracket)}}{C(x), x = x_0, t = t_0 \vdash \langle t' = 1\rangle\,(B[\theta_n(x_0,t), 2^{-n}] \subseteq \llbracket O \rrbracket \land t \le T)}}{C(x), x = x_0, t = t_0 \vdash \langle t' = 1\rangle\,(B[\theta_n(x_0,t), 2^{-n}] \subseteq \llbracket O \rrbracket \land [t' = -1](t \ge t_0 \rightarrow t \le T))}}{C(x), x = x_0, t = t_0 \vdash \langle t' = 1 \& t \le T\rangle B[\theta_n(x_0,t), 2^{-n}] \subseteq \llbracket O \rrbracket}}{\vdash C(x) \land x = x_0 \land t = t_0 \rightarrow \langle t' = 1 \& t \le T\rangle B[\theta_n(x_0,t), 2^{-n}] \subseteq \llbracket O \rrbracket}$$

where the final application of $\mathbb{R}$ is sound by the construction of n, and axiom $K\langle\cdot\rangle$ was applied assuming $t \le T \rightarrow [t' = -1]t \le T$, which is a valid invariant and can be proven by dInv. Next, the following formula can be derived with a direct application of axiom BDG$\langle\cdot\rangle$

$$C(x) \land x = x_0 \land t = t_0 \rightarrow \langle x' = f(x), t' = 1 \& t \le T\rangle B[\theta_n(x_0,t), 2^{-n}] \subseteq \llbracket O \rrbracket$$

which uses the (provable) formulas

$$C(x) \land x = x_0 \land t = t_0 \rightarrow [x' = f(x), t' = 1 \& t \le T]\, \|\theta_n(x_0,t) - x\|^2 \le 2^{-2n}$$
$$C(x) \land x = x_0 \land t = t_0 \rightarrow \langle t' = 1 \& t \le T\rangle B[\theta_n(x_0,t), 2^{-n}] \subseteq \llbracket O \rrbracket$$

Finally, applying axioms DR$\langle\cdot\rangle$,dW$\langle\cdot\rangle$ with the (provable) formulas

$$C(x) \land x = x_0 \land t = t_0 \rightarrow [x' = f(x), t' = 1 \& t \le T]\, \|\theta_n(x_0,t) - x\|^2 \le 2^{-2n}$$
$$C(x) \land x = x_0 \land t = t_0 \rightarrow \langle x' = f(x), t' = 1 \& t \le T\rangle B[\theta_n(x_0,t), 2^{-n}] \subseteq \llbracket O \rrbracket$$

proves

$$C(x) \land x{=}x_0 \land t{=}t_0 \rightarrow \langle x'{=}f(x), t'{=}1 \& t \le T\rangle (B[\theta_n(x_0,t), 2^{-n}] \subseteq \llbracket O \rrbracket \land \|\theta_n(x_0,t) - x\|^2 \le 2^{-2n})$$

another application of $K\langle\cdot\rangle$ gives

$$C(x) \land t = t_0 \rightarrow \langle x' = f(x), t' = 1 \& t \le T\rangle O(x)$$

completing the proof of completeness for open properties. □

6 Conclusion

By unifying both deductive and numerical techniques, this article establishes several completeness properties of compact IVPs. On a theoretical level, this proves complete reasoning principles for compact IVPs from purely qualitative properties. On a practical level, these results show that it is possible both to enjoy the capabilities of numerical methods, whilst retaining the rigorous level of trust provided by deductive, symbolic proofs. Alternatively, one could view such completeness results as a strengthening in the uniformity of such numerical algorithms. Standard numerical algorithms take in a single input and compute a corresponding output. As such, a different certifying proof of the output is needed for each individual input. This article improves on the level of uniformity for compact IVPs and establishes that there exists a single, symbolic proof in dL which proves the desired properties of the given compact IVP for *all initial conditions* from the compact domain.

To achieve these completeness results, the article crucially establishes that rigorous error bounds can be proved in dL by reducing them down to differential invariance questions, providing a modular, rigorous way of verifying error bounds for numerical approximations. Utilizing this result, this article then proves that dL is complete for (open and bounded) safety and liveness properties, as well as convergence for compact IVPs. This proof-theoretic result shows that not only is dL expressive enough, its axiomatization is also powerful enough to prove all such true properties of compact IVPs. The article also presented derivations of several classical theorems in dL along the way to establishing completeness, which are of independent interest, notably including the Weierstrass approximation theorem, intermediate value theorem and the correspondence between global existence of flows and absence of finite time blow-up.

For future work, it would be interesting to establish specific classes of LDAs that are general enough to preserve the completeness results while having a more tractable complexity in proving their error bounds in the sense of Theorem 5.1.

References

[1] Shaull Almagor, Edon Kelmendi, Joël Ouaknine, and James Worrell. 2020. Invariants for continuous linear dynamical systems. In *47th International Colloquium on Automata, Languages, and Programming, ICALP 2020, July 8-11, 2020, Saarbrücken, Germany (Virtual Conference) (LIPIcs, Vol. 168)*, Artur Czumaj, Anuj Dawar, and Emanuela Merelli (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 107:1–107:15. DOI: 10.4230/LIPICS.ICALP.2020.107

[2] Matthias Althoff. 2015. An introduction to CORA 2015. In *1st and 2nd International Workshop on Applied veRification for Continuous and Hybrid Systems, ARCH@CPSWeek 2014, Berlin, Germany, April 14, 2014 / ARCH@CPSWeek 2015, Seattle, WA, USA, April 13, 2015 (EPiC Series in Computing, Vol. 34)*, Goran Frehse and Matthias Althoff (Eds.). EasyChair, 120–151. DOI: 10.29007/ZBKV

[3] Rajeev Alur. 2015. *Principles of Cyber-Physical Systems.* The MIT Press.

[4] Erin M. Aylward, Pablo A. Parrilo, and Jean-Jacques E. Slotine. 2008. Stability and robustness analysis of nonlinear systems via contraction metrics and SOS programming. *Automatica* 44, 8 (Aug. 2008), 2163–2170. DOI: 10.1016/j.automatica.2007.12.012

[5] Paul C. Bell, Jean-Charles Delvenne, Raphaël M. Jungers, and Vincent D. Blondel. 2010. The continuous skolem-pisot problem. *Theor. Comput. Sci.* 411, 40-42 (2010), 3625–3634. DOI: 10.1016/J.TCS.2010.06.005

[6] Jacek Bochnak, Michel Coste, and Marie-Francoise Roy. 2013. *Real Algebraic Geometry.* Springer Science & Business Media.

[7] Sergiy Bogomolov, Marcelo Forets, Goran Frehse, Kostiantyn Potomkin, and Christian Schilling. 2019. JuliaReach: A toolbox for set-based reachability. In *Proceedings of the 22nd ACM International Conference on Hybrid Systems: Computation and Control, HSCC 2019, Montreal, QC, Canada, April 16-18, 2019*, Necmiye Ozay and Pavithra Prabhakar (Eds.). ACM, 39–44. DOI: 10.1145/3302504.3311804

[8] Brandon Bohrer, Vincent Rahli, Ivana Vukotic, Marcus Völp, and André Platzer. 2017. Formally verified differential dynamic logic. In *Certified Programs and Proofs—6th ACM SIGPLAN Conference, CPP 2017, Paris, France, January 16-17, 2017*, Yves Bertot and Viktor Vafeiadis (Eds.). ACM, 208–221. DOI: 10.1145/3018610.3018616

[9] Sylvie Boldo and Jean-Christophe Filliâtre. 2007. Formal verification of floating-point programs. In *18th IEEE Symposium on Computer Arithmetic (ARITH-18 2007), 25-27 June 2007, Montpellier, France.* IEEE Computer Society, 187–194. DOI: 10.1109/ARITH.2007.20

[10] Olivier Bournez and Riccardo Gozzi. 2024. Solving discontinuous initial value problems with unique solutions is equivalent to computing over the transfinite. In *41st International Symposium on Theoretical Aspects of Computer Science, STACS 2024, March 12-14, 2024, Clermont-Ferrand, France (LIPIcs, Vol. 289)*, Olaf Beyersdorff, Mamadou Moustapha Kanté, Orna Kupferman, and Daniel Lokshtanov (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 20:1–20:19. DOI: 10.4230/LIPICS.STACS.2024.20

[11] Olivier Bournez, Daniel Silva Graça, and Amaury Pouly. 2012. On the complexity of solving initial value problems. In *International Symposium on Symbolic and Algebraic Computation, ISSAC'12, Grenoble, France - July 22 - 25, 2012*, Joris van der Hoeven and Mark van Hoeij (Eds.). ACM, 115–121. DOI: 10.1145/2442829.2442849

[12] Olivier Bournez, Daniel Silva Graça, and Amaury Pouly. 2015. Rigorous numerical computation of polynomial differential equations over unbounded domains. In *Mathematical Aspects of Computer and Information Sciences - 6th International Conference, MACIS 2015, Berlin, Germany, November 11-13, 2015, Revised Selected Papers (Lecture Notes in Computer Science, Vol. 9582)*, Ilias S. Kotsireas, Siegfried M. Rump, and Chee K. Yap (Eds.). Springer, 469–473. DOI: 10.1007/978-3-319-32859-1_40

[13] Olivier Bournez, Daniel Silva Graça, and Amaury Pouly. 2016. Computing with polynomial ordinary differential equations. *J. Complex.* 36 (2016), 106–140. DOI: 10.1016/J.JCO.2016.05.002

[14] Olivier Bournez and Amaury Pouly. 2017. A universal ordinary differential equation. In *44th International Colloquium on Automata, Languages, and Programming, ICALP 2017, July 10-14, 2017, Warsaw, Poland (LIPIcs, Vol. 80)*, Ioannis Chatzigiannakis, Piotr Indyk, Fabian Kuhn, and Anca Muscholl (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 116:1–116:14. DOI: 10.4230/LIPICS.ICALP.2017.116

[15] Davide Bresolin, Pieter Collins, Luca Geretti, Roberto Segala, Tiziano Villa, and Sanja Zivanovic Gonzalez. 2020. A computable and compositional semantics for hybrid automata. In *HSCC '20: 23rd ACM International Conference on*

Hybrid Systems: Computation and Control, Sydney, New South Wales, Australia, April 21-24, 2020, Aaron D. Ames, Sanjit A. Seshia, and Jyotirmoy Deshmukh (Eds.). ACM, 18:1–18:11. DOI: 10.1145/3365365.3382202

[16] Xin Chen, Erika Ábrahám, and Sriram Sankaranarayanan. 2013. Flow*: An analyzer for non-linear hybrid systems. In *Computer Aided Verification - 25th International Conference, CAV 2013, Saint Petersburg, Russia, July 13-19, 2013. Proceedings (LNCS, Vol. 8044)*, Natasha Sharygina and Helmut Veith (Eds.). Springer, 258–263. DOI: 10.1007/978-3-642-39799-8_18

[17] Ventsislav Chonev, Joël Ouaknine, and James Worrell. 2016. On recurrent reachability for continuous linear dynamical systems. In *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science, LICS '16, New York, NY, USA, July 5-8, 2016*, Martin Grohe, Eric Koskinen, and Natarajan Shankar (Eds.). ACM, 515–524. DOI: 10.1145/2933575.2934548

[18] Ventsislav Chonev, Joël Ouaknine, and James Worrell. 2016. On the skolem problem for continuous linear dynamical systems. In *43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 11-15, 2016, Rome, Italy (LIPIcs, Vol. 55)*, Ioannis Chatzigiannakis, Michael Mitzenmacher, Yuval Rabani, and Davide Sangiorgi (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 100:1–100:13. DOI: 10.4230/LIPICS.ICALP.2016.100

[19] Pieter Collins, Davide Bresolin, Luca Geretti, and Tiziano Villa. 2012. Computing the evolution of hybrid systems using rigorous function calculus. In *4th IFAC Conference on Analysis and Design of Hybrid Systems, ADHS 2012, Eindhoven, The Netherlands, June 6-8, 2012 (IFAC Proceedings Volumes, Vol. 45)*, Maurice Heemels and Bart De Schutter (Eds.). Elsevier, 284–290. DOI: 10.3182/20120606-3-NL-3011.00063

[20] Julian D'Costa, Toghrul Karimov, Rupak Majumdar, Joël Ouaknine, Mahmoud Salamati, and James Worrell. 2022. The pseudo-reachability problem for diagonalisable linear dynamical systems. In *47th International Symposium on Mathematical Foundations of Computer Science, MFCS 2022, August 22-26, 2022, Vienna, Austria (LIPIcs, Vol. 241)*, Stefan Szeider, Robert Ganian, and Alexandra Silva (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 40:1–40:13. DOI: 10.4230/LIPICS.MFCS.2022.40

[21] Goran Frehse, Colas Le Guernic, Alexandre Donzé, Scott Cotton, Rajarshi Ray, Olivier Lebeltel, Rodolfo Ripado, Antoine Girard, Thao Dang, and Oded Maler. 2011. SpaceEx: Scalable verification of hybrid systems. In *Computer Aided Verification - 23rd International Conference, CAV 2011, Snowbird, UT, USA, July 14-20, 2011. Proceedings (LNCS, Vol. 6806)*, Ganesh Gopalakrishnan and Shaz Qadeer (Eds.). Springer, 379–395. DOI: 10.1007/978-3-642-22110-1_30

[22] Nathan Fulton, Stefan Mitsch, Jan-David Quesel, Marcus Völp, and André Platzer. 2015. KeYmaera X: An axiomatic tactical theorem prover for hybrid systems. In *Automated Deduction - CADE-25 - 25th International Conference on Automated Deduction, Berlin, Germany, August 1-7, 2015, Proceedings (LNCS, Vol. 9195)*, Amy P. Felty and Aart Middeldorp (Eds.). Springer, 527–538. DOI: 10.1007/978-3-319-21401-6_36

[23] Nathan Fulton, Stefan Mitsch, Jan-David Quesel, Marcus Völp, and André Platzer. 2015. *KeYmaera X: An Axiomatic Tactical Theorem Prover for Hybrid Systems.* LNCS, Vol. 9195. Springer International Publishing, Cham, 527–538. DOI: 10.1007/978-3-319-21401-6_36

[24] C. William Gear. 1971. *Numerical Initial Value Problems in Ordinary Differential Equations.* Englewood Cliffs, NJ: Prentice-Hall.

[25] Nicolò Giorgetti, George J. Pappas, and Alberto Bemporad. 2005. Bounded model checking of hybrid dynamical systems. In *44th IEEE IEEE Conference on Decision and Control and 8th European Control Conference Control, CDC/ECC 2005, Seville, Spain, 12-15 December, 2005.* IEEE, 672–677. DOI: 10.1109/CDC.2005.1582233

[26] Daniel Silva Graça and Ning Zhong. 2018. Computability of ordinary differential equations. In *Sailing Routes in the World of Computation—14th Conference on Computability in Europe, CiE 2018, Kiel, Germany, July 30 - August 3, 2018, Proceedings (LNCS, Vol. 10936)*, Florin Manea, Russell G. Miller, and Dirk Nowotka (Eds.). Springer, 204–213. DOI: 10.1007/978-3-319-94418-0_21

[27] D.S. Graça, N. Zhong, and J. Buescu. 2009. Computability, noncomputability and undecidability of maximal intervals of IVPs. *Trans. Amer. Math. Soc.* 361, 6 (Jan 2009), 2913–2927. DOI: 10.1090/S0002-9947-09-04929-0

[28] T. H. Grönwall. 1919. Note on the derivatives with respect to a parameter of the solutions of a system of differential equations. *Annals of Mathematics* 20, 4 (1919), 292–296. DOI: 10.2307/1967124

[29] Emmanuel Hainry. 2008. Reachability in linear dynamical systems. In *Logic and Theory of Algorithms, 4th Conference on Computability in Europe, CiE 2008, Athens, Greece, June 15-20, 2008, Proceedings (Lecture Notes in Computer Science, Vol. 5028)*, Arnold Beckmann, Costas Dimitracopoulos, and Benedikt Löwe (Eds.). Springer, 241–250. DOI: 10.1007/978-3-540-69407-6_28

[30] Philip Hartman. 2002. *Ordinary Differential Equations.* Society for Industrial and Applied Mathematics. DOI: 10.1137/1.9780898719222

[31] Fabian Immler. 2018. A verified ODE solver and the lorenz attractor. *J. Autom. Reason.* 61, 1-4 (2018), 73–111. DOI: 10.1007/S10817-017-9448-Y

[32] Tomasz Kapela, Marian Mrozek, Daniel Wilczak, and Piotr Zgliczynski. 2021. CAPD: : DynSys: A flexible C++ toolbox for rigorous numerical analysis of dynamical systems. *Commun. Nonlinear Sci. Numer. Simul.* 101 (2021), 105578. DOI: 10.1016/J.CNSNS.2020.105578

[33] Katherine Kosaian, Yong Kiam Tan, and André Platzer. 2023. A first complete algorithm for real quantifier elimination in isabelle/HOL. In *Proceedings of the 12th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2023, Boston, MA, USA, January 16-17, 2023*, Robbert Krebbers, Dmitriy Traytel, Brigitte Pientka, and Steve Zdancewic (Eds.). ACM, 211–224. DOI: 10.1145/3573105.3575672

[34] Rainer Kress. 1998. *Numerical Analysis.* Graduate Texts in Mathematics, Vol. 181. Springer, New York, NY. DOI: 10.1007/978-1-4612-0599-9

[35] Jiang Liu, Naijun Zhan, and Hengjun Zhao. 2011. Computing semi-algebraic invariants for polynomial dynamical systems. In *Proceedings of the 11th International Conference on Embedded Software, EMSOFT 2011, part of the Seventh Embedded Systems Week, ESWeek 2011, Taipei, Taiwan, October 9-14, 2011*, Samarjit Chakraborty, Ahmed Jerraya, Sanjoy K. Baruah, and Sebastian Fischmeister (Eds.). ACM, 97–106. DOI: 10.1145/2038642.2038659

[36] Angus Macintyre and A. J. Wilkie. 1996. On the decidability of the real exponential field. In *Kreiseliana.* A K Peters, Wellesley, MA, 441–467.

[37] Sewon Park and Holger Thies. 2024. A coq formalization of taylor models and power series for solving ordinary differential equations. In *15th International Conference on Interactive Theorem Proving, ITP 2024, September 9-14, 2024, Tbilisi, Georgia (LIPIcs, Vol. 309)*, Yves Bertot, Temur Kutsia, and Michael Norrish (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 30:1–30:19. DOI: 10.4230/LIPICS.ITP.2024.30

[38] André Platzer. 2008. Differential dynamic logic for hybrid systems. *J. Autom. Reason.* 41, 2 (2008), 143–189. DOI: 10.1007/S10817-008-9103-8

[39] André Platzer. 2012. The complete proof theory of hybrid systems. In *Proceedings of the 27th Annual IEEE Symposium on Logic in Computer Science, LICS 2012, Dubrovnik, Croatia, June 25-28, 2012.* IEEE Computer Society, 541–550. DOI: 10.1109/LICS.2012.64

[40] André Platzer. 2012. Logics of dynamical systems. In *Proceedings of the 27th Annual IEEE Symposium on Logic in Computer Science, LICS 2012, Dubrovnik, Croatia, June 25-28, 2012.* IEEE Computer Society, 13–24. DOI: 10.1109/LICS.2012.13

[41] André Platzer. 2017. A complete uniform substitution calculus for differential dynamic logic. *J. Autom. Reason.* 59, 2 (2017), 219–265. DOI: 10.1007/S10817-016-9385-1

[42] André Platzer. 2018. *Logical Foundations of Cyber-Physical Systems.* Springer. DOI: 10.1007/978-3-319-63588-0

[43] André Platzer and Yong Kiam Tan. 2017. *How to Prove "All" Differential Equation Properties.* Technical Report CMU-CS-17-117. School of Computer Science, Carnegie Mellon University, Pittsburgh, PA. Extended version at arXiv:1802.01226.pdf.

[44] André Platzer and Yong Kiam Tan. 2018. Differential equation axiomatization: The impressive power of differential ghosts. In *LICS*, Anuj Dawar and Erich Grädel (Eds.). ACM, New York, 819–828. DOI: 10.1145/3209108.3209147

[45] André Platzer and Yong Kiam Tan. 2020. Differential equation invariance axiomatization. *J. ACM* 67, 1 (2020), 6:1–6:66. DOI: 10.1145/3380825

[46] Henri Poincaré. 1881. Mémoire sur les courbes définies par une équation différentielle. *J. Math. Pures Appl.* 7, 3 (1881), 375–422.

[47] Keijo Ruohonen. 1996. An effective cauchy-peano existence theorem for unique solutions. *Int. J. Found. Comput. Sci.* 7, 2 (1996), 151–160. DOI: 10.1142/S0129054196000129

[48] Xin Chen Rwth, Sriram Sankaranarayanan, and Erika Abraham. 2014. Under-approximate flowpipes for non-linear continuous systems. In *2014 Formal Methods in Computer-Aided Design (FMCAD).* IEEE, Lausanne, Switzerland, 59–66. DOI: 10.1109/FMCAD.2014.6987596

[49] Robert I. Soare. 2016. *Turing Computability: Theory and Applications.* Springer. DOI: 10.1007/978-3-642-31933-4

[50] Andrew Sogokon and Paul B. Jackson. 2015. Direct formal verification of liveness properties in continuous and hybrid dynamical systems. In *FM 2015: Formal Methods - 20th International Symposium, Oslo, Norway, June 24-26, 2015, Proceedings (LNCS, Vol. 9109)*, Nikolaj S. Bjørner and Frank S. de Boer (Eds.). Springer, 514–531. DOI: 10.1007/978-3-319-19249-9_32

[51] Andrew Sogokon, Stefan Mitsch, Yong Kiam Tan, Katherine Cordwell, and André Platzer. 2021. Pegasus: Sound continuous invariant generation. *Formal Methods Syst. Des.* 58, 1-2 (2021), 5–41. DOI: 10.1007/S10703-020-00355-Z

[52] Yong Kiam Tan and André Platzer. 2021. An axiomatic approach to existence and liveness for differential equations. *Formal Aspects Comput.* 33, 4-5 (2021), 461–518. DOI: 10.1007/S00165-020-00525-0

[53] Alfred Tarski. 1948. *A Decision Method for Elementary Algebra and Geometry.* The Rand Corporation, Santa Monica, Calif.

[54] Wolfgang Walter. 1998. *Ordinary Differential Equations.* Graduate Texts in Mathematics, Vol. 182. Springer New York. DOI: 10.1007/978-1-4612-0601-9

[55] Klaus Weihrauch. 2000. *Computable Analysis: An Introduction.* Springer. DOI: 10.1007/978-3-642-56999-9

[56] Chee K Yap. 2004. On guaranteed accuracy computation. In *Geometric Computation.* World Scientific, 322–373. DOI: 10.1142/9789812794833_0012

Appendix

A dL Axiomatization

This section provides a complete record of dL's axiomatization that is needed for the article.

Theorem A.1 ([40, 45, 52]). *The following are sound axioms of* dL. *In axioms Cont, Dadj, BDG, the variables y is fresh. In axiom BDG, $Q(x)$ is required to be a formula of real arithmetic.*

$$\mathbb{R}\quad \frac{}{\Gamma \vdash \Delta} \qquad (\text{if } \textstyle\bigwedge_{P\in\Gamma} P \to \bigvee_{Q\in\Delta} Q \text{ is valid in } \mathrm{FOL}_{\mathbb{R}})$$

$$\langle\cdot\rangle\quad \langle\alpha\rangle P \leftrightarrow \neg[\alpha]\neg P$$

$$\langle'\rangle\quad \langle x' = f(x)\rangle p(x) \leftrightarrow \exists t{\ge}0\, \langle x := y(t)\rangle p(x) \qquad (y'(t) = f(y))$$

$$\mathrm{B}'\quad \langle x' = f(x)\,\&\,Q(x)\rangle \exists y P(x,y) \leftrightarrow \exists y\, \langle x' = f(x)\,\&\,Q(x)\rangle P(x,y) \qquad (y \notin x)$$

$$\mathrm{K}\quad [\alpha](\varphi\to\psi)\to([\alpha]\varphi\to[\alpha]\psi)$$

$$\mathrm{V}\quad \varphi\to[\alpha]\varphi \qquad (\text{no free variable of } \varphi \text{ is bound by } \alpha)$$

$$\mathrm{G}\quad \frac{\vdash \varphi}{\Gamma \vdash [\alpha]\varphi}$$

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

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

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

$$\mathrm{DGi}\quad [x' = f(x)\,\&\,Q(x)]P(x)\to\forall y[x' = f(x), y' = g(x,y)\,\&\,Q(x)]P(x)$$

$$[\&]\quad [x' = \theta\&\chi]\varphi \leftrightarrow \forall t_0{=}c_0 [x' = \theta]\,([x' = -\theta]\,(c_0 \ge t_0 \to \chi) \to \varphi)$$

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

$$\mathrm{Uniq}\quad \langle x' = f(x)\&Q_1 \wedge Q_2\rangle P \leftrightarrow (\langle x' = f(x)\&Q_1\rangle P) \wedge (\langle x' = f(x)\&Q_2\rangle P)$$

$$\mathrm{Cont}\quad x = y\to(\langle x' = f(x)\&e > 0\rangle x \ne y \leftrightarrow e > 0) \qquad (f(x) \ne 0)$$

$$\mathrm{Dadj}\quad \langle x' = f(x)\&Q(x)\rangle x = y \leftrightarrow \langle y' = -f(y)\&Q(y)\rangle y = x$$

$$\mathrm{RI}\quad [x' = f(x)]P \leftrightarrow \forall y[x' = f(x)\&P \vee x = y]\,(x = y \to P \wedge \langle x' = f(x)\&P \vee x = y\rangle x \ne y)$$

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

Remark A.2. In axioms [&] and Cont, it is assumed that the ODE $x' = f(x)$ includes a clock variable $c_0' = 1$. This assumption can be made without loss of generality since a clock variable can always be added using DG. The variable t_0 is also assumed to be fresh in [&].

The following derivable axioms will also be used.

Theorem A.3 ([40, 45, 52]). *The following axioms are derivable in* dL, *where e is a term. In axiom BDG⟨·⟩, $Q(x)$ is required to be a formula of real arithmetic.*

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

$$\text{dRW}\langle\cdot\rangle \quad \frac{R \vdash Q \qquad \Gamma \vdash \langle x' = f(x) \& R\rangle P}{\Gamma \vdash \langle x' = f(x) \& Q\rangle P}$$

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

$$K\langle\cdot\rangle \quad [\alpha]\,(\varphi \rightarrow \psi) \rightarrow (\langle\alpha\rangle\varphi \rightarrow \langle\alpha\rangle\psi)$$

$$\langle\rangle\vee \quad \langle\alpha\rangle\,(\varphi \vee \psi) \leftrightarrow \langle\alpha\rangle\varphi \vee \langle\alpha\rangle\psi$$

$$[]\wedge \quad [\alpha](\varphi \wedge \psi) \leftrightarrow [\alpha]\varphi \wedge [\alpha]\psi$$

$$\text{Enc} \quad \frac{\Gamma \vdash e \geq 0 \qquad \Gamma \vdash [x' = f(x) \& Q \wedge e \geq 0]e > 0}{\Gamma \vdash [x' = f(x) \& Q]e > 0}$$

Remark A.4. This article adopts “rich-test” dL which allows domain constraints Q to be general dL formulas with modalities rather than just first order formulas of arithmetic unless explicitly restricted otherwise. Thus one should be cautious when employing previous axiomatization [45, 52] and ensure that they are still sound. Indeed, while earlier works stated the soundness of such axioms under the assumption of “poor-test” dL, the proofs are more general and extend to “rich-test” dL.

This concludes the brief overview of dL’s proof calculus that will be needed for this article. The usual FOL proof rules are listed below for completeness [38].

$$\neg\text{L} \quad \frac{\Gamma \vdash P, \Delta}{\Gamma, \neg P \vdash \Delta}$$

$$\wedge\text{L} \quad \frac{\Gamma, P, Q \vdash \Delta}{\Gamma, P \wedge Q \vdash \Delta}$$

$$\vee\text{L} \quad \frac{\Gamma, P \vdash \Delta \qquad \Gamma, Q \vdash \Delta}{\Gamma, P \vee Q \vdash \Delta}$$

$$\neg\text{R} \quad \frac{\Gamma, P \vdash \Delta}{\Gamma \vdash \neg P, \Delta}$$

$$\wedge\text{R} \quad \frac{\Gamma \vdash P, \Delta \qquad \Gamma \vdash Q, \Delta}{\Gamma \vdash P \wedge Q, \Delta}$$

$$\text{cut} \quad \frac{\Gamma \vdash C, \Delta \qquad \Gamma, C \vdash \Delta}{\Gamma \vdash \Delta}$$

$$\vee\text{R} \quad \frac{\Gamma \vdash P, Q, \Delta}{\Gamma \vdash P \vee Q, \Delta}$$

$$\rightarrow\text{L} \quad \frac{\Gamma \vdash P, \Delta \qquad \Gamma, Q \vdash \Delta}{\Gamma, P \rightarrow Q \vdash \Delta}$$

$$\forall\text{L} \quad \frac{\Gamma, p(e) \vdash \Delta}{\Gamma, \forall x\, p(x) \vdash \Delta} \qquad \text{(arbitrary term } e\text{)}$$

$$\exists\text{L} \quad \frac{\Gamma, p(y) \vdash \Delta}{\Gamma, \exists x\, p(x) \vdash \Delta} \qquad (y \notin \Gamma,\Delta,\exists x\, p(x))$$

$$\rightarrow\text{R} \quad \frac{\Gamma, P \vdash Q, \Delta}{\Gamma \vdash P \rightarrow Q, \Delta}$$

$$\forall\text{R} \quad \frac{\Gamma \vdash p(y), \Delta}{\Gamma \vdash \forall x\, p(x), \Delta} \qquad (y \notin \Gamma,\Delta,\forall x\, p(x))$$

$$\exists\text{R} \quad \frac{\Gamma \vdash p(e), \Delta}{\Gamma \vdash \exists x\, p(x), \Delta} \qquad \text{(arbitrary term } e\text{)}$$

$$\text{id} \quad \frac{*}{\Gamma, P \vdash P, \Delta}$$

B Derived Axioms and Proof Rules

This section proves Lemma 5.9 and subsequently Theorem 5.7. The following lemma proves useful properties of constant assumptions and a diamond analog of axiom [&].

Lemma B.1 ([45, Appendix A.2]). *The following axioms/proof rules are derivable and thus sound, where $R(y)$ is a* dL *formula only depending on its free variables y which has no differential equation in $x' = f(x)$.*

dW⟨·⟩ $\langle x' = f(x)\&Q\rangle P \rightarrow \langle x' = f(x)\&Q\rangle\,(P \wedge Q)$

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

$$\text{V}\quad \frac{*}{\Gamma, \langle x' = f(x)\&Q\rangle(P \wedge R(y)) \vdash R(y)}$$

$$\text{V}\quad \frac{*}{R(y), \langle x' = f(x)\&Q\rangle P \vdash \langle x' = f(x)\&Q\rangle(P \wedge R(y))}$$

⟨&⟩ $\langle x' = \theta\&\chi\rangle\varphi \leftrightarrow \exists t_0{=}c_0\langle x' = \theta\rangle\,(\varphi \wedge [x' = -\theta]\,(c_0 \geq t_0 \rightarrow \chi))$

Proof. Axiom dW⟨·⟩ can be derived as follows

$$K\langle\cdot\rangle\,\dfrac{\text{K}\,\dfrac{\text{dW}\,\dfrac{*}{\vdash [x' = f(x)\&Q]Q}}{\vdash [x' = f(x)\&Q]\,(P \rightarrow P \wedge Q)}}{\vdash \langle x' = f(x)\&Q\rangle P \rightarrow \langle x' = f(x)\&Q\rangle\,(P \wedge Q)}$$

The last proof rule labeled as V can be derived using dW⟨·⟩

$$\text{DR}\langle\cdot\rangle\text{,V}\,\dfrac{\text{dW}\langle\cdot\rangle\,\dfrac{\text{dRW}\langle\cdot\rangle\,\dfrac{*}{\langle x' = f(x)\&Q \wedge R(y)\rangle(P \wedge R(y)) \vdash \langle x' = f(x)\&Q\rangle(P \wedge R(y))}}{\langle x' = f(x)\&Q \wedge R(y)\rangle P \vdash \langle x' = f(x)\&Q\rangle(P \wedge R(y))}}{R(y), \langle x' = f(x)\&Q\rangle P \vdash \langle x' = f(x)\&Q\rangle(P \wedge R(y))}$$

Axiom ⟨&⟩ can be derived directly from axioms [&],⟨·⟩, and the remaining proof-rules have been derived in earlier works [45, Appendix A.2]. □

Axiom dW⟨·⟩ asserts that domain constraints are always satisfied along the flow, the next three proof rules assert that the truth of constant properties remain unchanged along the ODE flows, all special cases of axiom V [45, Appendix A.2] and thus have the same name. Similar to earlier works [45], manipulations of constant properties in derivations will be abbreviated with V. Axiom ⟨&⟩ is the diamond analog of [&], similar to [&], $c_0' = 1$ is a clock variable in $x' = f(x)$ and t_0 is fresh.

Proof of Lemma 5.9. Rev: Suppose for the sake of contradiction that the claim was false, there would be some state along the flow of $x' = f(x)$ such that reversing the flow does not return to the original state where P is true. But this directly contradicts axiom Dadj, which says that it is always possible to reach the initial state by following the reverse flow.

$$\begin{prooftree}
\AxiomC{$*$}
\LeftLabel{$\langle\cdot\rangle$,$\neg$L,id}
\UnaryInfC{$P(x), \langle y' = -f(y)\&Q\rangle P(y), [y' = -f(y)\&Q]\neg P(y) \vdash \bot$}
\LeftLabel{V}
\UnaryInfC{$P(x), \langle y' = -f(y)\&Q\rangle x = y, [y' = -f(y)\&Q]\neg P(y) \vdash \bot$}
\LeftLabel{Dadj}
\UnaryInfC{$P(x), \langle x' = f(x)\&Q\rangle x = y, [y' = -f(y)\&Q]\neg P(y) \vdash \bot$}
\LeftLabel{V}
\UnaryInfC{$P(x), \langle x' = f(x)\&Q\rangle (x = y \land [y' = -f(y)\&Q]\neg P(y)) \vdash \bot$}
\AxiomC{$\textcircled{1}$}
\LeftLabel{cut,$K\langle\cdot\rangle$}
\BinaryInfC{$P(x), \langle x' = f(x)\&Q\rangle (x = y \land [x' = -f(x)\&Q]\neg P(x)) \vdash \bot$}
\LeftLabel{$\exists$L}
\UnaryInfC{$P(x), \exists y \langle x' = f(x)\&Q\rangle (x = y \land [x' = -f(x)\&Q]\neg P(x)) \vdash \bot$}
\LeftLabel{B$'$}
\UnaryInfC{$P(x), \langle x' = f(x)\&Q\rangle (\exists y (x = y) \land [x' = -f(x)\&Q]\neg P(x)) \vdash \bot$}
\LeftLabel{$K\langle\cdot\rangle$,G}
\UnaryInfC{$P(x), \langle x' = f(x)\&Q\rangle [x' = -f(x)\&Q]\neg P(x) \vdash \bot$}
\LeftLabel{$\to$R,$\langle\cdot\rangle$,$\neg$R}
\UnaryInfC{$\vdash P(x) \to [x' = f(x)\&Q]\langle x' = -f(x)\&Q\rangle P(x)$}
\end{prooftree}$$

The open premise resulting from a cut with $x = y \land [x' = f(x)\&Q]\neg P(x) \to [y' = f(y)\&Q]\neg P(y)$ is

$$\textcircled{1} \equiv x = y, [x' = f(x)\&Q]\neg P(x) \vdash [y' = f(y)\&Q]\neg P(y)$$

To complete the proof of Rev, premise ① needs to be resolved.

$$\begin{prooftree}
\AxiomC{$*$}
\LeftLabel{$\langle\cdot\rangle$,$\neg$L,id}
\UnaryInfC{$x = y, [x' = f(x)\&Q]\neg P(x), \langle x' = f(x)\&Q\rangle P(x) \vdash \bot$}
\LeftLabel{$K\langle\cdot\rangle$}
\UnaryInfC{$x = y, [x' = f(x)\&Q]\neg P(x), \langle x' = f(x)\&Q\rangle (x = z \land P(z)) \vdash \bot$}
\LeftLabel{V}
\UnaryInfC{$x = y, [x' = f(x)\&Q]\neg P(x), \langle x' = f(x)\&Q\rangle x = z, P(z) \vdash \bot$}
\LeftLabel{Dadj}
\UnaryInfC{$x = y, [x' = f(x)\&Q]\neg P(x), \langle z' = -f(z)\&Q\rangle z = x, P(z) \vdash \bot$}
\LeftLabel{V,$K\langle\cdot\rangle$}
\UnaryInfC{$x = y, [x' = f(x)\&Q]\neg P(x), \langle z' = -f(z)\&Q\rangle z = y, P(z) \vdash \bot$}
\LeftLabel{Dadj}
\UnaryInfC{$x = y, [x' = f(x)\&Q]\neg P(x), \langle y' = f(y)\&Q\rangle y = z, P(z) \vdash \bot$}
\LeftLabel{V}
\UnaryInfC{$x = y, [x' = f(x)\&Q]\neg P(x), \langle y' = f(y)\&Q\rangle (y = z \land P(z)) \vdash \bot$}
\LeftLabel{$K\langle\cdot\rangle$}
\UnaryInfC{$x = y, [x' = f(x)\&Q]\neg P(x), \langle y' = f(y)\&Q\rangle (y = z \land P(y)) \vdash \bot$}
\LeftLabel{$\exists$L}
\UnaryInfC{$x = y, [x' = f(x)\&Q]\neg P(x), \exists z \langle y' = f(y)\&Q\rangle (y = z \land P(y)) \vdash \bot$}
\LeftLabel{B$'$}
\UnaryInfC{$x = y, [x' = f(x)\&Q]\neg P(x), \langle y' = f(y)\&Q\rangle (\exists z (y = z) \land P(y)) \vdash \bot$}
\LeftLabel{G,$K\langle\cdot\rangle$}
\UnaryInfC{$x = y, [x' = f(x)\&Q]\neg P(x), \langle y' = f(y)\&Q\rangle P(y) \vdash \bot$}
\LeftLabel{$\langle\cdot\rangle$,$\neg$R}
\UnaryInfC{$x = y, [x' = f(x)\&Q]\neg P(x) \vdash [y' = f(y)\&Q]\neg P(y)$}
\end{prooftree}$$

This completes the proof of axiom Rev.

Stuck: While there might be easier ways to prove this, the completeness axiom dInv for differential invariants gives the difficult direction immediately.

$$\begin{prooftree}
\AxiomC{$\textcircled{1}$}
\UnaryInfC{$t = t_0, P \vdash [x' = f(x), t' = 1\&t \le t_0]P$}
\AxiomC{$*$}
\LeftLabel{$\mathbb{R}$}
\UnaryInfC{$t = t_0, t \le t_0 \to P \vdash P$}
\LeftLabel{DX}
\UnaryInfC{$t = t_0, [x' = f(x), t' = 1\&t \le t_0]P \vdash P$}
\LeftLabel{$\to$R}
\BinaryInfC{$t = t_0 \vdash [x' = f(x), t' = 1\&t \le t_0]P \leftrightarrow P$}
\LeftLabel{$\to$R}
\UnaryInfC{$\vdash t = t_0 \to ([x' = f(x), t' = 1\&t \le t_0]P \leftrightarrow P)$}
\end{prooftree}$$

Premise ① is easily proven by noting that if $x = x_0$ initially, then $I \equiv t = t_0 \land x = x_0$ is a valid differential invariant of the ODE $x' = f(x), t' = 1\&t \le t_0$, and can therefore be proven via dInv.

$$\text{cut,}\exists\text{L}\,\dfrac{\text{dC}\,\dfrac{\text{V,dW}\,\dfrac{*}{P(x_0,t_0) \vdash [x' = f(x), t' = 1 \& t \leq t_0 \land I]P(x,t)} \qquad \text{dInv}\,\dfrac{*}{\vdash I \rightarrow [x' = f(x), t' = 1 \& t \leq t_0]I}}{t = t_0, x = x_0, P(x_0,t_0) \vdash [x' = f(x), t' = 1 \& t \leq t_0]P(x,t)}}{t = t_0, P \vdash [x' = f(x), t' = 1 \& t \leq t_0]P}$$

This completes the proof of Stuck. The following useful corollary of Stuck will be used in future derivations.

$$t = t_0 \land \neg P \land \langle x' = f(x), t' = 1 \& Q\rangle P \rightarrow \langle x' = f(x), t' = 1 \& Q\rangle\, (P \land t > t_0)$$

Semantically this is not surprising, if P is not satisfied at the initial state, then there must be some evolution along the ODE to reach a state where P is true, and since $t' = 1$ is strictly increasing, such a state must also satisfy $t > t_0$. However, axiom Stuck provides a syntactic derivation of the axiom. The derivation begins with axiom B$'$ to quantify the final time value reached, cutting in an appropriate domain constraint that captures the monotonicity of $t' = 1$ then completes the derivation with an application of axiom Stuck.

$$\text{→R,}K\langle\cdot\rangle\,\dfrac{\text{B}',\exists\text{L}\,\dfrac{K\langle\cdot\rangle\,\dfrac{\text{K}\,\dfrac{\text{V}\,\dfrac{\text{cut}\,\dfrac{\text{dRW}\langle\cdot\rangle,K\langle\cdot\rangle\,\dfrac{\neg\text{R}\,\dfrac{\text{DR}\langle\cdot\rangle\text{,V}\,\dfrac{\langle\cdot\rangle,\neg\text{L}\,\dfrac{\text{Stuck}\,\dfrac{*}{t = t_0, \neg P \vdash [x' = f(x), t' = 1 \& t \leq t_0]\neg P}}{t = t_0, \neg P, \langle x' = f(x), t' = 1 \& t \leq t_0\rangle P \vdash \bot}}{t = t_0, s \leq t_0, \neg P, \langle x' = f(x), t' = 1 \& t \leq s\rangle P \vdash \bot}}{t = t_0, \neg P, \langle x' = f(x), t' = 1 \& t \leq s\rangle P \vdash s > t_0}}{t = t_0, \neg P, \langle x' = f(x), t' = 1 \& Q \land t \leq s\rangle\, (P \land t = s) \vdash s > t_0} \qquad ②}{t = t_0, \neg P, \langle x' = f(x), t' = 1 \& Q\rangle\, (P \land t = s) \vdash s > t_0}}{t = t_0, \neg P, \langle x' = f(x), t' = 1 \& Q\rangle\, (P \land t = s) \vdash [x' = f(x), t' = 1 \& Q]s > t_0}}{t = t_0, \neg P, \langle x' = f(x), t' = 1 \& Q\rangle\, (P \land t = s) \vdash [x' = f(x), t' = 1 \& Q](P \land t = s \rightarrow P \land t > t_0)}}{t = t_0, \neg P, \langle x' = f(x), t' = 1 \& Q\rangle\, (P \land t = s) \vdash \langle x' = f(x), t' = 1 \& Q\rangle\, (P \land t > t_0)}}{t = t_0, \neg P, \langle x' = f(x), t' = 1 \& Q\rangle\, (P \land \exists s (t = s)) \vdash \langle x' = f(x), t' = 1 \& Q\rangle\, (P \land t > t_0)}}{\vdash t = t_0 \land \neg P \land \langle x' = f(x), t' = 1 \& Q\rangle P \rightarrow \langle x' = f(x), t' = 1 \& Q\rangle\, (P \land t > t_0)}$$

The open premise ② arising from cutting in $\langle x' = f(x), t' = 1 \& Q \land t \leq s\rangle(P \land t = s)$ is:

$$② \equiv \langle x' = f(x), t' = 1 \& Q\rangle\, (P \land t = s) \vdash \langle x' = f(x), t' = 1 \& Q \land t \leq s\rangle\, (P \land t = s)$$

It therefore remains to prove ②, which follows directly from axiom $\langle\&\rangle$ with clock variable $t' = 1$ and noting that $t \leq s \rightarrow [x' = -f(x), t' = -1]t \leq s$ is a valid differential invariant, we also make the following abbreviation for clarity.

$$A \equiv \langle x' = f(x), t' = 1 \& Q \land t \leq s\rangle\, (P \land t = s)$$

$$\langle\&\rangle,\exists\text{L}\,\dfrac{\text{dInv,}K\langle\cdot\rangle\,\dfrac{\langle\&\rangle\text{,id}\,\dfrac{*}{t_0 = t, \langle x' = f(x), t' = 1\rangle\, (P \land t = s \land [x' = -f(x), t' = -1]\, (t \geq t_0 \rightarrow Q \land t \leq s)) \vdash A}}{t_0 = t, \langle x' = f(x), t' = 1\rangle\, (P \land t = s \land [x' = -f(x), t' = -1]\, (t \geq t_0 \rightarrow Q)) \vdash A}}{\langle x' = f(x), t' = 1 \& Q\rangle\, (P \land t = s) \vdash \langle x' = f(x), t' = 1 \& Q \land t \leq s\rangle\, (P \land t = s)}$$

This completes the proof. The corollaries of Stuck are recorded below as axioms, the positive time versions (i.e., Stuck$^+$,Mont$^+$) have been derived above, and the negative time versions can be derived in exactly the same fashion with $t' = -1$ instead of $t' = 1$.

$$\text{Stuck}^+ \quad t = t_0 \land \neg P \land \langle x' = f(x), t' = 1 \& Q\rangle P \rightarrow \langle x' = f(x), t' = 1 \& Q\rangle\, (P \land t > t_0)$$

$$\text{Stuck}^- \quad t = t_0 \land \neg P \land \langle x' = f(x), t' = -1 \& Q\rangle P \rightarrow \langle x' = f(x), t' = -1 \& Q\rangle\, (P \land t < t_0)$$

Premise ② and its negative time version will also be useful.

$$\text{Mont}^{+} \quad \langle x' = f(x), t' = 1\&Q\rangle\,(P \land t = s) \rightarrow \langle x' = f(x), t' = 1\&Q \land t \leq s\rangle\,(P \land t = s)$$

$$\text{Mont}^{-} \quad \langle x' = f(x), t' = -1\&Q\rangle\,(P \land t = s) \rightarrow \langle x' = f(x), t' = -1\&Q \land t \geq s\rangle\,(P \land t = s)$$

It is useful to note that by utilizing axiom B′, the condition $t = s$ in axioms Mont^{+},Mont^{-} can also be substituted by $t \leq s$ and $t \geq s$ respectively.

Idem: The derivation of axiom Idem heavily relies upon axiom $\langle\&\rangle$ to repeatedly remove domain constrains within modalities. The following abbreviation will be useful in its derivation.

$$A \equiv [x' = -f(x)]\,(c_0 \geq t_0 \rightarrow Q)$$

The proof first applies $\langle\&\rangle$ with the clock variable c_0 to the antecedent followed by Skolemizing the initial time value with $\exists$L to the witness t_0. Similarly, the second application of $\langle\&\rangle$ is applied to the succedent followed by Skolemizing the clock variable to the same witness t_0. Axiom $K\langle\cdot\rangle$ then reduces the open premise to proving an implication between the inner box-modalities that arised from $\langle\&\rangle$.

$$\begin{array}{rc}
 & \textcircled{1} \\ \cline{2-2}
 & P, A \vdash [x' = -f(x)]\,(c_0 \geq t_0 \rightarrow \langle x' = f(x)\&Q\rangle P) \\ \cline{2-2}
\scriptstyle \land\mathrm{R,id} & P, A \vdash P \land A \land [x' = -f(x)]\,(c_0 \geq t_0 \rightarrow \langle x' = f(x)\&Q\rangle P) \\ \cline{2-2}
\scriptstyle K\langle\cdot\rangle & t_0 = c_0, \langle x' = f(x)\rangle\,(P \land A) \vdash \langle x' = f(x)\rangle\,(P \land A \land [x' = -f(x)]\,(c_0 \geq t_0 \rightarrow \langle x' = f(x)\&Q\rangle P)) \\ \cline{2-2}
\scriptstyle []\land,K\langle\cdot\rangle & t_0 = c_0, \langle x' = f(x)\rangle\,(P \land A) \vdash \langle x' = f(x)\rangle\,(P \land [x' = -f(x)]\,(c_0 \geq t_0 \rightarrow Q \land \langle x' = f(x)\&Q\rangle P)) \\ \cline{2-2}
\scriptstyle \exists\mathrm{R} & t_0 = c_0, \langle x' = f(x)\rangle\,(P \land A) \vdash \exists s_0 = c_0 \langle x' = f(x)\rangle\,(P \land [x' = -f(x)]\,(c_0 \geq s_0 \rightarrow Q \land \langle x' = f(x)\&Q\rangle P)) \\ \cline{2-2}
\scriptstyle \langle\&\rangle & t_0 = c_0, \langle x' = f(x)\rangle\,(P \land A) \vdash \langle x' = f(x)\&Q \land \langle x' = f(x)\&Q\rangle P\rangle P \\ \cline{2-2}
\scriptstyle \exists\mathrm{L} & \exists t_0 = c_0 \langle x' = f(x)\rangle\,(P \land [x' = -f(x)]\,(c_0 \geq t_0 \rightarrow Q)) \vdash \langle x' = f(x)\&Q \land \langle x' = f(x)\&Q\rangle P\rangle P \\ \cline{2-2}
\scriptstyle \langle\&\rangle & \langle x' = f(x)\&Q\rangle P \vdash \langle x' = f(x)\&Q \land \langle x' = f(x)\&Q\rangle P\rangle P
\end{array}$$

The open premise ① can now be proven by first negating the succedent and then applying axiom Mont^{-}. Recall that $x' = -f(x)$ is assumed to contain the clock variable $c_0' = -1$ and therefore Mont^{-} is applicable with the time variable t being c_0.

$$\begin{array}{rc}
 & * \\ \cline{2-2}
\scriptstyle \langle\cdot\rangle,\neg\mathrm{L,id} & [x' = -f(x)\&Q]\langle x' = f(x)\&Q\rangle P, \langle x' = -f(x)\&Q\rangle[x' = f(x)\&Q]\neg P \vdash \bot \\ \cline{2-2}
\scriptstyle \mathrm{Rev} & P, \langle x' = -f(x)\&Q\rangle[x' = f(x)\&Q]\neg P \vdash \bot \\ \cline{2-2}
\scriptstyle \mathrm{DR}\langle\cdot\rangle & P, [x' = -f(x)]\,(c_0 \geq t_0 \rightarrow Q)\,, \langle x' = -f(x)\&c_0 \geq t_0\rangle[x' = f(x)\&Q]\neg P \vdash \bot \\ \cline{2-2}
\scriptstyle \mathrm{Mont}^{-} & P, [x' = -f(x)]\,(c_0 \geq t_0 \rightarrow Q)\,, \langle x' = -f(x)\rangle\,(c_0 \geq t_0 \land [x' = f(x)\&Q]\neg P) \vdash \bot \\ \cline{2-2}
\scriptstyle \langle\cdot\rangle,\neg\mathrm{R} & P, [x' = -f(x)]\,(c_0 \geq t_0 \rightarrow Q) \vdash [x' = -f(x)]\,(c_0 \geq t_0 \rightarrow \langle x' = f(x)\&Q\rangle P)
\end{array}$$

Uniq’: Before deriving this axiom, we make the following abbreviations for brevity:

$$\begin{aligned}
A &\equiv \langle x' = f(x)\&Q_1\rangle P_1 \\
\mathcal{A} &\equiv \langle x' = f(x)\&Q_1 \land A\rangle P_1 \\
B &\equiv \langle x' = f(x)\&Q_2\rangle P_2 \\
\mathcal{B} &\equiv \langle x' = f(x)\&Q_2 \land B\rangle P_2 \\
C &\equiv \langle x' = f(x)\&Q_1 \land Q_2\rangle\,(P_1 \land B) \lor \langle x' = f(x)\&Q_1 \land Q_2\rangle\,(P_2 \land A)
\end{aligned}$$

$$\text{→R,Idem}\ \dfrac{\text{K⟨·⟩,Uniq}\ \dfrac{\text{⟨⟩∨}\ \dfrac{\text{dW⟨·⟩,dRW⟨·⟩}\ \dfrac{\text{id}\ \dfrac{*}{\langle x' = f(x) \& Q_1 \wedge Q_2\rangle\,(P_1 \wedge B) \vee \langle x' = f(x) \& Q_1 \wedge Q_2\rangle\,(P_2 \wedge A) \vdash C}}{\langle x' = f(x) \& Q_1 \wedge Q_2 \wedge A \wedge B\rangle P_1 \vee \langle x' = f(x) \& Q_1 \wedge Q_2 \wedge A \wedge B\rangle P_2 \vdash C}}{\langle x' = f(x) \& Q_1 \wedge Q_2 \wedge A \wedge B\rangle\,(P_1 \vee P_2) \vdash C}}{\mathcal{A}, \mathcal{B} \vdash \langle x' = f(x) \& Q_1 \wedge Q_2\rangle\,(P_1 \wedge B) \vee \langle x' = f(x) \& Q_1 \wedge Q_2\rangle\,(P_2 \wedge A)}}{\vdash A \wedge B \rightarrow \langle x' = f(x) \& Q_1 \wedge Q_2\rangle\,(P_1 \wedge B) \vee \langle x' = f(x) \& Q_1 \wedge Q_2\rangle\,(P_2 \wedge A)}$$

IVT: Classically, the intermediate value theorem is usually proven directly from the completeness of $\mathbb{R}$ (and indeed they are equivalent), so it might be expected that axiom RI is utilized. Indeed, the derivation relies upon the derived proof rule Enc, which itself relies on RI. The derivation begins by contradiction, negating the succedent and applying Enc proves that $e < 0$ always holds along the flow under the domain constraint $t < \tau$. Note that $e \neq 0$ under the domain constraint of $e \leq 0$ reduces down to $e < 0$ by K.

$$\text{→R,⟨·⟩}\ \dfrac{\text{¬R,K}\ \dfrac{\text{Enc}\ \dfrac{\dfrac{①}{e \leq 0, \langle x' = f(x), t' = 1 \& Q\rangle\,(t = \tau \wedge e > 0)\,, [x' = f(x), t' = 1 \& Q \wedge t < \tau]e < 0 \vdash \bot}}{e \leq 0, \langle x' = f(x), t' = 1 \& Q\rangle\,(t = \tau \wedge e > 0)\,, [x' = f(x), t' = 1 \& Q \wedge t < \tau \wedge e \leq 0]e < 0 \vdash \bot}}{e \leq 0, \langle x' = f(x), t' = 1 \& Q\rangle\,(t = \tau \wedge e > 0) \vdash \neg[x' = f(x), t' = 1 \& Q \wedge t < \tau \wedge e \leq 0]e \neq 0}}{\vdash e \leq 0 \wedge \langle x' = f(x), t' = 1 \& Q\rangle\,(t = \tau \wedge e > 0) \rightarrow \langle x' = f(x), t' = 1 \& Q \wedge t < \tau \wedge e \leq 0\rangle e = 0}$$

Continuing from ①, the derivation crucially relies on Dadj which flows along the reverse ODE $x' = -f(x), t' = -1$ to reach a state where $t_0 < t < \tau \wedge e > 0$, with t_0 being the initial time value. Semantically, we have found a flow along $x' = f(x), t' = 1$ to a state where both $t < \tau$ and $e > 0$ are true, contradicting the fact that $e < 0$ holds along the flow while $t < \tau$. Synthesizing the argument above within dL first requires extensive use of B′ to instantiate extra variables which allows us to apply axiom Cont, flowing to a state where both $t < \tau$ and $e > 0$ hold. A final application of Uniq' then gives the desired contradictions. Again for brevity, we first make the following abbreviation.

$$\begin{aligned} \alpha(x,t) &\equiv x' = f(x), t' = 1 \\ -\alpha(x,t) &\equiv x' = -f(x), t' = -1 \\ A(x,t,\tau) &\equiv [\alpha(x,t) \& Q(x,t) \wedge t < \tau]e(x,t) < 0 \end{aligned}$$

$$\text{K⟨·⟩}\ \dfrac{\text{B′,∃L}\ \dfrac{\text{V,Dadj}\ \dfrac{\text{V}\ \dfrac{\text{Cont,Stuck}^-\ \dfrac{\text{Uniq',∨L}\ \dfrac{①\qquad ②}{e(x,t) \leq 0, A(x,t,s), e(y,\tau) > 0, \langle -\alpha(y,\tau) \& Q(y,\tau)\rangle\,(x = y \wedge \tau = t)\,, \langle -\alpha(y,\tau) \& e(y,\tau) > 0\rangle\,(\tau < s) \vdash \bot}}{e(x,t) \leq 0, A(x,t,s), e(y,\tau) > 0, y = z, \tau = s, \langle -\alpha(y,\tau) \& Q(y,\tau)\rangle\,(x = y \wedge \tau = t) \vdash \bot}}{e(x,t) \leq 0, A(x,t,\tau), e(y,\tau) > 0, y = z, \tau = s, \langle -\alpha(y,\tau) \& Q(y,\tau)\rangle\,(x = y \wedge \tau = t) \vdash \bot}}{e(x,t) \leq 0, \langle \alpha(x,t) \& Q(x,t)\rangle\,(x = y \wedge y = z \wedge t = \tau \wedge \tau = s \wedge e(x,t) > 0)\,, A(x,t,\tau) \vdash \bot}}{e(x,t) \leq 0, \langle \alpha(x,t) \& Q(x,t)\rangle\,(\exists y = x \wedge \exists z = x \wedge \exists s = \tau \wedge t = \tau \wedge e(x,t) > 0)\,, A(x,t,\tau) \vdash \bot}}{e(x,t) \leq 0, \langle x' = f(x), t' = 1 \& Q(x,t)\rangle\,(t = \tau \wedge e(x,t) > 0)\,, A(x,t,\tau) \vdash \bot}$$

Where the open premises arising from Uniq',∨L are

$$\begin{aligned} ① &\equiv e(x,t) \leq 0, \langle -\alpha(y,\tau) \& Q(y,\tau)\rangle\,(x = y \wedge t = \tau \wedge \langle -\alpha(y,\tau) \& e(y,\tau) > 0\rangle\,(\tau < s)) \vdash \bot \\ ② &\equiv A(x,t,s), \langle -\alpha(y,\tau) \& e(y,\tau) > 0\rangle\,(\tau < s \wedge \langle -\alpha(y,\tau) \& Q(y,\tau)\rangle\,(x = y \wedge t = \tau)) \vdash \bot \end{aligned}$$

Intuitively, ① yields a contradiction since the first diamond modality flows to a state where $e(y,\tau) = e(x,t) \leq 0$ is true, but the second diamond modality *requires* $e(y,\tau) > 0$ as a domain constraint. Since the domain constraint is not satisfied, the overall formula is indeed false. For ②, another application of Dadj to the inner modality gives a flow that contradicts $A(x, t, s)$. We deal with ① first:

$$\mathrm{V}\,\dfrac{K\langle\cdot\rangle,\mathrm{V}\,\dfrac{\langle\cdot\rangle,\neg\mathrm{L}\,\dfrac{\mathrm{DX}\,\dfrac{\rightarrow\!\mathrm{R}\,\dfrac{\mathbb{R}\,\dfrac{\dfrac{*}{\bot \vdash \tau \geq s \wedge [-\alpha(y,\tau)\&e(y,\tau) > 0]\,(\tau \geq s)}}{e(y,\tau) \leq 0, e(y,\tau) > 0 \vdash \tau \geq s \wedge [-\alpha(y,\tau)\&e(y,\tau) > 0]\,(\tau \geq s)}}{e(y,\tau) \leq 0 \vdash e(y,\tau) > 0 \rightarrow \tau \geq s \wedge [-\alpha(y,\tau)\&e(y,\tau) > 0]\,(\tau \geq s)}}{e(y,\tau) \leq 0 \vdash [-\alpha(y,\tau)\&e(y,\tau) > 0]\,(\tau \geq s)}}{e(y,\tau) \leq 0, \langle -\alpha(y,\tau)\&e(y,\tau) > 0\rangle\,(\tau < s) \vdash \bot}}{e(x,t) \leq 0, \langle -\alpha(y,\tau)\&Q(y,\tau)\rangle\,(e(y,\tau) \leq 0 \wedge \langle -\alpha(y,\tau)\&e(y,\tau) > 0\rangle\,(\tau < s)) \vdash \bot}}{e(x,t) \leq 0, \langle -\alpha(y,\tau)\&Q(y,\tau)\rangle\,(x = y \wedge t = \tau \wedge \langle -\alpha(y,\tau)\&e(y,\tau) > 0\rangle\,(\tau < s)) \vdash \bot}$$

Continuing with the proof of ②, we have:

$$\mathrm{V,dW}\langle\cdot\rangle\,\dfrac{K\langle\cdot\rangle,\mathrm{V}\,\dfrac{\mathrm{Dadj}\,\dfrac{\mathrm{Mont}^{+}\,\dfrac{\mathrm{DR}\langle\cdot\rangle,\mathrm{V}\,\dfrac{\langle\cdot\rangle\,\dfrac{\neg\mathrm{L,id}\,\dfrac{*}{A(x,t,s), \neg A(x,t,s) \vdash \bot}}{A(x,t,s), \langle \alpha(x,t)\&Q(x,t) \wedge t < s\rangle\,(e(x,t) > 0) \vdash \bot}}{A(x,t,s), e(y,\tau) > 0, \tau < s, \langle \alpha(x,t)\&Q(x,t) \wedge t \leq \tau\rangle\,(x = y \wedge t = \tau) \vdash \bot}}{A(x,t,s), e(y,\tau) > 0, \tau < s, \langle \alpha(x,t)\&Q(x,t)\rangle\,(x = y \wedge t = \tau) \vdash \bot}}{A(x,t,s), e(y,\tau) > 0, \tau < s, \langle -\alpha(y,\tau)\&Q(y,\tau)\rangle\,(x = y \wedge t = \tau) \vdash \bot}}{\langle -\alpha(y,\tau)\&e(y,\tau){>}0\rangle\,(A(x,t,s) \wedge e(y,\tau){>}0 \wedge \tau{<}s \wedge \langle -\alpha(y,\tau)\&Q(y,\tau)\rangle\,(x = y \wedge t = \tau)) \vdash \bot}}{A(x,t,s), \langle -\alpha(y,\tau)\&e(y,\tau) > 0\rangle\,(\tau < s \wedge \langle -\alpha(y,\tau)\&Q(y,\tau)\rangle\,(x = y \wedge t = \tau)) \vdash \bot}$$

This concludes the proof of Lemma 5.9. Note that for IVT, axiom B′ allows us to relax the condition of $t = \tau$ in the antecedent to $t \leq \tau$ without loss of provability. □

Proof of Theorem 5.7. StepDual$_{\rightarrow}$: To derive this axiom, we first utilize BDG to cut in the formula

$$\langle x' = f(x), t' = 1\&t \leq \tau\rangle t = \tau$$

after which an application of DR$\langle\cdot\rangle$ will give the desired outcome.

$$\rightarrow\!\mathrm{R,cut}\,\dfrac{\dfrac{\text{①}}{t \leq \tau, [x' = f(x), t' = 1\&t \leq \tau]B(x) \vdash \langle x' = f(x), t' = 1\&t \leq \tau\rangle t = \tau} \qquad \text{②}}{\vdash t \leq \tau \wedge [x' = f(x), t' = 1\&t \leq \tau]B(x) \rightarrow \langle x' = f(x), t' = 1\&B(x)\rangle t = \tau}$$

Where the premises arising from cut are

① $\equiv t \leq \tau, [x' = f(x), t' = 1\&t \leq \tau]B(x) \vdash \langle x' = f(x), t' = 1\&t \leq \tau\rangle t = \tau$

② $\equiv [x' = f(x), t' = 1\&t{\leq}\tau]B(x), \langle x' = f(x), t' = 1\&t{\leq}\tau\rangle t = \tau \vdash \langle x' = f(x), t' = 1\&B(x)\rangle t = \tau$

To prove ①, axiom BDG reduces the problem to proving $[x' = f(x), t' = 1\&t \leq \tau]\, \|x\|^2 \leq p(t)$, where $p(t)$ is some polynomial in terms of t. Since $B(x)$ is a bounded set, the FOL$_{\mathbb{R}}$ formula $\exists D \forall x (B(x) \rightarrow \|x\|^2 \leq D)$ is valid, and therefore $p(t)$ can be simply be chosen to be $p(t) \equiv D$ for some $D \in \mathbb{Q}^{+}$ a witness of the FOL$_{\mathbb{R}}$ formula. Expressing this argument in sequent form gives:

$$\mathrm{cut},\exists\mathrm{L},\mathbb{R}\,\dfrac{\mathrm{BDG}\langle\cdot\rangle\,\dfrac{\text{③} \qquad \langle{}'\rangle\,\dfrac{*}{t \leq \tau \vdash \langle t' = 1\&t \leq \tau\rangle t = \tau}}{t{\leq}\tau, \forall x \left(B(x) \rightarrow \|x\|^2 {\leq} D\right), [x' = f(x), t' = 1\&t \leq \tau]B(x) \vdash \langle x' = f(x), t' = 1\&t \leq \tau\rangle t = \tau}}{t \leq \tau, [x' = f(x), t' = 1\&t \leq \tau]B(x) \vdash \langle x' = f(x), t' = 1\&t \leq \tau\rangle t = \tau}$$

Where

③ $\equiv \forall x \left(B(x) \rightarrow \|x\|^2 \leq D\right), [x' = f(x), t' = 1\&t \leq \tau]B(x) \vdash [x' = f(x), t' = 1\&t \leq \tau]\, \|x\|^2 \leq D$

③ is proven by first applying dC to cut in the domain constraint $B(x)$ to the succedent, after which an application of dW completes the proof since the formula $\forall x\,\big(B(x) \rightarrow \|x\|^2 \le D\big)$ is independent of the ODE $x' = f(x), t' = 1$.

$$
\text{dC}\;\dfrac{\text{dW}\;\dfrac{\mathbb{R}\;\dfrac{*}{\forall x\,\big(B(x) \rightarrow \|x\|^2 \le D\big),\, t \le \tau \land B(x) \vdash \|x\|^2 \le D}}{\forall x\,\big(B(x) \rightarrow \|x\|^2 \le D\big) \vdash [x' = f(x), t' = 1 \& t \le \tau \land B(x)]\, \|x\|^2 \le D}}{\forall x\,\big(B(x) \rightarrow \|x\|^2 \le D\big),\, [x' = f(x), t' = 1 \& t \le \tau]B(x) \vdash [x' = f(x), t' = 1 \& t \le \tau]\, \|x\|^2 \le D}
$$

The open premise ③ has been proven and therefore so has ①. ② is now proved utilizing DR$\langle\cdot\rangle$ to add in the domain constraint of $B(x)$.

$$
\text{DR}\langle\cdot\rangle\;\dfrac{\text{dRW}\langle\cdot\rangle\;\dfrac{*}{\langle x' = f(x), t' = 1 \& t \le \tau \land B(x)\rangle t = \tau \vdash \langle x' = f(x), t' = 1 \& B(x)\rangle t = \tau}}{[x' = f(x), t' = 1 \& t \le \tau]B(x), \langle x' = f(x), t' = 1 \& t \le \tau\rangle t = \tau \vdash \langle x' = f(x), t' = 1 \& B(x)\rangle t = \tau}
$$

This completes the proof of StepDual$_{\rightarrow}$.

StepDual$_{\leftarrow}$: For brevity, first make the following abbreviations:

$$
\begin{aligned}
A &\equiv \langle x' = f(x), t' = 1 \& Q\rangle t \ge \tau \\
B &\equiv \langle x' = f(x), t' = 1 \& t \le \tau\rangle \neg Q
\end{aligned}
$$

Axiom StepDual$_{\leftarrow}$ says that if there is some flow of the ODE $x' = f(x), t' = 1 \& Q$ where time surpasses τ, then *every* flow of this ODE before time $t = \tau$ will remain within the domain constraint Q. Alternatively, this axiom is precisely the uniqueness property of ODE flows. Consequently, our derivation will follow the classical soundness argument. If the implication is not valid, then there are two disjoint flows of the ODE, contradicting Uniq'. For brevity, we also make the following abbreviations:

$$
\text{→R,⟨·⟩,¬R}\;\dfrac{\text{Uniq'}\;\dfrac{\vee\text{L}\;\dfrac{\dfrac{①}{\langle x' = f(x), t' = 1 \& Q \land t \le \tau\rangle\,(t \ge \tau \land B) \vdash \bot} \qquad \text{dW}\langle\cdot\rangle\;\dfrac{\text{V}\;\dfrac{*}{\langle x' = f(x), t' = 1 \& Q \land t \le \tau\rangle\,(\neg Q \land Q \land A) \vdash \bot}}{\langle x' = f(x), t' = 1 \& Q \land t \le \tau\rangle\,(\neg Q \land A) \vdash \bot}}{\langle x' = f(x), t' = 1 \& Q \land t \le \tau\rangle\,(t \ge \tau \land B) \lor \langle x' = f(x), t' = 1 \& Q \land t \le \tau\rangle\,(\neg Q \land A) \vdash \bot}}{\langle x' = f(x), t' = 1 \& Q\rangle t \ge \tau, \langle x' = f(x), t' = 1 \& t \le \tau\rangle \neg Q \vdash \bot}}{\vdash \langle x' = f(x), t' = 1 \& Q\rangle t \ge \tau \rightarrow [x' = f(x), t' = 1 \& t \le \tau]Q}
$$

The right branch arising from $\vee$L closes easily by noting $\neg Q \land Q \equiv \bot$ and applying axiom dW$\langle\cdot\rangle$. For ①, B says there is some flow along $x' = f(x), t' = 1 \& t \le \tau$ reaching $\neg Q$. But since the first diamond modality already reaches a state where $t \ge \tau$, there cannot possibly be any non-trivial evolution, and therefore Q must remain true, a contradiction.

$$
\text{dW}\langle\cdot\rangle\;\dfrac{K\langle\cdot\rangle\text{,Stuck}\;\dfrac{\text{V}\;\dfrac{*}{\langle x' = f(x), t' = 1 \& Q \land t \le \tau\rangle\,(t = \tau \land Q \land \neg Q) \vdash \bot}}{\langle x' = f(x), t' = 1 \& Q \land t \le \tau\rangle\,(t = \tau \land Q \land \langle x' = f(x), t' = 1 \& t \le \tau\rangle \neg Q) \vdash \bot}}{\langle x' = f(x), t' = 1 \& Q \land t \le \tau\rangle\,(t \ge \tau \land B) \vdash \bot}
$$

where we used Stuck by negating the succedent, resulting in

$$
t = \tau \rightarrow (\langle x' = f(x), t' = 1 \& t \le \tau\rangle \neg Q \leftrightarrow \neg Q)
$$

this completes the derivation of StepDual$_{\leftarrow}$.

StepEx: Derivation of StepEx mostly follows from axioms IVT and dInv. Mathematically, the boundedness requirement on $f(x)$ implies $\|x(t) - x_0\| \le M(t - t_0)$, essentially the multivariate mean value theorem where $x(t)$ is the flow of $x' = f(x), x(t_0) = x_0$ at time t. By StepDual$_{\rightarrow}$ and IVT, if the axiom does not hold, then there exists some point where the bound $\|x(t) - x_0\| \leq M(t - t_0)$ is violated, resulting in a contradiction. The derivation is as follows ($\max_{y \in B[x_0,R]} \|f(y)\|^2 \leq M^2$ abbreviates $\forall y(y \in B[x_0, R] \to \|f(y)\|^2 \leq M^2)$).

$$\begin{array}{rc}
 & \textcircled{1} \qquad \textcircled{2} \\ \hline
\text{cut} & \max_{y \in B[x_0,R]} \|f(y)\|^2 \leq M^2, x=x_0, t=t_0, \langle x'=f(x), t'=1 \& t < t_0 + \frac{R}{M} \land x \in B[x_0,R] \rangle \|x - x_0\|^2 = R^2 \vdash \bot \\ \hline
\text{IVT} & \max_{y \in B[x_0,R]} \|f(y)\|^2 \leq M^2, x=x_0, t=t_0, \langle x'=f(x), t'=1 \& t \leq t_0 + \frac{R}{M} \rangle \|x - x_0\|^2 > R^2 \vdash \bot \\ \hline
\langle \cdot \rangle, \neg\text{R} & \max_{y \in B[x_0,R]} \|f(y)\|^2 \leq M^2, x=x_0, t=t_0 \vdash [x'=f(x), t'=1 \& t \leq t_0 + \frac{R}{M}] x \in B[x_0,R] \\ \hline
\text{StepDual}_{\to} & \max_{y \in B[x_0,R]} \|f(y)\|^2 \leq M^2, x=x_0, t=t_0 \vdash \langle x'=f(x), t'=1 \& x \in B[x_0,R] \rangle t \geq t_0 + \frac{R}{M} \\ \hline
\to\text{R}, \to\text{R} & \vdash \max_{y \in B[x_0,R]} \|f(y)\|^2 \leq M^2 \to \left(x=x_0 \land t=t_0 \to \langle x'=f(x), t'=1 \& x \in B[x_0,R] \rangle t \geq t_0 + \frac{R}{M} \right)
\end{array}$$

Where we are cutting in the differential invariant representing the multivariate mean value theorem at the last step, giving:

$$\begin{aligned}
\alpha(x,t) &\equiv x' = f(x), t' = 1 \& t < t_0 + \frac{R}{M} \land x \in B[x_0, R] \\
I(x,t) &\equiv D(x,t) \to [x' = f(x), t' = 1 \& x \in B[x_0, R] \land \max_{y \in B[x_0,R]} \|f(y)\|^2 \leq M^2] D(x,t) \\
D(x,t) &\equiv \|x - x_0\|^2 \leq M^2 (t - t_0)^2 \land t \geq t_0 \\
\textcircled{1} &\equiv x = x_0, t = t_0, \max_{y \in B[x_0,R]} \|f(y)\|^2 \leq M^2, I(x,t), \langle \alpha(x,t) \rangle \|x - x_0\|^2 = R^2 \vdash \bot \\
\textcircled{2} &\equiv \ \vdash I(x,t)
\end{aligned}$$

② is derived first. By the completeness of differential invariants, it is suffices to establish the validity of $I(x,t)$ semantically. To show that ② holds semantically, let $\omega \in \mathbb{S}$ be some arbitrary state where $\omega \models D$. Let $\varphi : [0, \tau] \to \mathbb{S}$ be any solution satisfying the ODE $x' = f(x), t' = 1$ with $\varphi(0) = \omega$ and $\varphi(t) \models x' = f(x), t' = 1 \land x \in B[x_0, R] \land \max_{y \in B[x_0,R]} \|f(y)\|^2 \leq M^2$ for all $t \in [0, \tau]$. We want to show that $\varphi(\tau) \models D$ as well. To this end, let us denote $x(t) = \varphi(t)(x)$ as the trajectory of x under the given ODE. The triangle inequality together with the multivariate mean value theorem gives

$$\|x(\tau) - x_0\| \leq \|x(0) - x_0\| + \|x(\tau) - x(0)\| \leq M(\varphi(0)(t) - t_0) + \max_{\zeta \in [t_0, \tau]} \|x'(\zeta)\| \, \tau$$

Note that taking square roots implicitly used the assumption $\varphi(0) \models D$ and therefore $\varphi(0)(t) - t_0 \geq 0$. We will write x_0 (and similarly t_0) instead of $\varphi(s)(x_0)$ for all $s \in [0, \tau]$, as x_0, t_0 are just constants along the given ODE, and will therefore not vary along φ. Since $\varphi \models x' = f(x) \land x \in B[x_0, R] \land \max_{y \in B[x_0,R]} \|f(y)\|^2 \leq M^2$, this gives the bound $\max_{\zeta \in [t_0, \tau]} \|x'(\zeta)\| \leq M$ and consequently the following bound on $\|x(\tau) - x_0\|$

$$\begin{aligned}
\|x(\tau) - x_0\| \leq M(\varphi(0)(t) - t_0) + \max_{\zeta \in [t_0, \tau]} \|x'(\zeta)\| \, \tau &\leq M(\varphi(0)(t) - t_0) + M\tau \\
&= M(\tau + \varphi(0)(t) - t_0)
\end{aligned}$$

Finally, $\varphi \models t' = 1$ implies $\varphi(s)(t) = s + \varphi(0)(t)$ since the solution to $t' = 1$ is just $t(s) = s + t(0)$. In particular, this yields $\tau + \varphi(0)(t) = \varphi(\tau)(t)$, so we have

$$\|x(\tau) - x_0\| \leq M(\tau + \varphi(0)(t) - t_0) = M(\varphi(\tau)(t) - t_0)$$

Squaring both sides then gives the desired claim of $\varphi(\tau) \models D$, proving $I(x,t)$ to be valid. Consequently ② closes by a single application of axiom dInv.

For premise ①:

$$
\to\text{L}\,\dfrac{\text{dW}\langle\cdot\rangle\,\dfrac{\text{dRW}\langle\cdot\rangle\,\dfrac{K\langle\cdot\rangle,\mathbb{R}\,\dfrac{\langle\cdot\rangle,\neg\text{L},\text{id}\,\dfrac{*}{[x'=f(x),t'=1\&x\in B[x_0,R]]D(x,t),\langle x'=f(x),t'=1\&x\in B[x_0,R]\rangle\neg D(x,t)\vdash\bot}}{[x'=f(x),t'=1\&x\in B[x_0,R]]D(x,t),\langle x'=f(x),t'=1\&x\in B[x_0,R]\rangle\left(\|x-x_0\|^2=R^2\land t-t_0<\frac{R}{M}\right)\vdash\bot}}{[x'=f(x),t'=1\&x\in B[x_0,R]]D(x,t),\langle\alpha(x,t)\rangle\left(\|x-x_0\|^2=R^2\land t-t_0<\frac{R}{M}\right)\vdash\bot}}{[x'=f(x),t'=1\&x\in B[x_0,R]]D(x,t),\langle\alpha(x,t)\rangle\,\|x-x_0\|^2=R^2\vdash\bot}}{x=x_0,t=t_0,\max_{y\in B[x_0,R]}\|f(y)\|^2\le M^2,I(x,t),\langle\alpha(x,t)\rangle\,\|x-x_0\|^2=R^2\vdash\bot}
$$

This completes the derivation of StepEx.

StepExt: The main idea in deriving this axiom is to note that IVT and Uniq' allows one to decompose diamond modalities into different time steps, from which the premises allow us to complete the proof. We denote the premises as ⓐ, ⓑ, ⓒ and will indicate when they are used during the derivation, where:

$$
\begin{aligned}
&\text{ⓐ}\equiv\Gamma_1\vdash[x'=f(x),t'=1\&t\le t_0]P_1\\
&\text{ⓑ}\equiv\Gamma_2\vdash[x'=f(x),t'=1\&t\le t_0+t_1]P_2\\
&\text{ⓒ}\equiv t=t_0,P_1\vdash\Gamma_2
\end{aligned}
$$

$$
\langle\cdot\rangle,\neg\text{R}\,\dfrac{\langle\rangle\vee\,\dfrac{\text{①}\qquad\text{②}}{t\le t_0,\Gamma_1,\langle x'=f(x),t'=1\&t\le t_0+t_1\rangle\left((t\le t_0\land\neg P_1)\lor(t>t_0\land\neg P_2)\right)\vdash\bot}}{t\le t_0,\Gamma_1\vdash[x'=f(x),t'=1\&t\le t_0+t_1]\left((t\le t_0\to P_1)\land(t>t_0\to P_2)\right)}
$$

With the open premises being

$$\text{①}\equiv t\le t_0,\Gamma_1,\langle x'=f(x),t'=1\&t\le t_0+t_1\rangle\,(t\le t_0\land\neg P_1)\vdash\bot$$

$$\text{②}\equiv t\le t_0,\Gamma_1,\langle x'=f(x),t'=1\&t\le t_0+t_1\rangle\,(t>t_0\land\neg P_2)\vdash\bot$$

Premise ① is proven first, noting that the diamond modality directly contradicts ⓐ after applying Mont$^+$ to add in the domain constraint of $t\le t_0$.

$$
\text{Mont}^+\,\dfrac{\text{dRW}\langle\cdot\rangle\,\dfrac{K\langle\cdot\rangle\,\dfrac{\text{cut}\,\dfrac{\langle\cdot\rangle,\neg\text{L},\text{id}\,\dfrac{*}{t\le t_0,\Gamma_1,\langle x'=f(x),t'=1\&t\le t_0\rangle\neg P_1,[x'=f(x),t'=1\&t\le t_0]P_1\vdash\bot}\qquad\text{③}}{t\le t_0,\Gamma_1,\langle x'=f(x),t'=1\&t\le t_0\rangle\neg P_1\vdash\bot}}{t\le t_0,\Gamma_1,\langle x'=f(x),t'=1\&t\le t_0\rangle(t\le t_0\land\neg P_1)\vdash\bot}}{t\le t_0,\Gamma_1,\langle x'=f(x),t'=1\&t\le t_0+t_1\land t\le t_0\rangle\,(t\le t_0\land\neg P_1)\vdash\bot}}{t\le t_0,\Gamma_1,\langle x'=f(x),t'=1\&t\le t_0+t_1\rangle\,(t\le t_0\land\neg P_1)\vdash\bot}
$$

And ③ is

$$\text{③}\equiv\Gamma_1\vdash[x'=f(x),t'=1\&t\le t_0]P_1\equiv\text{ⓐ}$$

In other words, ① derives with premise ⓐ. We prove premise ② next, by first applying axiom IVT on the term $e\equiv t-t_0$.

$$
\text{IVT}\,\dfrac{\text{Uniq}',\vee\text{L}\,\dfrac{\text{④}\qquad\text{⑤}}{t\le t_0,\Gamma_1,\langle x'=f(x),t'=1\&t\le t_0+t_1\rangle\,(t>t_0\land\neg P_2)\,,\langle x'=f(x),t'=1\&t\le t_0\rangle t=t_0\vdash\bot}}{t\le t_0,\Gamma_1,\langle x'=f(x),t'=1\&t\le t_0+t_1\rangle\,(t>t_0\land\neg P_2)\vdash\bot}
$$

Where the open premises are the ones arising from the disjunction in Uniq', we have:

$$
\begin{aligned}
&④ \equiv \Gamma_1, \langle x' = f(x), t' = 1 \& t \le t_0 \rangle \, (t = t_0 \land \langle x' = f(x), t' = 1 \& t \le t_0 + t_1 \rangle \, (t > t_0 \land \neg P_2)) \vdash \bot \\
&⑤ \equiv \langle x' = f(x), t' = 1 \& t \le t_0 + t_1 \rangle \, (t > t_0 \land \neg P_2 \land \langle x' = f(x), t' = 1 \& t \le t_0 \rangle t = t_0) \vdash \bot
\end{aligned}
$$

Premise ⑤ is resolved first, noticing that the inequality $t > t_0$ contradicts with the domain constraint of the second diamond modality, so axiom DX yields the desired derivation.

$$
\mathrm{V}\;\dfrac{\langle\cdot\rangle,\neg\mathrm{L}\;\dfrac{\mathrm{DX}\;\dfrac{\to\mathrm{R}\;\dfrac{\mathbb{R}\;\dfrac{*}{t > t_0, t \le t_0, \neg P_2 \vdash t = t_0 \land [x' = f(x), t' = 1 \& t \le t_0] t = t_0}}{t > t_0, \neg P_2 \vdash t \le t_0 \to t = t_0 \land [x' = f(x), t' = 1 \& t \le t_0] t = t_0}}{t > t_0, \neg P_2 \vdash [x' = f(x), t' = 1 \& t \le t_0] t = t_0}}{t > t_0, \neg P_2, \langle x' = f(x), t' = 1 \& t \le t_0 \rangle t = t_0 \vdash \bot}}{\langle x' = f(x), t' = 1 \& t \le t_0 + t_1 \rangle \, (t > t_0 \land \neg P_2 \land \langle x' = f(x), t' = 1 \& t \le t_0 \rangle t = t_0) \vdash \bot}
$$

We now prove the remaining premise ④. Intuitively speaking, the first diamond modality reaches some state where $t = t_0, P_1$ are both true (by premise ⓐ), from which premise ⓒ implies the truth of Γ_2, and therefore premise ⓑ gives a contradiction with the second modality. This gives the following derivation, where each of ⓐ, ⓑ, ⓒ indicates the corresponding assumption being cut in:

$$
\mathrm{cut,DR}\langle\cdot\rangle\;\dfrac{\mathrm{dW}\langle\cdot\rangle\;\dfrac{\mathrm{V}\;\dfrac{\mathrm{cut}\;\dfrac{\mathrm{cut,\to L}\;\dfrac{\langle\cdot\rangle,\neg\mathrm{L}\;\dfrac{\mathrm{K}\;\dfrac{*}{[x'=f(x), t'=1\&t \le t_0 + t_1] P_2 \vdash [x'=f(x), t'=1\&t \le t_0 + t_1] \, (t \le t_0 \lor P_2)}}{[x'=f(x), t'=1\&t \le t_0 + t_1] P_2, \langle x'=f(x), t'=1\&t \le t_0 + t_1 \rangle \, (t > t_0 \land \neg P_2) \vdash \bot} \quad \text{ⓑ}}{\Gamma_2, \langle x'=f(x), t'=1\&t \le t_0 + t_1 \rangle \, (t > t_0 \land \neg P_2) \vdash \bot} \quad \text{ⓒ}}{t=t_0, P_1, \langle x'=f(x), t'=1\&t \le t_0 + t_1 \rangle \, (t > t_0 \land \neg P_2) \vdash \bot}}{\langle x'=f(x), t'=1\&t \le t_0 \land P_1 \rangle \, (t=t_0 \land P_1 \land \langle x'=f(x), t'=1\&t \le t_0 + t_1 \rangle \, (t > t_0 \land \neg P_2)) \vdash \bot}}{\Gamma_1, \langle x'=f(x), t'=1\&t \le t_0 \land P_1 \rangle \, (t=t_0 \land \langle x'=f(x), t'=1\&t \le t_0 + t_1 \rangle \, (t > t_0 \land \neg P_2)) \vdash \bot} \quad \text{ⓐ}}{\Gamma_1, \langle x'=f(x), t'=1\&t \le t_0 \rangle \, (t=t_0 \land \langle x'=f(x), t'=1\&t \le t_0 + t_1 \rangle \, (t > t_0 \land \neg P_2)) \vdash \bot}
$$

This completes the derivation of StepExt and thus also completing the proof of Theorem 5.7. □

The last part completes the proof of Example 5.10.

Proof of Example 5.10. Let $\varepsilon \in \mathbb{Q}^+$ be arbitrary, and assume without loss of generality that $\varepsilon < 1$. The main idea of the derivation is to iteratively apply axiom StepEx to obtain (shrinking) iterates of existence intervals using $R = \alpha|x_0|$ for some suitably chosen $\alpha \in \mathbb{Q}^+$, these existence intervals can be chained together using StepExt, giving the desired proof. First pick $\alpha \in \mathbb{Q}^+$ sufficiently small and $N \in \mathbb{N}$ sufficiently large such that the following hold

$$
\begin{aligned}
&-\tfrac{1}{\alpha+1} - \tfrac{1}{\alpha N+1} > 1 - \varepsilon \\
&-\tfrac{1}{\alpha+1} - \tfrac{1}{\alpha N+1} \ge \tfrac{1}{(\alpha+1)^3}.
\end{aligned}
$$

such choices are possible since $N \in \mathbb{N}$ is allowed to be arbitrarily large and dependent on α. The derivation will use N steps of StepEx to show that $x(t)$ is bounded in $B[x_0, \alpha N x_0]$ for $t \in [0, (1-\varepsilon)(\frac{1}{x_0} - \frac{1}{3x_0^3}))$ from which the desired claim concludes by axiom $\mathrm{StepDual}_{\rightarrow}$. Note that the bound $\max_{y \in B(x_0, n x_0)} |x^2 + 1| \le (n+1)^2 x_0^2 + 1$ holds for all $n \in \mathbb{N}$. The derivation first begins by handling the trivial case where $\frac{1}{x_0} - \frac{1}{3x_0^3} < 0$ holds.

$$\text{→R,cut,}\mathbb{R}\;\dfrac{\text{∨L}\;\dfrac{\text{⟨·⟩,¬R}\;\dfrac{\text{DX}\;\dfrac{\mathbb{R}\;\dfrac{*}{x = x_0, t = 0, x_0 > 0, \frac{1}{x_0} - \frac{1}{3x_0^3} < 0, t < (1-\varepsilon)\left(\frac{1}{x_0} - \frac{1}{3x_0^3}\right) \vdash \bot}}{x = x_0, t = 0, x_0 > 0, \frac{1}{x_0} - \frac{1}{3x_0^3} < 0, [x' = x^2 + 1, t' = 1]t < (1-\varepsilon)\left(\frac{1}{x_0} - \frac{1}{3x_0^3}\right) \vdash \bot}}{x = x_0, t = 0, x_0 > 0, \frac{1}{x_0} - \frac{1}{3x_0^3} < 0 \vdash \langle x' = x^2 + 1, t' = 1\rangle t \geq (1-\varepsilon)\left(\frac{1}{x_0} - \frac{1}{3x_0^3}\right)} \qquad ①}{x = x_0, t = 0, x_0 > 0, \frac{1}{x_0} - \frac{1}{3x_0^3} < 0 \lor \frac{1}{x_0} - \frac{1}{3x_0^3} \geq 0 \vdash \langle x' = x^2 + 1, t' = 1\rangle t \geq (1-\varepsilon)\left(\frac{1}{x_0} - \frac{1}{3x_0^3}\right)}}{\vdash x = x_0 \land t = 0 \land x_0 > 0 \rightarrow \langle x' = x^2 + 1, t' = 1\rangle t \geq (1-\varepsilon)\left(\frac{1}{x_0} - \frac{1}{3x_0^3}\right)}$$

The remaining premise ① represents the case where $\frac{1}{x_0} - \frac{1}{3x_0^3} \geq 0$

$$① \equiv x = x_0, t = 0, x_0 > 0, \frac{1}{x_0} - \frac{1}{3x_0^3} \geq 0 \vdash \langle x' = x^2 + 1, t' = 1\rangle t \geq (1-\varepsilon)\left(\frac{1}{x_0} - \frac{1}{3x_0^3}\right)$$

The derivation of ① begins with axiom StepDual$_{\rightarrow}$ and the bounded set $B[x_0, \alpha N x_0]$ (closed ball centered around x_0 with radius $\alpha N x_0$), followed by repeated applications of StepEx and StepExt. It uses the following constructs:

- Define the sequence $\{t_n\}_{0 \leq n \leq N}$ recursively with $t_0 = 0$, $t_n = t_{n-1} + \frac{\alpha x_0}{(\alpha n+1)^2 x_0^2 + 1}$.
- For each $0 \leq n \leq N$, define the ODEs
$$\gamma_n \equiv x' = x^2 + 1, t' = 1 \& t \leq t_n$$
$$\beta_n \equiv x' = x^2 + 1, t' = 1 \& x \in B[x_0, \alpha n x_0]$$
- For each $1 \leq n \leq N$, define the formula
$$\Gamma_n \equiv x_0 > 0 \land x \in B[x_0, \alpha n x_0] \land t = t_n$$
where $\alpha n x_0$ denotes standard multiplication. Note that crucially the upper bound N and the parameter α are constant, fixed values.

Note that formulas of the form

$$\varphi_n \equiv \Gamma_n \rightarrow [\gamma_{n+1}](x_0 > 0 \land x \in B[x_0, \alpha(n+1)x_0])$$

are valid and derivable from axiom StepEx for every $0 \leq n \leq N - 1$, the proof is as follows.

$$\text{→R,V}\;\dfrac{\text{cut,StepEx,dRW⟨·⟩}\;\dfrac{\text{StepDual}_{\leftarrow}\;\dfrac{\text{id}\;\dfrac{*}{[\gamma_{n+1}]x \in B[x_0, \alpha(n+1)x_0] \vdash [\gamma_{n+1}]x \in B[x_0, \alpha(n+1)x_0]}}{\langle \beta_{n+1}\rangle t \geq t_{n+1} \vdash [\gamma_{n+1}]x \in B[x_0, \alpha(n+1)x_0]} \qquad ②}{\Gamma_n \vdash [\gamma_{n+1}]x \in B[x_0, \alpha(n+1)x_0]}}{\vdash \Gamma_n \rightarrow [\gamma_{n+1}](x_0 > 0 \land x \in B[x_0, \alpha(n+1)x_0])}$$

Where the open premise ② arising from cut is

$$\vdash \forall x \in B[x_0, \alpha n x_0] \forall y \in B[x, \alpha x_0] \left\|y^2 + 1\right\| \leq (\alpha(n+1) + 1)^2 x_0^2 + 1$$

which is valid as $y^2 + 1$ is maximized when $|y|$ is maximized, therefore the maximum is attained when $y = x_0 + \alpha n x_0 + \alpha x_0 = (\alpha(n+1) + 1)x_0$ and the premise is proven by axiom $\mathbb{R}$. We can now derive the example.

$$\text{StepDual}_{\rightarrow}\,\dfrac{\text{dC,dW}\,\dfrac{\dfrac{\text{③}}{x = x_0, t = 0, x_0 > 0 \vdash [\gamma_N]x \in B[x_0, \alpha N x_0]} \qquad \mathbb{R}\,\dfrac{*}{t \le (1-\varepsilon)\left(\frac{1}{x_0} - \frac{1}{3x_0^3}\right) \vdash t \le t_N}}{x = x_0, t = 0, x_0 > 0 \vdash [x' = x^2 + 1, t' = 1 \& t \le (1-\varepsilon)\left(\frac{1}{x_0} - \frac{1}{3x_0^3}\right)]x \in B[x_0, \alpha N x_0]}}{x = x_0, t = 0, x_0 > 0, \frac{1}{x_0} - \frac{1}{3x_0^3} \ge 0 \vdash \langle x' = x^2 + 1, t' = 1\rangle t \ge (1-\varepsilon)\left(\frac{1}{x_0} - \frac{1}{3x_0^3}\right)}$$

The resolution of the right premise with axiom $\mathbb{R}$ requires justification, it is not trivial that the inequality $t_N \ge (1-\varepsilon)(\frac{1}{x_0} - \frac{1}{3x_0^3})$ holds. Lower-bounding t_N with the corresponding integral yields:

$$t_N = \sum_{n=1}^{N} \frac{\alpha x_0}{(\alpha n + 1)^2 x_0^2 + 1} \ge \int_1^N \frac{\alpha x_0}{(\alpha t + 1)^2 x_0^2 + 1} dt = \arctan((\alpha N + 1)x_0) - \arctan((\alpha + 1)x_0)$$

It is well-known that the bound

$$\frac{\pi}{2} - \frac{1}{x} \le \arctan(x) \le \frac{\pi}{2} - \frac{1}{x} + \frac{1}{3x^3}$$

holds for all $x > 0$ (can be derived from standard Taylor bounds of $\arctan(x)$ and the identity $\arctan(x) + \arctan(\frac{1}{x}) = \frac{\pi}{2}$). Utilizing this, we have

$$\begin{aligned}
t_N &\ge \arctan((\alpha N + 1)x_0) - \arctan((\alpha + 1)x_0) \\
&\ge \arctan((\alpha N + 1)x_0) - \frac{\pi}{2} + \frac{1}{(\alpha + 1)x_0} - \frac{1}{3(\alpha + 1)^3 x_0^3} \\
&\ge \frac{\pi}{2} - \frac{1}{(\alpha N + 1)x_0} - \frac{\pi}{2} + \frac{1}{(\alpha + 1)x_0} - \frac{1}{3(\alpha + 1)^3 x_0^3} \\
&= \frac{1}{x_0}\left(\frac{1}{\alpha + 1} - \frac{1}{\alpha N + 1}\right) - \frac{1}{3x_0^3}\left(\frac{1}{(\alpha + 1)^3}\right) \\
&\ge \left(\frac{1}{\alpha + 1} - \frac{1}{\alpha N + 1}\right)\left(\frac{1}{x_0} - \frac{1}{3x_0^3}\right)
\end{aligned}$$

where the final inequality follows from the assumption that $\frac{1}{\alpha+1} - \frac{1}{\alpha N+1} \ge \frac{1}{(\alpha+1)^3}$. Finally, since $\frac{1}{\alpha+1} - \frac{1}{\alpha N+1} \ge 1-\varepsilon$ by construction, the desired bound holds and the application of axiom $\mathbb{R}$ is justified. At last, the derivation of ③ can be completed by iteratively applying axioms StepEx,StepExt, note that by construction $t = t_n, x_0 > 0, x \in B[x_0, \alpha n x_0] \vdash \Gamma_n$ is always valid.

$$\text{cut,StepEx}\,\dfrac{\rightarrow\text{L}\,\dfrac{\text{StepExt,}\rightarrow\text{L}\,\dfrac{\text{StepExt,}\rightarrow\text{L}\,\dfrac{\dfrac{\text{StepExt,}\rightarrow\text{L}\,\dfrac{\text{id}\,\dfrac{*}{x_0 > 0, t=0, [\gamma_N]x \in B[x_0, \alpha N x_0] \vdash [\gamma_N]x \in B[x_0, \alpha N x_0]}}{\cdots}}{}}{x_0 > 0, t=0, [\gamma_2]x \in B[x_0, 2\alpha x_0] \vdash [\gamma_N]x \in B[x_0, \alpha N x_0]} \quad \mathbb{R}\,\dfrac{*}{t=t_1, x_0 > 0, x \in B[x_0, \alpha x_0] \vdash \Gamma_1} \quad \text{StepEx}\,\dfrac{*}{\varphi_1}}{x_0 > 0, t=0, [\gamma_1](x_0 > 0 \land x \in B[x_0, \alpha N x_0]) \vdash [\gamma_N]x \in B[x_0, \alpha N x_0]}}{x=x_0, t=0, x_0 > 0, \varphi_0 \vdash [\gamma_N]x \in B[x_0, \alpha N x_0]}}{x=x_0, t=0, x_0 > 0 \vdash [\gamma_N]x \in B[x_0, \alpha N x_0]}$$

Where the abbreviated derivation consists of N levels, at the n-th level $[\gamma_n]x \in B[x_0, \alpha n x_0]$ is proven via applications of StepEx,StepExt, this completes the derivation of the example. Note that when choosing the parameters α, N, all sufficiently small α and all sufficiently large N will suffice. As an example, suppose that the desired error threshold is $1 - 0.1 = 0.9$ with $\varepsilon = 0.1$, then $\alpha = 0.01$ and $N = 10^4$ works. □

Received 17 October 2024; revised 24 June 2025; accepted 17 August 2025