Deductive Stability Proofs for Ordinary Differential Equations

Yong Kiam Tan   André Platzer *

Abstract

Stability is required for real world controlled systems as it ensures that those systems can tolerate small, real world perturbations around their desired operating states. This paper shows how stability for continuous systems modeled by ordinary differential equations (ODEs) can be formally verified in differential dynamic logic (dL). The key insight is to specify ODE stability by suitably nesting the dynamic modalities of dL with first-order logic quantifiers. Elucidating the logical structure of stability properties in this way has three key benefits: *i)* it provides a flexible means of formally specifying various stability properties of interest, *ii)* it yields rigorous proofs of those stability properties from dL's axioms with dL's ODE safety and liveness proof principles, and *iii)* it enables formal analysis of the relationships between various stability properties which, in turn, inform proofs of those properties. These benefits are put into practice through an implementation of stability proofs for several examples in KeYmaera X, a hybrid systems theorem prover based on dL.

Keywords: differential equations, stability, differential dynamic logic

1 Introduction

The study of stability has its roots in efforts to understand mechanical systems, particularly those arising in celestial mechanics [Hir84, Lia07, Poi99]. Today, it is an important part of numerous applications in dynamical systems [Str15] and control theory [HC08, Kha92]. This paper studies proofs of stability for continuous dynamical systems described by *ordinary differential equations* (ODEs), such as those used to model feedback control systems [HC08, Kha92]. For such systems, ODE stability is a key correctness requirement [Alu15] that deserves fully rigorous proofs *alongside* other key properties such as safety and liveness of those ODEs [PT20, TPar]. Despite this, formal stability verification has received less attention compared to proofs of safety and liveness, e.g., through reachability or deductive techniques [DFPP18].

Stability for a continuous system (or ODEs) requires that *i)* its system state always stays close to some desired operating state(s) when initially slightly perturbed from those operating state(s), and *ii)* those perturbations are eventually dissipated so the system returns to a desired operating state. These properties are especially crucial for engineered systems because they must be robust to real world perturbations deviating from idealized system models. Simple pendulums provide canonical examples of stability phenomena: they are always observed to settle in the rest position of Fig. 1 (bottom) after some time regardless of how they are initially released. In contrast, the inverted pendulum in Fig. 1 (top) is *theoretically* also at a resting position but can only be observed transiently in practice because the slightest real world perturbation will cause the pendulum
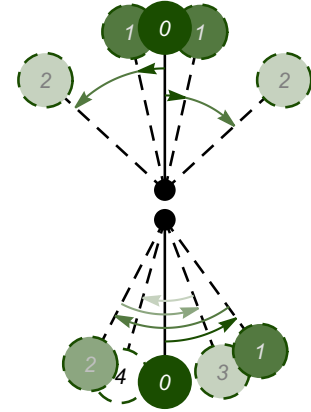

Figure 1: A pendulum (in green) hung by a rigid rod from a pivot (in black) perturbed from its resting state (bottom) and from its inverted, upright position (top). Perturbed states (with dashed boundaries) are faded out to show the progression of time.

to fall due to gravity. Stability explains these observations—the resting position is (asymptotically) stable while the inverted position is unstable and requires active control to ensure its stability. Proofs of safety and liveness properties are still required for the inverted pendulum under control, e.g., its controller must never generate unsafe amounts of

---

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

torque and the pendulum must eventually reach the inverted position. The *triumvirate* of safety, liveness, and stability is required for holistic correctness of the inverted pendulum controller.

The classical way of distinguishing the aforementioned stability situations is by designing a *Lyapunov function* [Lia07], i.e., an energy-like auxiliary measure satisfying certain *arithmetical conditions* [HC08, Kha92, RHL77] which implies that the auxiliary energy decreases along system trajectories towards local minima at the stable resting state(s), see Fig. 2. Prior approaches [APA20, GKD+19, KDSA14, LZZ12, SCÁ13] have emphasized the need to formally verify those arithmetical conditions in order to guarantee that a conjectured Lyapunov function correctly implies stability for a given system.

Figure 2: A Lyapunov function that decreases along the pendulum trajectory shown in Fig. 1 (bottom).

This paper shows how deductive proofs of ODE stability can be carried out in differential dynamic logic (dL) [Pla12, Pla17, Pla18], a logic for *deductive verification* of hybrid systems.[1] The key insight is that stability properties can be specified by suitably nesting the dynamic modalities of dL with quantifiers of first-order logic. The resulting specifications are amenable to rigorous proof by combining dL's ODE safety [PT20] and liveness [TPar] proof principles with real arithmetic and first-order quantifier reasoning. This makes it possible to *syntactically derive* stability for a given system from the small set of dL axioms which, in turn, enables trustworthy stability proofs in the KeYmaera X theorem prover for hybrid systems [FMQ+15, Pla17]. Notably, this approach directly verifies *stability specifications*, which goes beyond verifying arithmetic that imply those specifications [APA20, GKD+19, KDSA14, LZZ12, SCÁ13]. This is crucial for advanced stability notions because those variations generally require subtle twists to the required arithmetical conditions on their Lyapunov functions [HC08]; proofs of stability specifications alleviate the onus on system designers to correctly pick and check the appropriate conditions for their applications. Section 3 shows how various stability properties for ODE equilibria can be formally specified and proved in dL with Lyapunov function techniques. Section 4 generalizes those stability specifications, yielding unambiguous formal specifications of advanced stability properties from the literature [HC08, Kha92], along with their derived proof rules. These specifications also provide rigorous insights into the logical relationship between various stability notions, which are used to inform their respective proofs. Section 5 illustrates the practicality of this paper's dL approach through several stability case studies formalized in KeYmaera X.

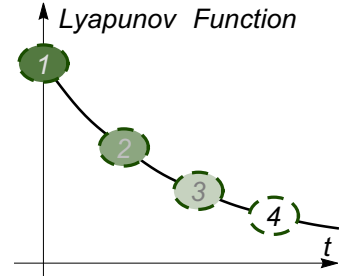All omitted definitions and proofs are available in Appendices A–C.

2   Background: Differential Dynamic Logic

This section briefly recalls the syntax and semantics of dL, focusing on its continuous fragment which has a complete axiomatization for ODE invariants [PT20]. Full presentations of dL, including its discrete fragment, are available elsewhere [Pla17, Pla18].

Syntax and Semantics.   The grammar of dL terms is as follows, where $x \in \mathcal{V}$ is a variable and $c \in \mathbb{Q}$ is a rational constant. These terms are polynomials over $\mathcal{V}$ (extensions with Noetherian functions [PT20] such as $\exp, \sin, \cos$ are possible):

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

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

$$\phi, \psi ::= p \sim q \mid \phi \wedge \psi \mid \phi \vee \psi \mid \neg \phi \mid \forall v\, \phi \mid \exists v\, \phi \mid [\alpha]\phi \mid \langle \alpha \rangle \phi$$

This grammar features atomic comparisons ($p \sim q$), propositional connectives ($\neg$, $\wedge$, $\vee$), first-order quantifiers over the reals ($\forall$, $\exists$), and the box ($[\alpha]\phi$) and diamond ($\langle \alpha \rangle \phi$) modality formulas which express that all or some runs of hybrid program α satisfy ϕ, respectively. The modalities $[\cdot], \langle \cdot \rangle$ can be freely nested with first-order and modal

---

[1]Hybrid systems are mathematical models describing discrete and continuous dynamics, and interactions thereof. This paper's formal understanding of ODE stability is crucial for subsequent investigation of hybrid systems stability [Bra05, GST12, Lib03].

connectives, which is crucial for the specification of stability properties in Sections 3 and 4. Formulas not containing the modalities are formulas of first-order real arithmetic and are written as P, Q, R.

This paper focuses on the *continuous* fragment of hybrid programs $\alpha \equiv x' = f(x) \,\&\, Q$, where $x' = f(x)$ is an n-dimensional system of ordinary differential equations (ODEs), $x'_1 = f_1(x), \ldots, x'_n = f_n(x)$, over variables $x = (x_1, \ldots, x_n)$, the LHS x'_i is the time derivative of x_i and the RHS $f_i(x)$ is a polynomial over variables x. The evolution domain constraint Q specifies the set of states in which the ODE is allowed to evolve continuously. When Q is the formula *true*, the ODE is also written as $x' = f(x)$. For n-dimensional vectors x, y, the dot product is $x \cdot y \stackrel{\text{def}}{=} \sum_{i=1}^n x_i y_i$ and $\|x\|^2 \stackrel{\text{def}}{=} \sum_{i=1}^n x_i^2$ denotes the squared Euclidean norm. Variables $z \in \mathcal{V} \setminus \{x\}$ not occurring on the LHS of ODE $x' = f(x)$ are *parameters* that remain constant along ODE solutions. The following parametric ODE model of a simple pendulum is used as a running example.

Example 1 (Pendulum model). The ODE $\alpha_p \equiv \theta' = \omega$, $\omega' = -\frac{g}{L}\sin(\theta) - b\omega$ models a pendulum (illustrated below) suspended from a pivot by a rod of length L, where θ is the angle of displacement, ω is the angular velocity of the pendulum, and $g > 0$ is the gravitational constant. Parameter $a = \frac{g}{L}$ is a positive scaling constant and parameter $b \geq 0$ is the coefficient of friction for angular velocity.

The symbolic parameters a, b make analysis of α_p apply to a range of concrete values, e.g., pendulums that are suspended by a long rod (with large L) are modeled by small positive values of a, while frictionless pendulums have $b = 0$. A simplification of α_p is used because stability analyses often concern the behavior of the pendulum near its resting (or inverted) state where $\theta = 0$. For such nearby states with $\theta \approx 0$, the small angle approximation $\sin(\theta) \approx \theta$ yields a linear ODE:[2]

$$\alpha_l \equiv \theta' = \omega, \ \omega' = -a\theta - b\omega \tag{1}$$

An *inverted* pendulum is modeled by a similar ODE (illustrated on the right) under a change of coordinates. Such a pendulum requires an external torque input $u(\theta, \omega)$ to maintain its stability; $u(\theta, \omega)$ is determined and proved correct in Section 5.

$$\alpha_i \equiv \theta' = \omega, \ \omega' = a\theta - b\omega - u(\theta, \omega) \tag{2}$$
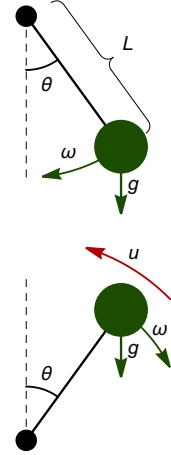
States $\nu : \mathcal{V} \to \mathbb{R}$ assign real values to each variable in $\mathcal{V}$; the set of all states is $\mathbb{S}$. The semantics of dL formula ϕ is the set of states $[\![\phi]\!] \subseteq \mathbb{S}$ in which ϕ is true [Pla17, Pla18], where the semantics of first-order logical connectives are defined as usual, e.g., $[\![\phi \wedge \psi]\!] = [\![\phi]\!] \cap [\![\psi]\!]$. For ODEs, the semantics of the modal operators is as follows.[3] Let $\nu \in \mathbb{S}$ and $\boldsymbol{\varphi} : [0, T) \to \mathbb{S}$ for some $0 < T \leq \infty$, be the unique, right-maximal solution [Chi06] to ODE $x' = f(x)$ with initial value $\boldsymbol{\varphi}(0) = \nu$:

$\nu \in [\![[x' = f(x) \,\&\, Q]\phi]\!]$ iff for all $0 \leq \tau < T$ where $\boldsymbol{\varphi}(\zeta) \in [\![Q]\!]$ for all $0 \leq \zeta \leq \tau$: $\boldsymbol{\varphi}(\tau) \in [\![\phi]\!]$

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

For a formula P the ε-neighborhood of P with respect to x is defined as $\mathcal{U}_\varepsilon(P) \stackrel{\text{def}}{=} \exists y \left(\|x - y\|^2 < \varepsilon^2 \wedge P(y) \right)$, where the existentially quantified variables y are fresh in P. The neighborhood formula $\mathcal{U}_\varepsilon(P)$ characterizes the set of states within distance ε from P, with respect to the dynamically evolving variables x. This is useful for syntactically expressing small ε perturbations in the stability definitions of Sections 3 and 4. For formulas P of first-order real arithmetic, the ε-neighborhood, $\mathcal{U}_\varepsilon(P)$, can be equivalently expressed in quantifier-free form by quantifier elimination [BCR98]. For example, $\mathcal{U}_\varepsilon(x = 0)$ is equivalent to the formula $\|x\|^2 < \varepsilon^2$. Formulas $\overline{P}$ and ∂P are the syntactically definable topological closure and boundary of the set characterized by P, respectively [BCR98].

Proof Calculus. All derivations and proof rules are presented in a classical sequent calculus. The semantics of *sequent* $\Gamma \vdash \phi$ is equivalent to the formula $\left(\bigwedge_{\psi \in \Gamma} \psi \right) \to \phi$. A sequent is valid iff its corresponding formula is valid.

---

[2]This linearization is justified by the Hartman-Grobman theorem [Chi06]. A nonlinear polynomial approximation, such as $\sin(\theta) \approx \theta - \frac{\theta^3}{6}$, can also be used.

[3]The semantics of dL formulas is defined compositionally elsewhere [Pla17, Pla18].

Completed branches in a sequent proof are marked with $*$. Assumptions $\psi \in \Gamma$ that have only ODE parameters as free variables remain true along ODE evolutions and are soundly kept across ODE deduction steps [Pla17, Pla18]. First-order real arithmetic is decidable [BCR98] so we assume such a decision procedure and label proof steps with $\mathbb{R}$ when they follow from real arithmetic. Axioms and proof rules are *derivable* iff they can be deduced from sound dL axioms and proof rules [Pla17, Pla18].

Formula I is an *invariant* of the ODE $x' = f(x) \,\&\, Q$ iff the formula $I \rightarrow [x' = f(x) \,\&\, Q]I$ is valid. The dL proof calculus is *complete* for ODE invariants [PT20], i.e., any true ODE invariant expressible in first-order real arithmetic can be proved in the calculus. The calculus also supports refinement reasoning [TPar] for proving ODE liveness properties $P \rightarrow \langle x' = f(x) \,\&\, Q \rangle R$, which says that the goal R is reached along the ODE $x' = f(x) \,\&\, Q$ from precondition P.

An important syntactic tool for reasoning with ODE $x' = f(x)$ is the *Lie derivative* of term p defined as $\dot{p} \stackrel{\text{def}}{=} \sum_{x_i \in x} \frac{\partial p}{\partial x_i} f_i(x)$, whose semantic value is equal to the time derivative of the value of p along solutions φ of the ODE [Pla17, PT20]. They are provably definable in dL using syntactic differentials [Pla17].

3 Asymptotic Stability of an Equilibrium Point

This section presents Lyapunov's classical notion of asymptotic stability [Lia07] and its formal specification in dL. This formalization enables the derivation of dL stability proof rules with *Lyapunov functions* [HC08, Kha92, Lia07, RHL77]. Several related stability concepts are formalized in dL, along with their relationships and rules.

3.1 Mathematical Preliminaries

An *equilibrium point* of ODE $x' = f(x)$ is a point $x_0 \in \mathbb{R}^n$ where $f(x_0) = 0$, so a system that starts at x_0 stays at x_0 along its continuous evolution. Such points are often interesting in real-world systems, e.g., the equilibrium point $\theta = 0, \omega = 0$ for α_l from (1) is the resting state of a pendulum. For a controlled system, equilibrium points often correspond to desired steady system states where no further continuous control input (modeled as part of $f(x)$) is required [Kha92].

For brevity, assume the origin $0 \in \mathbb{R}^n$ is an equilibrium point of interest. Any other equilibrium point(s) of interest $x_0 \in \mathbb{R}^n$ can be translated to the origin with the change of coordinates $x \mapsto x - x_0$ for the ODE, see Lemma 24.

The following definition of asymptotic stability is standard [HC08, Kha92, RHL77].[4]

Definition 2 (Asymptotic stability [HC08, Kha92, RHL77]). *The origin $0 \in \mathbb{R}^n$ of ODE $x' = f(x)$ is*

- ***stable** if, for all $\varepsilon > 0$, there exists $\delta > 0$ such that for all initial states $x = x(0)$ with $\|x\| < \delta$, the right-maximal ODE solution $x(t) : [0, T) \rightarrow \mathbb{R}^n$ satisfies $\|x(t)\| < \varepsilon$ for all times $0 \leq t < T$,*

- ***attractive** if there exists $\delta > 0$ such that for all $x = x(0)$ with $\|x\| < \delta$, the right-maximal ODE solution $x(t) : [0, T) \rightarrow \mathbb{R}^n$ satisfies $\lim_{t \to T} x(t) = 0$,*

- ***asymptotically stable** if it is stable and attractive.*

These definitions can be understood using the resting state of the pendulum from Fig. 1 (bottom) which is asymptotically stable. When the pendulum is given a light push from its bottom resting state (formally, $\|x\| < \delta$), it gently oscillates near that resting state (formally, $\|x(t)\| < \varepsilon$). In the presence of friction, these oscillations eventually dissipate so the pendulum asymptotically returns to its resting state (formally, $\lim_{t \to T} x(t) = 0$). This behavior is *local*, i.e., for any given $\varepsilon > 0$, there *exists* a sufficiently small $\delta > 0$ perturbation of the initial state that results in gentle oscillations with $\|x(t)\| < \varepsilon$, see Fig. 3 (left). A strong push, e.g., with $\delta > \varepsilon$, could instead cause the pendulum to spin around on its pivot.

Remark 3. Stability and attractivity *do not* imply each other [RHL77, Chapter I.2.7]. However, if the origin is stable, attractivity can be defined in a simpler way. This is proved in dL, after characterizing stability and attractivity syntactically.

---

[4]Some definitions require, or implicitly assume, right-maximal solutions $x(t)$ to be global, i.e., with $T = \infty$, see [Kha92, Definition 4.1] and associated discussion. The definitions presented here are better suited for subsequent generalizations.
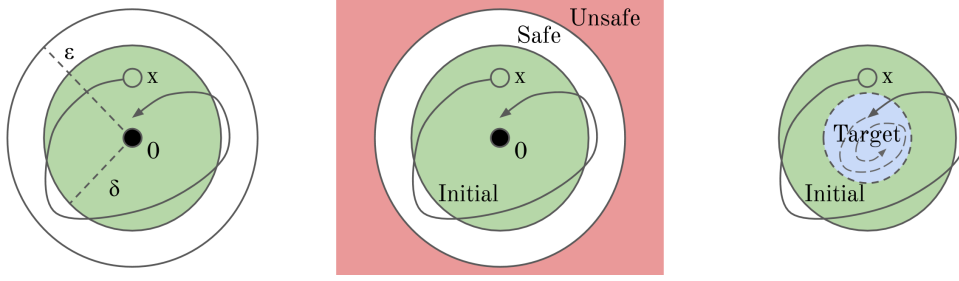
Figure 3: Solutions from points in the δ ball around the origin, like the green initial point x, remain within the ε ball around the origin $0 \in \mathbb{R}^n$ (black dot) and asymptotically approach the origin. The latter two plots illustrate how asymptotic stability for an ODE can be broken down into a pair of (quantified) ODE safety and liveness properties.

3.2 Formal Specification

The formal specification of asymptotic stability in dL combines *i)* the dynamic modalities of dL, which are used to quantify over the dynamics of the ODE, and *ii)* the first-order logic quantifiers, which are used to express combinations of (topologically) local and asymptotic properties of those dynamics.

Lemma 4 (Asymptotic stability in dL). *The origin of ODE $x' = f(x)$ is, respectively, i) **stable**, ii) **attractive**, and iii) **asymptotically stable** iff the dL formulas i) $\mathrm{Stab}(x' = f(x))$, ii) $\mathrm{Attr}(x' = f(x))$, and iii) $\mathrm{AStab}(x' = f(x))$ respectively are valid. Variables ε, δ are fresh, i.e., not in $x, f(x)$.*

$$\mathrm{Stab}(x' = f(x)) \equiv \forall \varepsilon{>}0 \, \exists \delta{>}0 \, \forall x \, \big(\mathcal{U}_\delta(x=0) \to [x' = f(x)] \mathcal{U}_\varepsilon(x=0) \big)$$
$$\mathrm{Attr}(x' = f(x)) \equiv \exists \delta{>}0 \, \forall x \, \big(\mathcal{U}_\delta(x=0) \to \mathrm{Asym}(x' = f(x), x=0) \big)$$
$$\mathrm{AStab}(x' = f(x)) \equiv \mathrm{Stab}(x' = f(x)) \wedge \mathrm{Attr}(x' = f(x))$$

Formula $\mathrm{Asym}(x' = f(x), P) \equiv \forall \varepsilon{>}0 \, \langle x' = f(x) \rangle [x' = f(x)] \mathcal{U}_\varepsilon(P)$ characterizes the set of states that asymptotically approach P along ODE solutions.

Formula $\mathrm{Stab}(x' = f(x))$ is a syntactic dL rendering of the corresponding quantifiers from Def. 2. The safety property $\mathcal{U}_\delta(x=0) \to [x' = f(x)] \mathcal{U}_\varepsilon(x=0)$ expresses that solutions starting from the δ-neighborhood of the origin always (for all times) stay safely in the ε-neighborhood, as visualized in Fig. 3 (middle).

Formula $\mathrm{Attr}(x' = f(x))$ uses the subformula $\mathrm{Asym}(x' = f(x), x = 0)$ which characterizes the limit in Def. 2. Recall $\lim_{t \to T} x(t) = 0$ iff for all $\varepsilon > 0$ there exists a time τ with $0 \le \tau < T$ such that for all times t with $\tau \le t < T$, the solution satisfies $\|x(t)\| < \varepsilon$, i.e., the limit requires for all distances $\varepsilon > 0$, the ODE solution will *eventually always* be within distance ε of the origin, as visualized in Fig. 3 (right). This limit is characterized using nested $\langle \cdot \rangle [\cdot]$ modalities, together with first-order quantification according to Def. 2. More generally, formula $\mathrm{Asym}(x' = f(x), P)$ characterizes the set of initial states where the right-maximal ODE solution asymptotically approaches P; this set is known as the *region of attraction* of P [Kha92]. Thus, attractivity requires that the region of attraction of the origin contains an open neighborhood $\mathcal{U}_\delta(x=0)$ of the origin.

From Lemma 4, proving validity of the formula $\mathrm{AStab}(x' = f(x))$ yields a rigorous proof of asymptotic stability for $x' = f(x)$. However, if the origin is stable, then attractivity can be provably simplified with the following corollary.

Corollary 5 (Stable attractivity). *The following axiom is derivable in dL.*
SAttr $\mathrm{Stab}(x' = f(x)) \to \big(\mathrm{Asym}(x' = f(x), x{=}0) \leftrightarrow \forall \varepsilon{>}0 \, \langle x' = f(x) \rangle \mathcal{U}_\varepsilon(x{=}0) \big)$

Corollary 5 simplifies the syntactic characterization of the region of attraction for stable equilibria from a nested $\langle \cdot \rangle [\cdot]$ formula to a $\langle \cdot \rangle$ formula, which is then directly amenable to ODE liveness reasoning [TPar]. This corollary is used to simplify proofs of asymptotic stability, as explained next.

3.3 Lyapunov Functions

Lyapunov functions are the standard tool for showing stability of general, non-linear ODEs [HC08, Kha92, RHL77] and finding suitable Lyapunov functions is an important problem in its own right [APA20, For91, GKD$^+$19, KDSA14, LZZ12, PP02, Par00, SCÁ13, TPS08]. This section shows how a candidate Lyapunov function, once found, can be used to rigorously prove stability. The following proof rules derive Lyapunov stability arguments [HC08, Kha92, RHL77] syntactically in dL.

Lemma 6 (Lyapunov functions). *The following Lyapunov function proof rules are derivable in* dL.

$$\text{Lyap}_\geq \quad \frac{\vdash f(0) = 0 \wedge v(0) = 0 \quad \vdash \exists \gamma{>}0\, \forall x \left(0{<}\|x\|^2{\leq}\gamma^2 \to v > 0 \wedge \dot{v} \leq \mathbf{0}\right)}{\vdash \text{Stab}(x' = f(x))}$$

$$\text{Lyap}_> \quad \frac{\vdash f(0) = 0 \wedge v(0) = 0 \quad \vdash \exists \gamma{>}0\, \forall x \left(0{<}\|x\|^2{\leq}\gamma^2 \to v > 0 \wedge \dot{v} < \mathbf{0}\right)}{\vdash \text{AStab}(x' = f(x))}$$

Rules Lyap$_\geq$, Lyap$_>$ use the Lyapunov function v as an auxiliary, energy-like function near the origin which is positive and has non-positive (resp. negative Lyap$_>$) derivative $\dot{v}$. This guarantees that v is non-increasing (resp. decreasing) along ODE solutions near the origin, see Fig. 2. The right premise of both rules use $\exists \gamma{>}0\, \forall x \left(0{<}\|x\|^2{\leq}\gamma^2 \to \cdots\right)$ to require that the Lyapunov function conditions are true in a γ-neighborhood of the origin. The subtle difference in sign condition for $\dot{v}$ between rules Lyap$_\geq$, Lyap$_>$ is illustrated for the pendulum.

Example 7 (Pendulum asymptotic stability). For ODE α_l from (1), a suitable Lyapunov function for proving its stability [Kha92] is $v = a\frac{\theta^2}{2} + \frac{(b\theta+\omega)^2+\omega^2}{4}$, where the Lie derivative of v along α_l is $\dot{v} = -\frac{b}{2}(a\theta^2 + \omega^2)$. Stability[5] is formally proved in dL for *any* parameter values $a > 0, b \geq 0$ using rule Lyap$_\geq$ because both of its resulting arithmetical premises are provable by $\mathbb{R}$. The full dL derivation, also used in KeYmaera X (Section 5), is shown in the proof of Lemma 6 (Appendix B).

When $b > 0$, i.e., friction is non-negligible, an identical derivation with Lyap$_>$ instead of Lyap$_\geq$ proves asymptotic stability because $-\frac{b}{2}(a\theta^2 + \omega^2)$ is negative except at the origin. Indeed, displacements to the pendulum's resting state can only be dissipated in the presence of friction, not when $b = 0$.

3.4 Asymptotic Stability Variations

Asymptotic stability is a strong guarantee about the local behavior of ODE solutions near equilibrium points of interest. In certain applications, stronger stability guarantees may be needed for those equilibria [Kha92]. This section examines two standard stability variations, shows how they can be proved in dL, and formally analyzes their logical relationship with asymptotic stability.

Exponential Stability. As the name suggests, the first stability variation, exponential stability, guarantees an exponential rate of convergence towards the equilibrium point from an initial displacement. This is useful, e.g., for bounding the time spent by a perturbed system far away from its desired operating state.

Definition 8 (Exponential stability [HC08, Kha92, RHL77]). *The origin* $0 \in \mathbb{R}^n$ *of ODE* $x' = f(x)$ *is **exponentially stable** if there are positive constants* $\alpha, \beta, \delta > 0$ *such that for all initial states* $x = x(0)$ *with* $\|x\| < \delta$*, the right-maximal ODE solution* $x(t) : [0, T) \to \mathbb{R}^n$ *satisfies* $\|x(t)\| \leq \alpha\|x(0)\| \exp(-\beta t)$ *for all times* $0 \leq t < T$.

Exponential stability bounds the norm of solutions to ODE $x' = f(x)$ near the origin by a decaying exponential. It is specified in dL as follows.

Lemma 9 (Exponential stability in dL). *The origin of ODE* $x' = f(x)$ *is **exponentially stable** iff the following* dL *formula is valid. Variables* α, β, δ, y *are fresh, i.e., not in* $x, f(x)$.

$$\text{EStab}(x' = f(x)) \equiv \exists \alpha{>}0\, \exists \beta{>}0\, \exists \delta{>}0\, \forall x \left(\mathcal{U}_\delta(x = 0) \to [y := \alpha^2\|x\|^2; x' = f(x), y' = -2\beta y]\, \|x\|^2 \leq y\right)$$

---

[5]For the trigonometric pendulum ODE α_p from Example 1, the Lyapunov function $v = a(1 - \cos(\theta)) + \frac{(b\theta+\omega)^2+\omega^2}{4}$ with Lie derivative $\dot{v} = -\frac{b}{2}(a\theta\sin(\theta) + \omega^2)$ proves its stability [Kha92] but requires arithmetic reasoning over trigonometric functions.

The discrete assignment $y := \alpha^2 \|x\|^2$ sets the value of variable y to that of $\alpha^2 \|x\|^2$ and ; denotes sequential composition of hybrid programs [Pla17, Pla18].

Formula $\mathrm{EStab}(x' = f(x))$ uses a fresh variable y with ODE $y' = -2\beta y$ and initialized to $\alpha^2 \|x\|^2$ so that y *differentially axiomatizes* [PT20] the (squared) decaying exponential function $\alpha^2 \|x(0)\|^2 \exp(-2\beta t)$ along ODE solutions. Such an implicit (polynomial) characterization of exponential decay allows syntactic proof steps to use decidable real arithmetic reasoning.

Lemma 10 (Lyapunov function for exponential stability). *The following Lyapunov function proof rule for exponential stability is derivable in* dL, *where $k_1, k_2, k_3 \in \mathbb{Q}$ are positive constants.*

$$\mathrm{Lyap}_{\mathrm{E}} \quad \frac{\vdash \exists \gamma {>} 0 \, \forall x \left(\|x\|^2 {\leq} \gamma^2 \to k_1^2 \|x\|^2 \leq v \leq k_2^2 \|x\|^2 \wedge \dot{v} \leq -2k_3 v \right)}{\vdash \mathrm{EStab}(x' = f(x))}$$

Rule $\mathrm{Lyap}_{\mathrm{E}}$ enables proofs of exponential stability in dL. In fact, the proof of Lemma 10 (Appendix B) yields *quantitative* bounds, where $\mathrm{EStab}(x' = f(x))$ is explicitly witnessed with scaling constant $\alpha = \frac{k_2}{k_1}$ and decay rate $\beta = k_3$. These can be used to calculate time bounds when the system state will return sufficiently close to the origin. Similarly, the disturbance δ in $\mathrm{EStab}(x' = f(x))$ is quantitatively witnessed by $\frac{k_1}{k_2}\gamma$ for any γ witnessing validity of the premise of rule $\mathrm{Lyap}_{\mathrm{E}}$. This yields a provable estimate of the region around the origin where exponential stability holds; this latter estimate is explored next.

Region of Attraction. Formulas $\mathrm{Attr}(x' = f(x))$ and $\mathrm{EStab}(x' = f(x))$ both feature a subformula of the form $\exists \delta > 0 \, \forall x \, (\mathcal{U}_\delta(x = 0) \to \cdots)$ which expresses that attractivity (or exponential stability) is locally true in *some* δ neighborhood of the origin. In many applications, it is useful to find and rigorously prove that a given set is attractive or exponentially stable with respect to the origin [Kha92, Chapter 8.2]. The second stability variation yields *provable* subsets of the region of attraction, including the special case where it is the entire state space. This is formalized using the following variants of $\mathrm{Attr}(x' = f(x))$ and $\mathrm{EStab}(x' = f(x))$ within a region given by a formula P.

$$\mathrm{Attr}^{\mathrm{P}}(x' = f(x), P) \equiv \forall x \left(P \to \mathrm{Asym}(x' = f(x), x = 0) \right)$$

$$\mathrm{EStab}^{\mathrm{P}}(x' = f(x), P) \equiv \exists \alpha {>} 0 \, \exists \beta {>} 0 \, \forall x \left(P \to [y := \alpha^2 \|x\|^2; x' = f(x), y' = -2\beta y] \, \|x\|^2 \leq y \right)$$

The formula $\mathrm{Attr}^{\mathrm{P}}(x' = f(x), P)$ is valid iff the set characterized by P is a subset of the origin's region of attraction [Kha92]. For example, $\mathrm{Attr}(x' = f(x))$ is $\exists \delta > 0 \, \mathrm{Attr}^{\mathrm{P}}(x' = f(x), \mathcal{U}_\delta(x = 0))$. This generalization is useful for formalizing stronger notions of stability in dL, such as the following *global* stability notions [HC08, Kha92]. For brevity, dL specifications of the stability properties (in **bold**) are given below with mathematical definitions deferred to Appendix B.

Lemma 11 (Global stability in dL). *The origin of ODE $x' = f(x)$ is **globally asymptotically stable** iff the dL formula* $\mathrm{Stab}(x' = f(x)) \wedge \mathrm{Attr}^{\mathrm{P}}(x' = f(x), \mathit{true})$ *is valid. The origin is **globally exponentially stable** iff the dL formula* $\mathrm{EStab}^{\mathrm{P}}(x' = f(x), \mathit{true})$ *is valid.*

Global stability ensures that *all* perturbations to the system state are eventually dissipated. Their proof rules are similar to $\mathrm{Lyap}_>$ and $\mathrm{Lyap}_{\mathrm{E}}$ respectively.

Lemma 12 (Lyapunov function for global stability). *The following Lyapunov function proof rules for global asymptotic and exponential stability are derivable in* dL. *In rule Lyap_E^G, $k_1, k_2, k_3 \in \mathbb{Q}$ are positive constants.*

$$\mathrm{Lyap}_>^{\mathrm{G}} \quad \frac{\vdash f(0){=}0 \wedge v(0){=}0 \quad x{\neq}0 \vdash v{>}0 \wedge \dot{v}{<}0 \quad \vdash \forall b \, \exists \gamma {>} 0 \, \forall x \left(v {\leq} b {\to} \mathcal{U}_\gamma(x {=} 0) \right)}{\vdash \mathrm{Stab}(x' = f(x)) \wedge \mathrm{Attr}^{\mathrm{P}}(x' = f(x), \mathit{true})}$$

$$\mathrm{Lyap}_{\mathrm{E}}^{\mathrm{G}} \quad \frac{\vdash k_1^2 \|x\|^2 \leq v \leq k_2^2 \|x\|^2 \wedge \dot{v} \leq -2k_3 v}{\vdash \mathrm{EStab}^{\mathrm{P}}(x' = f(x), \mathit{true})}$$

Example 13 (Pendulum global exponential stability). For simplicity, instantiate Example 7 with parameters $a = 1, b = 1$. The Lyapunov function then simplifies to $v = \frac{\theta^2}{2} + \frac{(\theta + \omega)^2 + \omega^2}{4}$ with Lie derivative $\dot{v} = -\frac{(\theta^2 + \omega^2)}{2}$, which satisfies the real arithmetic inequalities $\frac{\theta^2 + \omega^2}{4} \leq v \leq \theta^2 + \omega^2$ and $\dot{v} \leq -\frac{1}{2}v$. Thus, rule $\mathrm{Lyap}_{\mathrm{E}}^{\mathrm{G}}$ proves global exponential stability of α_l with $k_1 = \frac{1}{2}$, $k_2 = 1$, and $k_3 = \frac{1}{4}$. An important caveat is that Example 7 used a local small angle approximation, so this global phenomenon does *not* hold for a real world pendulum (nor for α_p).

Logical Relationships. With the proliferation of stability variations just introduced, it is useful to take stock of their logical relationships. An important example of such a relationship is shown in the following corollary.

Corollary 14 (Exponential stability implies asymptotic stability). *The following axioms are derivable in* dL.
EStabStab $\mathrm{EStab}(x' = f(x)) \to \mathrm{Stab}(x' = f(x))$

EStabAttr $\mathrm{EStab}^{\mathrm{P}}(x' = f(x), P) \to \mathrm{Attr}^{\mathrm{P}}(x' = f(x), P)$

Derived axioms EStabStab, EStabAttr show that exponential stability implies asymptotic stability. In proofs, axiom EStabAttr allows the region of attraction to be estimated by the region where solutions are exponentially bounded.

4 General Stability

This section provides stability definitions and proof rules that generalize stability for an equilibrium point from Section 3 to the stability of sets. These definitions are useful when the desired stable system state(s) is not modeled by a single equilibrium point, but may instead, e.g., lie on a periodic trajectory [Kha92], a hyperplane, or a continuum of equilibrium points within the state space [HC08]. The generalized definition is used to formalize two stability notions from the literature [HC08, Kha92], and to justify their Lyapunov function proof rules.

4.1 General Stability and General Attractivity

The following *general stability* formula defines stability in dL with respect to an ODE $x' = f(x)$ and formulas P, R. The quantified variables ε, δ are assumed to be fresh by bound renaming, i.e., do not appear in $x, f(x), P$ or R.

$$\mathrm{Stab}_{\mathrm{R}}^{\mathrm{P}}(x' = f(x), P, R) \equiv \forall \varepsilon{>}0 \,\exists \delta{>}0 \,\forall x \left(\mathcal{U}_{\delta}(P) \to [x' = f(x)]\, \mathcal{U}_{\varepsilon}(R) \right)$$

This formula generalizes stability of the origin $\mathrm{Stab}(x' = f(x))$ by adding two logical tuning knobs that can be intuitively understood as follows. The *precondition* P characterizes the initial states from which the system state is expected to be disturbed by some disturbance δ. The *postcondition* R characterizes the set of desired operating states that the system must remain close (within the ε neighborhood of R) after being disturbed from its initial states.

The *general attractivity* formula similarly generalizes $\mathrm{Attr}^{\mathrm{P}}(x' = f(x), P)$ with a postcondition R towards which the ODE solutions from initial states satisfying precondition P are asymptotically attracted.

$$\mathrm{Attr}_{\mathrm{R}}^{\mathrm{P}}(x' = f(x), P, R) \equiv \forall x \left(P \to \mathrm{Asym}(x' = f(x), R) \right)$$

Lemma 15 (General Lyapunov functions). *The following Lyapunov function proof rule for general stability with two stacked premises is derivable in* dL.

$$\mathrm{GLyap} \quad \frac{\begin{array}{l} \vdash P \to R \\[4pt] \vdash \forall \varepsilon{>}0 \,\exists 0{<}\gamma{\le}\varepsilon \,\exists k \left(\begin{array}{l} \forall x \left(\partial(\mathcal{U}_{\gamma}(R)) \to v \ge k \right) \wedge \\ \exists 0{<}\delta{\le}\gamma \,\forall x \left(\mathcal{U}_{\delta}(P) \to R \vee v{<}k \right) \wedge \\ \forall x \left(R \vee v{<}k \to [x' = f(x) \,\&\, \overline{\mathcal{U}_{\gamma}(R)}](R \vee v{<}k) \right) \end{array} \right) \end{array}}{\vdash \mathrm{Stab}_{\mathrm{R}}^{\mathrm{P}}(x' = f(x), P, R)}$$

Rule GLyap proves general stability for precondition P and postcondition R. It generalizes the Lyapunov function reasoning underlying rule Lyap$_{\ge}$ to support arbitrary pre- and postconditions. The conjunct $\forall x \left(\partial(\mathcal{U}_{\gamma}(R)) \to v \ge k \right)$ requires $v{\ge}k$ on the boundary of $\mathcal{U}_{\gamma}(R)$ while the middle conjunct requires $v{<}k$ for some small neighborhood of P excluding R. The conjunct $\forall x \left(R \vee v{<}k \to \cdots \right)$ asserts that $R \vee v < k$ is an invariant of the ODE *within* closed domain $\overline{\mathcal{U}_{\gamma}(R)}$. When R is a formula of real arithmetic, this invariance question is provably equivalent in dL to a formula of real arithmetic [PT20], so the premise of rule GLyap is, *in theory*, decidable by $\mathbb{R}$ for a candidate Lyapunov function v. In practice, it is prudent to consider specialized stability notions, for which the premise of rule GLyap can be arithmetically simplified. Proof rules for generalized attractivity are also derivable for specialized instances.

4.2   Specialization

General stability specializes to several stability notions in the literature. For brevity, dL specifications of the stability properties (in **bold**) are given below with mathematical definitions deferred to Appendix B.

Set Stability.   An important special case is when the desired operating states are exactly the states from which disturbances are expected, i.e., $R \equiv P$. This leads to the notion of **set stability** of the set characterized by P [HC08, Kha92].

Lemma 16 (Set Stability in dL). *For the ODE $x' = f(x)$, the set characterized by formula P is i) **stable**, ii) **attractive**, iii) **asymptotically stable**, and iv) **globally asymptotically stable** iff the following dL formulas are valid:*

  i) $\mathrm{Stab}_{\mathrm{R}}^{\mathrm{P}}(x' = f(x), P, P)$,

  ii) $\exists \delta {>} 0 \ \mathrm{Attr}_{\mathrm{R}}^{\mathrm{P}}(x' = f(x), \mathcal{U}_\delta(P), P)$,

  iii) $\mathrm{Stab}_{\mathrm{R}}^{\mathrm{P}}(x' = f(x), P, P) \wedge \exists \delta {>} 0 \ \mathrm{Attr}_{\mathrm{R}}^{\mathrm{P}}(x' = f(x), \mathcal{U}_\delta(P), P)$, *and*

  iv) $\mathrm{Stab}_{\mathrm{R}}^{\mathrm{P}}(x' = f(x), P, P) \wedge \mathrm{Attr}_{\mathrm{R}}^{\mathrm{P}}(x' = f(x), true, P)$

The intuition for Lemma 16 is similar to Lemmas 4 and 11, except formula P (instead of the origin) characterizes the set of desirable states. An application of set stability is shown in the following example.

Example 17 (Tennis racket theorem [ACC91]).   The following system of ODEs models the rotation of a 3D rigid body [Chi06, HC08], where x_1, x_2, x_3 are angular velocities and $I_1 > I_2 > I_3 > 0$ are the principal moments of inertia along the respective axes.

$$\alpha_r \equiv x_1' = \frac{I_2 - I_3}{I_1} x_2 x_3, \quad x_2' = \frac{I_3 - I_1}{I_2} x_3 x_1, \quad x_3' = \frac{I_1 - I_2}{I_3} x_1 x_2$$

When such a rigid object is spun or rotated on each of its axes, a well-known physical curiosity [ACC91] is that the rotation is stable in the first and third axes, whilst additional (unstable) twisting motion is observed for the intermediate axis. Mathematically, a perfect rotation, e.g., around x_1, corresponds to a (large) initial value for x_1 with no rotation in the other axes, i.e., $x_2 = 0$, $x_3 = 0$. Accordingly the real world observation of stability for rotations about the first principal axis is explained by stability with respect to small perturbations in x_2, x_3, as formally specified by formula (3) below. Note that the set characterized by formula $x_2 = 0 \wedge x_3 = 0$ is the entire x_1 axis, not just a single point. Similarly, rotations are stable around the third principal axis iff formula (4) is valid.

$$\mathrm{Stab}_{\mathrm{R}}^{\mathrm{P}}(\alpha_r, x_2 = 0 \wedge x_3 = 0, x_2 = 0 \wedge x_3 = 0) \tag{3}$$

$$\mathrm{Stab}_{\mathrm{R}}^{\mathrm{P}}(\alpha_r, x_1 = 0 \wedge x_2 = 0, x_1 = 0 \wedge x_2 = 0) \tag{4}$$

The validity of formulas (3) and (4) are proved in Example 20.

The formal specification of set stability yields three provable logical consequences which are important stepping stones for the set stability proof rules.

Corollary 18 (Set stability properties). *The following axioms are derivable in dL. In axiom SClosure, formula $\overline{P}$ characterizes the topological closure of formula P. In axiom SClosed, formula P characterizes a closed set.*

SetSAttr $\mathrm{Stab}_{\mathrm{R}}^{\mathrm{P}}(x' = f(x), P, P) \rightarrow \big(\mathrm{Asym}(x' = f(x), P) \leftrightarrow \forall \varepsilon {>} 0 \, \langle x' = f(x) \rangle \, \mathcal{U}_\varepsilon(P) \big)$

SClosure $\mathrm{Stab}_{\mathrm{R}}^{\mathrm{P}}(x' = f(x), P, P) \leftrightarrow \mathrm{Stab}_{\mathrm{R}}^{\mathrm{P}}(x' = f(x), \overline{P}, \overline{P})$

SClosed $\mathrm{Stab}_{\mathrm{R}}^{\mathrm{P}}(x' = f(x), P, P) \rightarrow \forall x \, \big(P \rightarrow [x' = f(x)]P \big)$

Axiom SetSAttr generalizes SAttr and provides a syntactic simplification of the region of attraction for formula P when P is stable. Axiom SClosure says that stability of P is equivalent to stability of its closure $\overline{P}$, because for any perturbation $\delta > 0$, the neighborhoods $\mathcal{U}_\delta(P)$ and $\mathcal{U}_\delta(\overline{P})$ are provably equivalent in real arithmetic. Axiom SClosed says that for closed formulas P, invariance of P is a necessary condition for stability of P. Without loss of generality, it suffices to develop proof rules for stability of formulas characterizing closed (using SClosure) and invariant (using SClosed) sets. Indeed, standard definitions of set stability [HC08, Kha92] usually assume that the set of concern is closed and invariant.

Lemma 19 (Set stability Lyapunov functions). *The following Lyapunov function proof rules for set stability are derivable in* dL. *In rules SLyap$_\geq$, SLyap$_>$, formula P characterizes a compact (i.e., closed and bounded) set. In rule SLyap$_\geq^*$, the two premises are stacked.*

$$\text{SLyap}_\geq \quad \frac{P \vdash [x' = f(x)]P \quad \neg P \vdash v > 0 \wedge \dot{v} \leq 0 \quad \partial P \vdash v \leq 0}{\vdash \text{Stab}_R^P(x' = f(x), P, P)}$$

$$\text{SLyap}_> \quad \frac{P \vdash [x' = f(x)]P \quad \neg P \vdash v > 0 \wedge \dot{v} < 0 \quad \partial P \vdash v \leq 0}{\vdash \text{Stab}_R^P(x' = f(x), P, P) \wedge \exists \delta{>}0 \ \text{Attr}_R^P(x' = f(x), \mathcal{U}_\delta(P), P)}$$

$$\text{SLyap}_\geq^* \quad \frac{\begin{array}{l} P \vdash [x' = f(x)]P \\[4pt] \vdash \forall \varepsilon{>}0 \, \exists 0{<}\gamma{\leq}\varepsilon \left(\exists k \left(\begin{array}{l} \forall x \, (\partial(\mathcal{U}_\gamma(P)) \to v \geq k) \wedge \\ \exists 0{<}\delta{\leq}\gamma \, \forall x \, (\mathcal{U}_\delta(P) \wedge \neg P \to v < k) \end{array} \right) \wedge \\ \quad\quad\quad\quad\quad\quad\quad\quad \forall x \, (\overline{\mathcal{U}_\gamma(P)} \wedge \neg P \to \dot{v} \leq 0) \right) \end{array}}{\vdash \text{Stab}_R^P(x' = f(x), P, P)}$$

All three proof rules have the necessary premise $P \vdash [x' = f(x)]P$ which says that formula P is an invariant of the ODE $x' = f(x)$. Rules SLyap$_\geq$, SLyap$_>$ are slight generalizations of Lyapunov function proof rules for set stability [HC08] and they respectively generalize rules Lyap$_\geq$, Lyap$_>$ to prove stability for an invariant P. Importantly, both rules assume that P characterizes a compact, i.e., closed and bounded set, which simplifies the arithmetical conditions on v in their premises. The rule *without* the boundedness requirement on P suggested in the remark after [Kha92, Definition 8.1], is unsound, see Counterexample 28.

For asymptotic stability (in rule SLyap$_>$), boundedness also guarantees that perturbed ODE solutions always exist for sufficient duration, which is a fundamental step in the ODE liveness proofs [TPar]. Rule SLyap$_\geq^*$ is derived from rule GLyap using invariance of P by the first premise; it provides a means of formally proving the set stability properties (3) and (4) from Example 17.

Example 20 (Stability of rigid body motion). The proof for (3) uses the Lyapunov function $v = \frac{1}{2}\left(\frac{I_1 - I_2}{I_3} x_2^2 - \frac{I_3 - I_1}{I_2} x_3^2\right)$, whose Lie derivative is $\dot{v} = 0$, and rule SLyap$_\geq^*$ with formula $P \equiv x_2 = 0 \wedge x_3 = 0$. The proof for (4) is symmetric. For the top premise of rule SLyap$_\geq^*$, formula $\overline{P}$ is a provable invariant [PT20] of the ODE α_r. The bottom premise, although arithmetically complicated, can be simplified by choosing $\gamma = \varepsilon$ and deciding the resulting formula by $\mathbb{R}$.

Recall that the x_1 axis is *not* a compact set so neither of the standard proof rules for set stability SLyap$_\geq$, SLyap$_>$ would be sound for this proof.

Epsilon-Stability   Motivated by numerical robustness of proofs of stability, Gao et al. [GKD$^+$19] define ε-stability for ODEs. The following dL characterization shows how ε-stability can be understood as an instance of general stability.

Lemma 21 (ε-Stability in dL). *The origin of ODE $x' = f(x)$ is **ε-stable** for constant $\varepsilon > 0$ iff the dL formula* $\text{Stab}_R^P(x' = f(x), x = 0, \mathcal{U}_\varepsilon(x = 0))$ *is valid.*

Unlike set stability, ε-stability is an instance of general stability where the pre- and postconditions differ. In ε-stability, systems are perturbed from the precondition $x = 0$ (the origin), but the postcondition enlarges the set of desired states to a $\varepsilon > 0$ neighborhood of the origin, which is considered indistinguishable from the origin itself [GKD$^+$19]. An immediate consequence of Lemma 21 is that rule GLyap can be used to prove ε-stability, as shown in the next section.

5 Stability in KeYmaera X

This section puts the dL stability specifications and derivations from the preceding sections into practice through proofs for several case studies in the KeYmaera X theorem prover [FMQ+15].[6] Examples 7, 13, 17, 20 have also been formalized. The insights from these proofs are discussed after an overview of the case studies.

Inverted Pendulum. The stability of the resting state of the pendulum is investigated in Examples 7 and 13. For the inverted pendulum α_i from (2), the controlled torque $u(\theta, \omega)$ must be designed and rigorously proved to ensure *feedback stabilization* [Kha92] of the inverted position. A standard PD (Proportional-Derivative) controller can be used for stabilization, where the control input has the form $u(\theta, \omega) = k_1\theta + k_2\omega$ for tuning parameters k_1, k_2. Asymptotic stability of the inverted position is achieved for any control parameter choice where $k_1 > a$ and $k_2 > -b$. The sequent $a > 0, b \geq 0, k_1 > a, k_2 > -b \vdash \mathrm{AStab}(\alpha_i)$ is proved in KeYmaera X using the Lyapunov function $\frac{(k_1-a)\theta^2}{2} + \frac{(((b+k_2)\theta+\omega)^2+\omega^2)}{4}$.

Frictional Tennis Racket Theorem. The stability of a 3D rigid body is investigated for α_r in Examples 17 and 20. The following ODEs model additional frictional forces that oppose the rotational motion in each axis of the rigid body, where $\alpha_1, \alpha_2, \alpha_3 > 0$ are positive coefficients of friction:

$$\alpha_f \equiv x_1' = \frac{I_2 - I_3}{I_1}x_2x_3 - \alpha_1x_1, \ x_2' = \frac{I_3 - I_1}{I_2}x_3x_1 - \alpha_2x_2, \ x_3' = \frac{I_1 - I_2}{I_3}x_1x_2 - \alpha_3x_3$$

In the presence of friction, rotations of the rigid body are globally asymptotically stable in the first and third principal axes, as proved in KeYmaera X.

$$\Gamma \equiv I_1 > I_2, I_2 > I_3, I_3 > 0, \alpha_1 > 0, \alpha_2 > 0, \alpha_3 > 0$$
$$\Gamma \vdash \mathrm{Stab}_R^P(\alpha_f, x_2=0 \wedge x_3=0, x_2=0 \wedge x_3=0) \wedge \mathrm{Attr}_R^P(\alpha_f, \mathit{true}, x_2=0 \wedge x_3=0)$$
$$\Gamma \vdash \mathrm{Stab}_R^P(\alpha_f, x_1=0 \wedge x_2=0, x_1=0 \wedge x_2=0) \wedge \mathrm{Attr}_R^P(\alpha_f, \mathit{true}, x_1=0 \wedge x_2=0)$$

Both asymptotic stability properties are proved using $\mathrm{SLyap}_{\geq}^*$ and the liveness property [TPar] that the kinetic energy $I_1x_1^2 + I_2x_2^2 + I_3x_3^2$ of the system tends to zero over time. The latter property implies that solutions of α_f exist globally and that the values of x_1, x_2, x_3 asymptotically tend to zero, which proves global asymptotic stability with the aid of SetSAttr. Even though a proof rule for (global) asymptotic stability of general nonlinear ODEs and unbounded sets is not available (Section 4), this example shows that formalized stability properties can still be proved on a case-by-case basis using dL's ODE reasoning principles.

Moore-Greitzer Jet Engine [GKD+19]. The origin of the ODE modeling a simplified jet engine $\alpha_m \equiv x_1' = -x_2 - \frac{3}{2}x_1^2 - \frac{1}{2}x_1^3, \ x_2' = 3x_1 - x_2$ is ε-stable for $\varepsilon = 10^{-10}$ [GKD+19]. The following sequent is proved in KeYmaera X: $\varepsilon = 10^{-10} \vdash \mathrm{Stab}_R^P(\alpha_m, x_1^2 + x_2^2 = 0, x_1^2 + x_2^2 < \varepsilon^2)$. The key proof ingredients are an ε-Lyapunov function [GKD+19] and manual arithmetic steps, e.g., instantiating existential quantifiers appearing in the specification of ε-stability with appropriate values [GKD+19].

Other Examples [APA20]. Stability for several ODEs with Lyapunov functions generated by an inductive synthesis technique [APA20, Examples 5–11] were successfully verified in KeYmaera X. The proof for the largest, 6-dim. non-linear ODE [APA20, Example 5] required substantial manual arithmetic reasoning in KeYmaera X.[7]

The arithmetical conditions in [APA20, Equation 1] are identical to the premises of rule $\mathrm{Lyap}_{\geq}$ except it unsoundly omits the condition $v(0) = 0$, see Counterexample 29. The generated Lyapunov functions remain correct because the inductive synthesis technique [APA20] implicitly guarantees this omitted condition.

---

[6]See https://github.com/LS-Lab/KeYmaeraX-projects/blob/master/stability

[7]The Lyapunov function in [APA20, Example 5] does *not* work for its associated ODE. It works if the ODE is corrected with $\dot{x}_1 = -x_1^3 + 4x_2^3 - 6x_3x_4$, as in the literature [PP02].

Summary.   These case studies demonstrate the feasibility of carrying out proofs of various (advanced) stability properties within KeYmaera X using this paper's stability specifications. The proofs share similar high-level proof structure, which suggests that proof automation could significantly reduce proof effort [FMBP17]. Such automation should also support user input of key insights for difficult reasoning steps, e.g., real arithmetic reasoning with nested, alternating quantifiers.

6   Related Work

Stability is a fundamental property of interest across many different fields of mathematics [Chi06, Hir84, Lia07, Poi99, RHL77, Str15] and engineering [HC08, Kha92, Lib03]. This related work discussion focuses on formal approaches to stability of ODEs.

Logical Specification of Stability.   Rouche, Habets, and Laloy [RHL77] provide a pioneering example of using logical notation to specify and classify stability properties of ODEs. Alternative logical frameworks have also been used to specify stability and related properties: stability is expressed in HyperSTL [NKJ$^+$17] as a hyperproperty relating the trace of an ODE against two constant traces; ϵ-stability is studied in the context of δ-complete reasoning over the reals [GKD$^+$19]; region stability for hybrid systems [PW06] is discussed using CTL*; the syntactic specification of $\mathrm{Asym}(x' = f(x), P)$ resembles the limit definition using filters [HIH13]. This paper uses dL as a *sweet spot* logical framework, general enough to specify various stability properties of interest, e.g., asymptotic or exponential stability, and the stability of sets, while also enabling syntactic proofs of those properties.

Formal Verification of Stability.   There is a vast literature on finding Lyapunov functions for stability, e.g., through numerical [Par00, PP02, TPS08] and algebraic methods [For91, LZZ12]. Formal approaches are often based on finding Lyapunov function candidates and *certifying* the correctness of those generated candidates [APA20, GKD$^+$19, KDSA14, SCÁ13]. This paper's approach enables highly trustworthy certification of those candidates in dL and KeYmaera X, with stability proof rules that are soundly *derived* from dL's parsimonious axiomatization [Pla12, Pla17, Pla18], as implemented in KeYmaera X [FMQ$^+$15, Pla17]. Sections 4 and 5 further show that this paper's approach supports verification of advanced stability properties [GKD$^+$19, HC08, Kha92] within the same dL framework. New stability proof rules like GLyap can also be soundly and *syntactically* justified in dL without the need for (low-level) semantic reasoning about the underlying ODE mathematics. As an example of the latter, semantic approach, LaSalle's invariance principle is formalized in Coq [CR17] and used to verify the correctness of an inverted pendulum controller [Rou18].

7   Conclusion

This paper shows how ODE stability can be formalized in dL using the key idea that stability properties are $\forall/\exists$-quantified dynamical formulas. These specifications, their proof rules, and their logical relationships are all syntactically derived from dL's sound proof calculus. This further enables trustworthy KeYmaera X proofs that rigorously verify *every step* in an ODE stability argument, from arithmetical premises down to dynamical reasoning for ODEs. Directions for future work include *i)* formalization of stability with respect to perturbations of the system dynamics, and *ii)* generalizations of stability to hybrid systems.

References

[ACC91] Mark S. Ashbaugh, Carmen C. Chicone, and Richard H. Cushman. The twisting tennis racket. *Journal of Dynamics and Differential Equations*, 3:67–85, 1991. doi:10.1007/BF01049489.

[Alu15] Rajeev Alur. *Principles of Cyber-Physical Systems*. MIT Press, 2015.

[APA20] Daniele Ahmed, Andrea Peruffo, and Alessandro Abate. Automated and sound synthesis of Lyapunov functions with SMT solvers. In Armin Biere and David Parker, editors, *TACAS*, volume 12078 of *LNCS*, pages 97–114. Springer, 2020. doi:10.1007/978-3-030-45190-5_6.

[BCR98] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. *Real Algebraic Geometry*. Springer, Heidelberg, 1998. doi:10.1007/978-3-662-03718-8.

[Boh17] Brandon Bohrer. Differential dynamic logic. *Arch. Formal Proofs*, 2017, 2017. URL https://www.isa-afp.org/entries/Differential_Dynamic_Logic.shtml.

[Bra05] Michael S. Branicky. Introduction to hybrid systems. In Dimitrios Hristu-Varsakelis and William S. Levine, editors, *Handbook of Networked and Embedded Control Systems*, pages 91–116. Birkhäuser, 2005. doi:10.1007/0-8176-4404-0_5.

[Chi06] Carmen Chicone. *Ordinary Differential Equations with Applications*. Springer, New York, second edition, 2006. doi:10.1007/0-387-35794-7.

[CR17] Cyril Cohen and Damien Rouhling. A formal proof in Coq of LaSalle's invariance principle. In Mauricio Ayala-Rincón and César A. Muñoz, editors, *ITP*, volume 10499 of *LNCS*, pages 148–163. Springer, 2017. doi:10.1007/978-3-319-66107-0_10.

[DFPP18] Laurent Doyen, Goran Frehse, George J. Pappas, and André Platzer. Verification of hybrid systems. In Edmund M. Clarke, Thomas A. Henzinger, Helmut Veith, and Roderick Bloem, editors, *Handbook of Model Checking*, pages 1047–1110. Springer, Cham, 2018. doi:10.1007/978-3-319-10575-8_30.

[FMBP17] Nathan Fulton, Stefan Mitsch, Brandon Bohrer, and André Platzer. Bellerophon: Tactical theorem proving for hybrid systems. In Mauricio Ayala-Rincón and César A. Muñoz, editors, *ITP*, volume 10499 of *LNCS*, pages 207–224. Springer, 2017. doi:10.1007/978-3-319-66107-0_14.

[FMQ+15] Nathan Fulton, Stefan Mitsch, Jan-David Quesel, Marcus Völp, and André Platzer. KeYmaera X: an axiomatic tactical theorem prover for hybrid systems. In Amy P. Felty and Aart Middeldorp, editors, *CADE*, volume 9195 of *LNCS*, pages 527–538, Cham, 2015. Springer. doi:10.1007/978-3-319-21401-6_36.

[For91] K. Forsman. Construction of Lyapunov functions using Gröbner bases. In *CDC*, volume 1, pages 798–799. IEEE, 1991. doi:10.1109/CDC.1991.261424.

[GKD+19] Sicun Gao, James Kapinski, Jyotirmoy V. Deshmukh, Nima Roohi, Armando Solar-Lezama, Nikos Aréchiga, and Soonho Kong. Numerically-robust inductive proof rules for continuous dynamical systems. In Isil Dillig and Serdar Tasiran, editors, *CAV*, volume 11562 of *LNCS*, pages 137–154. Springer, 2019. doi:10.1007/978-3-030-25543-5_9.

[GST12] Rafal Goebel, Ricardo G. Sanfelice, and Andrew R. Teel. *Hybrid Dynamical Systems: Modeling, Stability, and Robustness*. Princeton University Press, 2012.

[HC08] Wassim M. Haddad and VijaySekhar Chellaboina. *Nonlinear Dynamical Systems and Control: A Lyapunov-Based Approach*. Princeton University Press, 2008.

[HIH13] Johannes Hölzl, Fabian Immler, and Brian Huffman. Type classes and filters for mathematical analysis in Isabelle/HOL. In Sandrine Blazy, Christine Paulin-Mohring, and David Pichardie, editors, *ITP*, volume 7998 of *LNCS*, pages 279–294. Springer, 2013. doi:10.1007/978-3-642-39634-2_21.

[Hir84] Morris W. Hirsch. The dynamical systems approach to differential equations. *Bull. Amer. Math. Soc. (N.S.)*, 11(1):1–64, 07 1984.

[KDH+20] Juraj Kolcák, Jérémy Dubut, Ichiro Hasuo, Shin-ya Katsumata, David Sprunger, and Akihisa Yamada. Relational differential dynamic logic. In Armin Biere and David Parker, editors, *TACAS*, volume 12078 of *LNCS*, pages 191–208. Springer, 2020. doi:10.1007/978-3-030-45190-5_11.

[KDSA14] James Kapinski, Jyotirmoy V. Deshmukh, Sriram Sankaranarayanan, and Nikos Aréchiga. Simulation-guided Lyapunov analysis for hybrid dynamical systems. In Martin Fränzle and John Lygeros, editors, *HSCC*, pages 133–142. ACM, 2014. doi:10.1145/2562059.2562139.

[Kha92] Hassan K. Khalil. *Nonlinear systems*. Macmillan Publishing Company, New York, 1992.

[Lia07] A. Liapounoff. Probléme général de la stabilité du mouvement. *Annales de la Faculté des sciences de Toulouse : Mathématiques*, 9:203–474, 1907.

[Lib03] Daniel Liberzon. *Switching in Systems and Control*. Systems & Control: Foundations & Applications. Birkhäuser, 2003. doi:10.1007/978-1-4612-0017-8.

[LZZ12] Jiang Liu, Naijun Zhan, and Hengjun Zhao. Automatically discovering relaxed Lyapunov functions for polynomial dynamical systems. *Math. Comput. Sci.*, 6(4):395–408, 2012. doi:10.1007/s11786-012-0133-6.

[NKJ+17] Luan Viet Nguyen, James Kapinski, Xiaoqing Jin, Jyotirmoy V. Deshmukh, and Taylor T. Johnson. Hyperproperties of real-valued signals. In Jean-Pierre Talpin, Patricia Derler, and Klaus Schneider, editors, *MEMOCODE*, pages 104–113. ACM, 2017. doi:10.1145/3127041.3127058.

[Par00] Pablo A. Parrilo. *Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization*. PhD thesis, California Institute of Technology, 2000.

[Pla12] André Platzer. The complete proof theory of hybrid systems. In *LICS*, pages 541–550. IEEE Computer Society, 2012. doi:10.1109/LICS.2012.64.

[Pla17] André Platzer. A complete uniform substitution calculus for differential dynamic logic. *J. Autom. Reasoning*, 59(2):219–265, 2017. doi:10.1007/s10817-016-9385-1.

[Pla18] André Platzer. *Logical Foundations of Cyber-Physical Systems*. Springer, Cham, 2018. doi:10.1007/978-3-319-63588-0.

[Poi99] Henri Poincaré. *Les méthodes nouvelles de la mécanique céleste*. Gauthier-Villars, Paris, 1892–1899.

[PP02] A. Papachristodoulou and S. Prajna. On the construction of Lyapunov functions using the sum of squares decomposition. In *CDC*, volume 3, pages 3482–3487. IEEE, 2002. doi:10.1109/CDC.2002.1184414.

[PT20] André Platzer and Yong Kiam Tan. Differential equation invariance axiomatization. *J. ACM*, 67(1), 2020. doi:10.1145/3380825.

[PW06] Andreas Podelski and Silke Wagner. Model checking of hybrid systems: From reachability towards stability. In João P. Hespanha and Ashish Tiwari, editors, *HSCC*, volume 3927 of *LNCS*, pages 507–521. Springer, 2006. doi:10.1007/11730637_38.

[RHL77] Nicolas Rouche, P. Habets, and M. Laloy. *Stability Theory by Liapunov's Direct Method*. Springer, New York, 1977. doi:10.1007/978-1-4684-9362-7.

[Rou18] Damien Rouhling. A formal proof in Coq of a control function for the inverted pendulum. In June Andronick and Amy P. Felty, editors, *CPP*, pages 28–41. ACM, 2018. doi:10.1145/3167101.

[Rud76] Walter Rudin. *Principles of Mathematical Analysis*. McGraw-Hill, third edition, 1976.

[SCÁ13] Sriram Sankaranarayanan, Xin Chen, and Erika Ábrahám. Lyapunov function synthesis using Handelman representations. In Sophie Tarbouriech and Miroslav Krstic, editors, *NOLCOS*, pages 576–581. IFAC, 2013. doi:10.3182/20130904-3-FR-2041.00198.

[Str15] Steven H. Strogatz. *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*. Westview Press, Boulder, CO, second edition, 2015.

[TPar] Yong Kiam Tan and André Platzer. An axiomatic approach to existence and liveness for differential equations. *Formal Aspects Comput.*, to appear. doi:10.1007/s00165-020-00525-0.

[TPS08]   Ufuk Topcu, Andrew K. Packard, and Peter J. Seiler. Local stability analysis using simulations and sum-of-squares programming. *Autom.*, 44(10):2669–2675, 2008. doi:10.1016/j.automatica.2008.03.010.

A   Proof Calculus

This appendix gives an extended introduction to the dL proof calculus that is used for the proofs in Appendix B. Propositional proof rules, e.g., cut, ¬R, →R, are omitted as they are standard from propositional sequent calculus and can be found in the literature [Pla18, PT20]; the first-order quantifier rules ∀L, ∃R instantiate quantified variables with a given term. The following lemma summarizes the base axioms and proof rules of dL.

Lemma 22 (Axioms and proof rules of dL [Pla17, Pla18])**.** *The following are sound axioms and proof rules of* dL.
$\langle \cdot \rangle \ \langle \alpha \rangle P \leftrightarrow \neg [\alpha] \neg P \qquad \mathsf{K} \ [\alpha](R \to P) \to ([\alpha]R \to [\alpha]P)$

$\mathsf{V} \ \phi \to [\alpha]\phi \quad$ (no free variable of ϕ is bound by α)

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

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

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

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

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

Proof. The soundness of all axioms and proof rules in Lemma 22 are proved elsewhere [Pla17, Pla18].   □

The first three hybrid program axioms ⟨·⟩, K, V [Pla17, Pla18] of dL are used in this paper when the hybrid program α is an ODE. Axiom ⟨·⟩ expresses the duality between the box and diamond modalities. It is used to switch between the two in proofs to turn a liveness property (⟨·⟩) of an ODE to a (negated) safety property ([·]) of the same ODE, or vice versa. Axiom K is the modus ponens principle for the box modality. Vacuous axiom V says if no free variable of ϕ is changed by hybrid program α, then the truth value of ϕ is also unchanged. This axiom formally justifies that assumptions involving only constant ODE parameters can be soundly kept across ODE deduction steps in proofs [Pla18], as explained in Section 2.

Differential invariants $\mathrm{dI}_{\succcurlyeq}$ say that if the Lie derivatives obey the inequality $\dot{p} \geq \dot{q}$, then $p \succcurlyeq q$ is an invariant of the ODE. Differential cuts dC say that if one can separately prove that formula C is always satisfied along ODE solutions, then C may be assumed in the domain constraint when proving the same for formula P. Differential ghosts DG say that, in order to prove safety postcondition $P(x)$ for the ODE $x' = f(x)$, it suffices to prove $P(x)$ for a larger system with an added ODE $y' = a(x)y + b(x)$ that is linear in the fresh ghost variable y (because $a(x), b(x)$ do not mention y). This addition is sound because the ODE $x' = f(x)$ does not mention the added variables y, and so the evolution of $x' = f(x)$ is unaffected by the addition of a *linear* ODE for y [Pla17]. Since y is fresh, its initial value can be either existentially (DG) or universally (DG$_\forall$) quantified [Pla17].

In the box modality, solutions are restricted to stay in the domain constraint Q. Thus, differential weakening dW says that postcondition P is always satisfied along solutions if it is already implied by the domain constraint. Using dW, K, ⟨·⟩, the final two monotonicity proof rules M['], M⟨'⟩ for differential equations are derivable. They strengthen the postcondition from P to R, assuming domain constraint Q, for the box and diamond modalities respectively.

The dL proof calculus has a sound and complete axiomatization for ODE invariants [PT20]; completeness means that for ODE $x' = f(x)$, if formula P is an invariant of the ODE, then its invariance is syntactically provable in dL. For added clarity in this paper's invariance proofs, the following lemma lists additional axioms and proof rules that are useful for step-by-step proofs (Appendix B). The additional detail in these proofs helps inform the implementation

of stability proof rules in KeYmaera X [FMQ$^+$15, PT20]. The lemma also lists axioms and proof rules from dL's refinement-based proof approach for ODE liveness properties [TPar].

Lemma 23 (Invariance and liveness dL axioms and proof rules [PT20, TPar]). *The following are sound axioms and proof rules of* dL.

DX $[x' = f(x) \,\&\, Q]P \leftrightarrow (Q \rightarrow P \land [x' = f(x) \,\&\, Q]P)$ $(x' \notin P, Q)$

D[;] $[x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x) \,\&\, Q][x' = f(x) \,\&\, Q]P$

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

DCC $[x' = f(x) \,\&\, Q \land P]R \land [x' = f(x) \,\&\, Q](\neg P \rightarrow [x' = f(x) \,\&\, Q]\neg P) \rightarrow [x' = f(x) \,\&\, Q](P \rightarrow R)$

B' $\langle x' = f(x) \,\&\, Q(x) \rangle \exists y P(x, y) \leftrightarrow \exists y \langle x' = f(x) \,\&\, Q(x) \rangle P(x, y)$ $(y \notin x)$

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

Enc $\dfrac{\Gamma \vdash \overline{P} \quad \Gamma \vdash [x' = f(x) \,\&\, Q \land \overline{P}]P}{\Gamma \vdash [x' = f(x) \,\&\, Q]P}$ (formula P characterizes an open set)

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

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

SP$_c$ $\dfrac{\Gamma \vdash [x' = f(x) \,\&\, \neg P]S \quad S \vdash \dot{p} > 0}{\Gamma \vdash \langle x' = f(x) \rangle P}$ (formula S characterizes a compact set)

Proof. The soundness of all axioms and proof rules in Lemma 23 are proved elsewhere [PT20, TPar] except axioms D[;] and DCC. Axiom DCC is stated as a proof rule elsewhere [KDH$^+$20] and its axiomatic version is formally verified [Boh17]. Axiom D[;] is proved sound next.

Consider the initial state $\nu \in \mathbb{S}$ and let $\boldsymbol{\varphi} : [0, T) \rightarrow \mathbb{S}, 0 < T \leq \infty$ be the unique, right-maximal solution [Chi06] to the ODE $x' = f(x)$ with initial value $\boldsymbol{\varphi}(0) = \nu$. Unfolding the semantics, the RHS of axiom D[;] is true in state ν iff for all times $0 \leq \tau < T$ such that $\boldsymbol{\varphi}(\zeta) \in [\![Q]\!]$ for all $0 \leq \zeta \leq \tau$, the solution at time τ satisfies $\boldsymbol{\varphi}(\tau) \in [\![[x' = f(x) \,\&\, Q]P]\!]$. Further unfolding the semantics, by uniqueness of ODE solutions [Chi06], this means that for all times $\tau \leq t < T$, such that $\boldsymbol{\varphi}(\zeta) \in [\![Q]\!]$ for all $\tau \leq \zeta \leq t$, the solution at time t satisfies $\boldsymbol{\varphi}(t) \in [\![P]\!]$. Thus, the RHS is true in state ν iff for all times $0 \leq \tau < T$ such that $\boldsymbol{\varphi}(\zeta) \in [\![Q]\!]$ for all $0 \leq \zeta \leq \tau$, the solution at time τ satisfies $\boldsymbol{\varphi}(\tau) \in [\![P]\!]$, which is the unfolded semantics of the LHS of axiom D[;]. $\square$

Differential skip DX is a reflexivity property of differential equation solutions, if the domain constraint Q is true initially, then P must also be true initially because of the ODE solution at time 0. Differential compose D[;] is a transitivity property of differential equation solutions, because any state reachable from two sequential runs of an ODE is reachable in a single run of the ODE.

Axiom DMP is the modus ponens principle for domain constraints. Axiom DCC says in order to prove that an implication $P \rightarrow R$ is always true along an ODE, it suffices to prove it assuming P in the domain if $\neg P$ is invariant along the ODE. The ODE Barcan axiom B' specializes the Barcan axiom [Pla18, PT20] to ODEs in the diamond modality, allowing an existential quantifier $\exists y$ to be commuted with the diamond modality. The bounded differential ghosts axiom BDG generalizes DG by allowing a vectorial ghost ODE with arbitrary RHS $y' = g(x, y)$ to be added. For soundness, this RHS must be bounded in norm with respect to the existing variables x of the ODE so that the added ODEs for y do not blow up before the original solution for $x' = f(x)$ [TPar]. Rule Enc is a derived proof rule which says that to prove that a solution always stays in the open set characterized by formula P, it suffices to prove it assuming the closure $\overline{P}$ in the domain constraint. Rule dbx$_{\succcurlyeq}$ is a derived proof rule [PT20] which proves the invariance of formula $p \succcurlyeq 0$ if its Lie derivative satisfies inequality $\dot{p} \geq gp$ for an arbitrarily chosen cofactor term g.

Axiom K$\langle\&\rangle$ is a derived ODE liveness refinement axiom [TPar]. The formula $[x' = f(x) \,\&\, Q \land \neg P]\neg G$ says G never happens along the solution while $\neg P$ holds. Thus, the solution cannot get to G unless it gets to P first. Rule SP$_c$

is a derived ODE liveness proof rule [TPar]. Its left premise says that as long as the ODE solution has not reached the target P, it stays in the compact staging set S. Its right premise says that the value of p increases as long as solutions stay in S. Due to the compactness assumption, p *cannot* increase indefinitely in S and so the ODE solution must eventually leave the staging set by entering the target P. This rule implicitly proves that the ODE solution exists for sufficient duration to reach P, which is a fundamental requirement for soundness in ODE liveness arguments [TPar].

B   Proofs

This appendix provides proofs for all lemmas and corollaries from Sections 3 and 4 using the dL proof calculus in Appendix A. For ease of reference, this appendix is organized into two sections, corresponding to proofs for Section 3 and Section 4 respectively. Additional definitions and lemmas omitted in the main paper are provided as required.

B.1   Proofs for Asymptotic Stability of an Equilibrium Point

This section concerns stability for the origin, whose ε neighborhoods $\mathcal{U}_\varepsilon(x = 0)$ are equivalently unfolded as the formula $\|x\|^2 < \varepsilon^2$. The following lemma formalizes the claim in Section 3.1 that a point x_0 of interest for the ODE $x' = f(x)$ can be rigorously translated *with proof* to the origin so that, without loss of generality, only stability of the origin needs to be considered for the stability proof rules of Section 3.

Lemma 24 (Translation to origin). *The following axioms are derivable in* dL, *where ODE $y' = f(y + x_0)$ has point x_0 translated to the origin and variables y are fresh, i.e., not in ODE $x' = f(x)$ or formula $P(x)$.*

Trans $y = x - x_0 \rightarrow \big([x' = f(x)]P(x - x_0) \leftrightarrow [y' = f(y + x_0)]P(y)\big)$

TransStab $\mathrm{Stab}(y' = f(y + x_0)) \rightarrow \mathrm{Stab}_{\mathrm{R}}^{\mathrm{P}}(x' = f(x), x = x_0, x = x_0)$

Proof. Axiom Trans is derived first before axiom TransStab is derived from it as a corollary. Only the "$\rightarrow$" direction of the inner equivalence for axiom Trans is derived since the "$\leftarrow$" direction follows from the "$\rightarrow$" direction by renaming and translation with respect to $-x_0$.

Let $\alpha_{xy} \equiv x' = f(x), y' = f(y + x_0)$ abbreviate the combined ODE for variables x and y. The derivation starts with a cut of formula $[\alpha_{xy}]\, y = x - x_0$, which says the value of y is always equal to $x - x_0$ along solutions of the combined ODE α_{xy}. This cut is provable in dL using its complete, derived proof rule for algebraic invariants [PT20]. Subsequently, axiom BDG adds the ghost ODE $y' = f(y + x_0)$ to the antecedent box modality and ODE $x' = f(x)$ to the succedent box modality. The resulting boundedness premises from the use of BDG are respectively abbreviated ① and ②, and are both proved using the cut antecedent as shown further below.

$$
\cfrac{
\cfrac{
\cfrac{
\cfrac{② \quad [\alpha_{xy}]y = x - x_0, [\alpha_{xy}]P(x - x_0) \vdash [\alpha_{xy}]P(y)}
{① \quad [\alpha_{xy}]y = x - x_0, [\alpha_{xy}]P(x - x_0) \vdash [y' = f(y + x_0)]P(y)} \text{BDG}}
{[\alpha_{xy}]y = x - x_0, [x' = f(x)]P(x - x_0) \vdash [y' = f(y + x_0)]P(y)} \text{BDG}}
{y = x - x_0, [x' = f(x)]P(x - x_0) \vdash [y' = f(y + x_0)]P(y)} \text{cut}}
$$

From the (unabbreviated) open right premise, a dC step adds formulas $y = x - x_0$ and $P(x - x_0)$ to the domain constraint of the succedent. A subsequent dW step completes the proof by substituting $y = x - x_0$.

$$
\cfrac{
\cfrac{
\cfrac{
\cfrac{*}{y = x - x_0 \land P(x - x_0) \vdash P(y)} \mathbb{R}}
{\vdash [\alpha_{xy} \,\&\, y = x - x_0 \land P(x - x_0)]P(y)} \text{dW}}
{[\alpha_{xy}]P(x - x_0) \vdash [\alpha_{xy} \,\&\, y = x - x_0]P(y)} \text{dC}}
{[\alpha_{xy}]y = x - x_0, [\alpha_{xy}]P(x - x_0) \vdash [\alpha_{xy}]P(y)} \text{dC}}
$$

For premise ①, the ghost variables y are provably bounded in (squared) norm by the term $\|x - x_0\|^2$ for ODE α_{xy}. The dC step adds $y = x - x_0$ from the antecedent box modality to the domain constraint, and the subsequent dW step completes the proof by substituting $y = x - x_0$ and $\mathbb{R}$.

$$\mathbb{R} \dfrac{\qquad\qquad *}{y = x - x_0 \vdash \|y\|^2 \le \|x - x_0\|^2}$$
$$\text{dW} \dfrac{}{\vdash [\alpha_{xy} \,\&\, y = x - x_0]\|y\|^2 \le \|x - x_0\|^2}$$
$$\text{dC} \dfrac{}{[\alpha_{xy}]y = x - x_0 \vdash [\alpha_{xy}]\|y\|^2 \le \|x - x_0\|^2}$$

The derivation for premise ② is similar, where the ghost variables x are provably bounded in (squared) norm by the term $\|y + x_0\|^2$ for ODE α_{xy}.

$$\mathbb{R} \dfrac{\qquad\qquad *}{y = x - x_0 \vdash \|x\|^2 \le \|y + x_0\|^2}$$
$$\text{dW} \dfrac{}{\vdash [\alpha_{xy} \,\&\, y = x - x_0]\|x\|^2 \le \|y + x_0\|^2}$$
$$\text{dC} \dfrac{}{[\alpha_{xy}]y = x - x_0 \vdash [\alpha_{xy}]\|x\|^2 \le \|y + x_0\|^2}$$

The derivation of axiom TransStab starts by Skolemizing ε in the succedent with $\forall$R and then instantiating the antecedent with the resulting fresh Skolem variable ε using $\forall$L. This is followed by $\exists$L, $\exists$R which Skolemizes δ in the antecedent and then witnesses the succedent with δ. Next, $\forall$R, $\rightarrow$R Skolemizes the succedent before $\forall$L instantiates y in the quantified antecedent, with the translated coordinate $y = x - x_0$. Formula $y = x - x_0 \land \|x - x_0\|^2 < \delta^2 \rightarrow \|y\|^2 < \delta^2$ is provable in real arithmetic, so $\rightarrow$L, $\mathbb{R}$ proves the LHS of the implication ($\|y\|^2 < \delta^2$) in the antecedent before Trans completes the proof. The formulas are abbreviated $R_y \equiv [y' = f(y + x_0)]\,\|y\|^2 < \varepsilon^2$ and $R \equiv [x' = f(x)]\,\|x - x_0\|^2 < \varepsilon^2$, respectively.

$$\text{Trans} \dfrac{\qquad\qquad *}{y = x - x_0, R_y \vdash R}$$
$$\rightarrow\text{L, }\mathbb{R} \dfrac{}{y = x - x_0, \|y\|^2 < \delta^2 \rightarrow R_y, \|x - x_0\|^2 < \delta^2 \vdash R}$$
$$\forall\text{L} \dfrac{}{\forall y\left(\|y\|^2 < \delta^2 \rightarrow R_y\right), \|x - x_0\|^2 < \delta^2 \vdash R}$$
$$\forall\text{R, }\rightarrow\text{R} \dfrac{}{\forall y\left(\|y\|^2 < \delta^2 \rightarrow R_y\right) \vdash \forall x\left(\|x - x_0\|^2 < \delta^2 \rightarrow R\right)}$$
$$\exists\text{L, }\exists\text{R} \dfrac{}{\exists \delta{>}0\,\forall y\left(\|y\|^2 < \delta^2 \rightarrow R_y\right) \vdash \exists \delta{>}0\,\forall x\left(\|x - x_0\|^2 < \delta^2 \rightarrow R\right)}$$
$$\forall\text{R, }\forall\text{L} \dfrac{}{\text{Stab}(y' = f(y + x_0)) \vdash \text{Stab}_{\text{R}}^{\text{P}}(x' = f(x), x = x_0, x = x_0)} \qquad \square$$

Proof of Lemma 4. The correctness of these specifications follows directly from the semantics of dL formulas [Pla17, Pla18] because they syntactically express the logical connectives and quantifiers from Def. 2 in dL. The open neighborhood formulas $\mathcal{U}_\delta(x = 0)$ and $\mathcal{U}_\varepsilon(x = 0)$ are true in states where $\|x\| < \delta$ and $\|x\| < \varepsilon$ respectively. The main subtlety is formula $\text{Attr}(x' = f(x))$ which characterizes the limit $\lim_{t \to T} x(t) = 0$ using its subformula $\text{Asym}(x' = f(x), x = 0)$ as follows.

Unfolding the semantics, formula $\text{Asym}(x' = f(x), P)$ is true in an initial state iff for any $\varepsilon > 0$, the right-maximal ODE solution to $x' = f(x)$ (restricted to variables x) denoted $x(t) : [0, T) \to \mathbb{R}^n$ has a time $\tau \in [0, T)$ where, because of uniqueness of ODE solutions [Chi06, Theorem 1.2], for all future times t with $\tau \le t < T$, the solution at $x(t)$ satisfies formula $\mathcal{U}_\varepsilon(P)$; for $P \equiv x = 0$, this implies the bound $\|x(t)\| < \varepsilon$ at those future times, which is the real analytic definition of the limit $\lim_{t \to T} x(t) = 0$ [Rud76, Definition 4.1]. $\qquad \square$

Proof of Corollary 5. A full proof is omitted as axiom SAttr is an instance of the more general axiom SetSAttr derived in Corollary 18 (where $P \equiv x = 0$). Briefly, the "$\rightarrow$" direction of the inner equivalence is valid even without assuming stability because postcondition $[x' = f(x)]\mathcal{U}_\varepsilon(x{=}0)$ monotonically implies postcondition $\mathcal{U}_\varepsilon(x{=}0)$. The (interesting) "$\leftarrow$" direction of the inner equivalence uses the stability assumption by choosing $\delta > 0$ sufficiently small so that solutions reaching $\mathcal{U}_\delta(x{=}0)$ must stay in $\mathcal{U}_\varepsilon(x{=}0)$ thereafter because of stability. $\qquad \square$

Proof of Lemma 6. Rule Lyap$_\ge$ is derived first as it is an important stepping stone in the derivation of rule Lyap$_>$.

The derivation of rule Lyap$_\ge$ begins with a series of arithmetic cuts which are justified stepwise. For any $\varepsilon > 0$ and an equilibrium point at the origin with $f(0) = 0$, the second (right) premise of Lyap$_\ge$ can be equivalently strengthened to choose $\gamma \le \varepsilon$, i.e., the second premise provably implies the following formula in real arithmetic; the universal quantifier on x is also distributed across the inner conjunction as shown in conjuncts ⓐ and ⓑ below:

$$\exists 0{<}\gamma{\le}\varepsilon\left(\underbrace{\forall x\left(0 < \|x\|^2 \le \gamma^2 \rightarrow v > 0\right)}_{\text{ⓐ}} \land \underbrace{\forall x\left(\|x\|^2 \le \gamma^2 \rightarrow \dot{v} \le 0\right)}_{\text{ⓑ}}\right)$$

The derivation begins with a cut of this formula and Skolemizing with $\exists L$, yielding antecedents ⓐ and ⓑ as indicated above. The postcondition is then monotonically strengthened to $\|x\|^2 < \gamma^2$ using antecedent $\gamma \leq \varepsilon$.

$$
\begin{array}{c}
\cfrac{
\cfrac{
\cfrac{
\gamma > 0, ⓐ, ⓑ \vdash \exists \delta{>}0\, \forall x \left(\|x\|^2 < \delta^2 \to [x' = f(x)]\, \|x\|^2 < \gamma^2\right)
}{
\gamma > 0, \gamma \leq \varepsilon, ⓐ, ⓑ \vdash \exists \delta{>}0\, \forall x \left(\|x\|^2 < \delta^2 \to [x' = f(x)]\, \|x\|^2 < \varepsilon^2\right)
}\text{\scriptsize M[']}
}{
\varepsilon > 0 \vdash \exists \delta{>}0\, \forall x \left(\|x\|^2 < \delta^2 \to [x' = f(x)]\, \|x\|^2 < \varepsilon^2\right)
}\text{\scriptsize cut, }\exists L
}{
\vdash \text{Stab}(x' = f(x))
}\text{\scriptsize $\forall$R}
\end{array}
$$

From ⓐ, the continuous Lyapunov function v is positive on the compact set characterized by $\|x\|^2 = \gamma^2$ and therefore is bounded below by its minimum $k > 0$ on that set. Furthermore, from premise $v(0) = 0$, by continuity, v must take values smaller than k in a ball with sufficiently small radius $0 < \delta < \gamma$ around the origin. Thus, the following formula proves in real arithmetic from ⓐ.

$$
\exists k \left(\underbrace{\forall x \left(\|x\|^2 = \gamma^2 \to v \geq k\right)}_{ⓒ} \wedge \exists 0{<}\delta{<}\gamma\, \underbrace{\forall x \left(\|x\|^2 < \delta^2 \to v < k\right)}_{ⓓ} \right)
$$

The proof continues with a cut of the formula and Skolemizing the resulting antecedent with $\exists L$.

$$
\cfrac{
0{<}\delta{<}\gamma, ⓑ, ⓒ, ⓓ \vdash \exists \delta{>}0\, \forall x \left(\|x\|^2 < \delta^2 \to [x' = f(x)]\, \|x\|^2 < \gamma^2\right)
}{
\gamma > 0, ⓐ, ⓑ \vdash \exists \delta{>}0\, \forall x \left(\|x\|^2 < \delta^2 \to [x' = f(x)]\, \|x\|^2 < \gamma^2\right)
}\text{\scriptsize cut, }\mathbb{R}, \exists L
$$

The succedent existential quantifier $\exists \delta{>}0$ is instantiated with the antecedent's δ using $\exists R$, followed by simplification steps, Skolemizing and unfolding the succedent with $\forall R$, $\to R$ then instantiating ⓓ by $\forall L$, $\to L$ with the resulting $\|x\|^2 < \delta^2$ assumption.

$$
\begin{array}{c}
\cfrac{
\cfrac{
\cfrac{
\delta{<}\gamma, ⓑ, ⓒ, \|x\|^2 < \delta^2, v < k \vdash [x' = f(x)]\, \|x\|^2 < \gamma^2
}{
\delta{<}\gamma, ⓑ, ⓒ, ⓓ, \|x\|^2 < \delta^2 \vdash [x' = f(x)]\, \|x\|^2 < \gamma^2
}\text{\scriptsize $\forall$L, $\to$L}
}{
\delta{<}\gamma, ⓑ, ⓒ, ⓓ \vdash \forall x \left(\|x\|^2 < \delta^2 \to [x' = f(x)]\, \|x\|^2 < \gamma^2\right)
}\text{\scriptsize $\forall$R, $\to$R}
}{
0{<}\delta{<}\gamma, ⓑ, ⓒ, ⓓ \vdash \exists \delta{>}0\, \forall x \left(\|x\|^2 < \delta^2 \to [x' = f(x)]\, \|x\|^2 < \gamma^2\right)
}\text{\scriptsize $\exists$R}
\end{array}
$$

Since formula $\|x\|^2 < \gamma^2$ characterizes an open ball and $\delta < \gamma$ so antecedent $\|x\|^2 < \delta^2$ implies $\|x\|^2 < \gamma^2$ arithmetically, rule Enc is used to assume its closure $\|x\|^2 \leq \gamma^2$ in the domain constraint of the succedent ODE. With the strengthened domain, dC adds $\dot{v} \leq 0$ to the domain constraint using ⓑ, which is universally quantified over x.

$$
\cfrac{
\cfrac{
ⓒ, v < k \vdash [x' = f(x)\, \&\, \|x\|^2 \leq \gamma^2 \wedge \dot{v} \leq 0]\, \|x\|^2 < \gamma^2
}{
ⓑ, ⓒ, v < k \vdash [x' = f(x)\, \&\, \|x\|^2 \leq \gamma^2]\, \|x\|^2 < \gamma^2
}\text{\scriptsize dC}
}{
\delta{<}\gamma, ⓑ, ⓒ, \|x\|^2 < \delta^2, v < k \vdash [x' = f(x)]\, \|x\|^2 < \gamma^2
}\text{\scriptsize Enc}
$$

The proof continues using dC to add invariant $v < k$ to the domain constraint; this differential cut proves by $dI_{\succcurlyeq}$ using conjunct $\dot{v} \leq 0$ in the domain constraint. The subsequent dC step adds $\|x\|^2 \neq \gamma^2$ to the domain constraint using the contrapositive direction of the universally quantified antecedent ⓒ. Finally, a dW step completes the proof since conjuncts $\|x\|^2 \leq \gamma^2$ and $\|x\|^2 \neq \gamma^2$ in the resulting domain constraint imply the postcondition $\|x\|^2 < \gamma^2$ by $\mathbb{R}$.

$$
\begin{array}{c}
\cfrac{
\cfrac{
\cfrac{
\cfrac{*}{
\|x\|^2 \leq \gamma^2, \|x\|^2 \neq \gamma^2 \vdash \|x\|^2 < \gamma^2
}\text{\scriptsize $\mathbb{R}$}
}{
\vdash [x' = f(x)\, \&\, \|x\|^2 \leq \gamma^2 \wedge \cdots \wedge \|x\|^2 \neq \gamma^2]\, \|x\|^2 < \gamma^2
}\text{\scriptsize dW}
}{
ⓒ \vdash [x' = f(x)\, \&\, \|x\|^2 \leq \gamma^2 \wedge \dot{v} \leq 0 \wedge v < k]\, \|x\|^2 < \gamma^2
}\text{\scriptsize dC}
}{
ⓒ, v < k \vdash [x' = f(x)\, \&\, \|x\|^2 \leq \gamma^2 \wedge \dot{v} \leq 0]\, \|x\|^2 < \gamma^2
}\text{\scriptsize $dI_{\succcurlyeq}$, dC}
\end{array}
$$

The derivation of rule $\text{Lyap}_>$ starts with a cut that proves stability using rule $\text{Lyap}_\geq$ because the premises of $\text{Lyap}_>$ are identical to those of $\text{Lyap}_\geq$ except for a strict inequality requirement on the Lie derivative of v. The right conjunct of the right premise of $\text{Lyap}_>$ is cut and Skolemized with $\exists L$; the resulting antecedent is abbreviated with ⓔ $\equiv$ $\forall x \left(0 < \|x\|^2 \leq \gamma^2 \to \dot{v} < 0\right)$ below. Next, instantiating $\varepsilon = \gamma$ in the stability antecedent with $\forall L$ and Skolemizing

yields an initial disturbance $\delta > 0$ so that the ODE solution from states satisfying $\|x\|^2 < \delta^2$ always stay within the γ ball $\|x\|^2 < \gamma^2$. The resulting antecedent is abbreviated with $\textcircled{f} \equiv \forall x \left(\|x\|^2 < \delta^2 \to [x' = f(x)] \|x\|^2 < \gamma^2 \right)$.

$$
\begin{array}{c}
\cfrac{
\cfrac{
\cfrac{
\text{Stab}(x' = f(x)), \textcircled{e}, \delta > 0, \textcircled{f} \vdash \text{Attr}(x' = f(x))
}{
\text{Stab}(x' = f(x)), \gamma > 0, \textcircled{e} \vdash \text{Attr}(x' = f(x))
} \; \scriptstyle{\forall \text{L}, \exists \text{L}}
}{
\text{Stab}(x' = f(x)) \vdash \text{Attr}(x' = f(x))
} \; \scriptstyle{\text{cut}, \exists \text{L}}
}{
\vdash \text{AStab}(x' = f(x))
} \; \scriptstyle{\text{cut}, \text{Lyap}_\geq}
\end{array}
$$

The existential quantifier in the succedent is witnessed by δ with $\exists$R and the resulting sequent is simplified by Skolemization and instantiation of $\textcircled{f}$ (similar to $\text{Lyap}_\geq$) before axiom SAttr is used to further simplify the succedent using the stability assumption.

$$
\begin{array}{c}
\cfrac{
\cfrac{
\cfrac{
\cfrac{
\cfrac{
\textcircled{e}, [x' = f(x)] \|x\|^2 < \gamma^2, \varepsilon > 0 \vdash \langle x' = f(x) \rangle \|x\|^2 < \varepsilon^2
}{
\textcircled{e}, [x' = f(x)] \|x\|^2 < \gamma^2 \vdash \forall \varepsilon > 0 \, \langle x' = f(x) \rangle \|x\|^2 < \varepsilon^2
} \; \scriptstyle{\forall \text{R}}
}{
\text{Stab}(x' = f(x)), \textcircled{e}, [x' = f(x)] \|x\|^2 < \gamma^2 \vdash \text{Asym}(x' = f(x), x = 0)
} \; \scriptstyle{\text{SAttr}}
}{
\text{Stab}(x' = f(x)), \textcircled{e}, \textcircled{f}, \|x\|^2 < \delta^2 \vdash \text{Asym}(x' = f(x), x = 0)
} \; \scriptstyle{\forall \text{L}, \to \text{L}}
}{
\text{Stab}(x' = f(x)), \textcircled{e}, \textcircled{f} \vdash \forall x \left(\|x\|^2 < \delta^2 \to \text{Asym}(x' = f(x), x = 0) \right)
} \; \scriptstyle{\forall \text{R}, \to \text{R}}
}{
\text{Stab}(x' = f(x)), \textcircled{e}, \delta > 0, \textcircled{f} \vdash \text{Attr}(x' = f(x))
} \; \scriptstyle{\exists \text{R}}
\end{array}
$$

The remaining open premise is a liveness property which is proved using rule SP_c with the choice of compact staging set $S \equiv \varepsilon^2 \leq \|x\|^2 \leq \gamma^2$ and $p \equiv v$.

$$
\begin{array}{c}
\cfrac{
\cfrac{
\cfrac{
*
}{
\vdash [x' = f(x) \, \& \, \|x\|^2 \geq \varepsilon^2 \wedge \|x\|^2 < \gamma^2] S
} \; \scriptstyle{\text{dW}, \mathbb{R}}
}{
[x' = f(x)] \|x\|^2 < \gamma^2 \vdash [x' = f(x) \, \& \, \|x\|^2 \geq \varepsilon^2] S
} \; \scriptstyle{\text{dC}}
\qquad
\cfrac{
*
}{
\textcircled{e}, \varepsilon > 0, S \vdash \dot{v} < 0
}
}{
\textcircled{e}, [x' = f(x)] \|x\|^2 < \gamma^2, \varepsilon > 0 \vdash \langle x' = f(x) \rangle \|x\|^2 < \varepsilon^2
} \; \scriptstyle{\text{SP}_c}
\end{array}
$$

The left premise proves with a differential cut dC of the antecedent and dW, $\mathbb{R}$ from the resulting strengthened domain constraint $\|x\|^2 \geq \varepsilon^2 \wedge \|x\|^2 < \gamma^2$. The right premise proves using $\textcircled{e}$ with antecedents S and $\varepsilon > 0$ to prove its implication LHS. $\qquad\square$

Proof of Lemma 9. The quantifiers $\exists \alpha > 0 \, \exists \beta > 0 \, \exists \delta > 0 \, \forall x \left(\mathcal{U}_\delta(x = 0) \to \cdots \right)$ syntactically express the respective quantifiers in the definition of exponential stability from Def. 8 in dL. For an initial state satisfying $\mathcal{U}_\delta(x = 0)$, i.e., with $\|x(0)\| < \delta$, the assignment $y := \alpha^2 \|x\|^2$ sets the initial value of fresh variable y (before the ODE) to $\alpha^2 \|x(0)\|^2$. Let $x(t) : [0, T) \to \mathbb{R}^n$ and $y(t) : [0, T) \to \mathbb{R}$ respectively be the x and y projections of the unique, right-maximal solution of the ODE $x' = f(x), y' = -2\beta y$. By construction, the unique ODE solution for the y-coordinates is $y(t) = \alpha^2 \|x(0)\|^2 \exp(-2\beta t)$, so the postcondition $\|x\|^2 \leq y$ of the box modality expresses that for all times $0 \leq t < T$, $\|x(t)\|^2 \leq \alpha^2 \|x(0)\|^2 \exp(-2\beta t)$ or, equivalently, $\|x(t)\| \leq \alpha \|x(0)\| \exp(-\beta t)$, as required. $\qquad\square$

Proof of Lemma 10. The proof starts by instantiating the existentially quantified variables α, β in $\text{EStab}(x' = f(x))$ with $\alpha = \frac{k_2}{k_1}$ and decay rate $\beta = k_3$. Since k_1, k_2, k_3 are all positive constants, these choices satisfy $\alpha > 0, \beta > 0$.

$$
\cfrac{
\vdash \exists \delta > 0 \, \forall x \left(\|x\|^2 < \delta^2 \to [y := (\tfrac{k_2}{k_1})^2 \|x\|^2; x' = f(x), y' = -2k_3 y] \|x\|^2 \leq y \right)
}{
\vdash \text{EStab}(x' = f(x))
} \; \scriptstyle{\exists \text{R}}
$$

The subsequent cut step adds the premise of rule Lyap_E to the antecedents and Skolemizes it with $\exists$L. The resulting antecedent is abbreviated with $\textcircled{a} \equiv \forall x \left(\|x\|^2 \leq \gamma^2 \to k_1^2 \|x\|^2 \leq v \leq k_2^2 \|x\|^2 \wedge \dot{v} \leq -2k_3 v \right)$. Then $\exists$R instantiates the succedent with $\delta = \frac{k_1}{k_2} \gamma$ and the sequent is propositionally simplified. Note $\textcircled{a}$ also implies $k_1 \leq k_2$ as $k_1, k_2 > 0$ so $\delta \leq \gamma$ and $\|x\|^2 < \delta^2$ implies $\|x\|^2 < \gamma$ in real arithmetic. The hybrid program $y := (\tfrac{k_2}{k_1})^2 \|x\|^2; x' = f(x), y' = -2k_3 y$ is abbreviated with $\cdots$ in the first three steps.

$$
\begin{array}{c}
\cfrac{
\cfrac{
\cfrac{
\gamma > 0, \textcircled{a}, \|x\|^2 < (\tfrac{k_1}{k_2} \gamma)^2 \vdash [y := (\tfrac{k_2}{k_1})^2 \|x\|^2; x' = f(x), y' = -2k_3 y] \|x\|^2 \leq y
}{
\gamma > 0, \textcircled{a} \vdash \forall x \left(\|x\|^2 < (\tfrac{k_1}{k_2} \gamma)^2 \to [\cdots] \|x\|^2 \leq y \right)
} \; \scriptstyle{\to \text{R}, \to \text{L}}
}{
\gamma > 0, \textcircled{a} \vdash \exists \delta > 0 \, \forall x \left(\|x^2\| < \delta^2 \to [\cdots] \|x\|^2 \leq y \right)
} \; \scriptstyle{\exists \text{R}}
}{
\vdash \exists \delta > 0 \, \forall x \left(\|x^2\| < \delta^2 \to [\cdots] \|x\|^2 \leq y \right)
} \; \scriptstyle{\text{cut}, \exists \text{L}}
\end{array}
$$

The discrete assignment $y := (\frac{k_2}{k_1})^2\|x\|^2$ sets the value of variable y to $(\frac{k_2}{k_1})^2\|x\|^2$ initially. It is turned into an equational assumption with the assignment axiom [:=] of dL as follows (the axiom is omitted but can be found in the literature [Pla17, Pla18]).

$$[:=] \frac{\gamma > 0, \textcircled{a}, \|x\|^2 < (\frac{k_1}{k_2}\gamma)^2, y = (\frac{k_2}{k_1})^2\|x\|^2 \vdash [x' = f(x), y' = -2k_3y] \, \|x\|^2 \le y}{\gamma > 0, \textcircled{a}, \|x\|^2 < (\frac{k_1}{k_2}\gamma)^2 \vdash [y := (\frac{k_2}{k_1})^2\|x\|^2; x' = f(x), y' = -2k_3y] \, \|x\|^2 \le y}$$

The antecedents are abbreviated $\Gamma \equiv \gamma > 0, \textcircled{a}, \|x\|^2 < (\frac{k_1}{k_2}\gamma)^2, y = (\frac{k_2}{k_1})^2\|x\|^2$. The derivation continues with a differential cut dC adding formula $\|x\|^2 < \gamma^2$ to the domain constraint. This cut is abbreviated ① and proved further below. The next differential cut dC adds formula $v \le k_1^2 y$ to the domain constraint. This cut is abbreviated ② and also proved further below. The derivation is completed with a dW, ℝ step with the quantified antecedent ⓐ and the domain constraint, since they imply the chain of inequalities $k_1^2\|x\|^2 \le v \le k_1^2 y$, which implies the succedent (after dW) $\|x\|^2 \le y$ by ℝ.

$$
\begin{array}{c}
\text{dW} \cfrac{\text{ℝ} \cfrac{*}{\textcircled{a}, \|x\|^2 < \gamma^2, v \le k_1^2 y \vdash \|x\|^2 \le y}}{\text{dC} \cfrac{② \quad \Gamma \vdash [x' = f(x), y' = -2k_3y \, \& \, \|x\|^2 < \gamma^2 \wedge v \le k_1^2 y] \|x\|^2 \le y}{\text{dC} \cfrac{① \quad \Gamma \vdash [x' = f(x), y' = -2k_3y \, \& \, \|x\|^2 < \gamma^2] \|x\|^2 \le y}{\Gamma \vdash [x' = f(x), y' = -2k_3y] \|x\|^2 \le y}}}
\end{array}
$$

Returning to premise ①, the derivation uses Enc to assume $\|x\|^2 \le \gamma^2$ in the domain constraint, since $\|x\|^2 < \gamma^2$ is true initially. Then, a dC, dI$_\succcurlyeq$ step adds formula $v < k_1^2\gamma^2$ to the domain constraint. This formula is proved true initially by ℝ with antecedents Γ using the chain of inequalities from ⓐ, $v \le k_2^2\|x\|^2 < k_2^2\left(\frac{k_1}{k_2}\gamma\right)^2 = k_1^2\gamma^2$. It is proved invariant by dI$_\succcurlyeq$ because domain constraint $\|x\|^2 \le \gamma^2$ and quantified antecedent ⓐ proves the chain of inequalities $\dot{v} \le -2k_3v \le -2k_3(k_1^2\|x\|^2) \le 0$. A dW, ℝ step completes the proof because the domain constraint $\|x\|^2 \le \gamma^2 \wedge v < k_1^2\gamma^2$ and quantified antecedent ⓐ prove the chain of inequalities $k_1^2\|x\|^2 \le v < k_1^2\gamma^2$, which implies the succedent (after dW) $\|x\|^2 < \gamma^2$ by ℝ.

$$
\begin{array}{c}
\text{dW, ℝ} \cfrac{\cfrac{*}{\Gamma \vdash [x' = f(x), y' = -2k_3y \, \& \, \|x\|^2 \le \gamma^2 \wedge v < k_1^2\gamma^2] \|x\|^2 < \gamma^2}}{\text{dC, dI}_\succcurlyeq \cfrac{\Gamma \vdash [x' = f(x), y' = -2k_3y \, \& \, \|x\|^2 \le \gamma^2] \|x\|^2 < \gamma^2}{\text{Enc} \quad \Gamma \vdash [x' = f(x), y' = -2k_3y] \|x\|^2 < \gamma^2}}
\end{array}
$$

For premise ②, the inequality $k_1^2 y - v \ge 0$ is proved invariant using rule dbx$_\succcurlyeq$ with cofactor $g = -2k_3$ as follows.

$$
\begin{array}{c}
\text{dbx}_\succcurlyeq \cfrac{\text{ℝ}\cfrac{*}{\Gamma \vdash k_1^2 y - v \ge 0} \qquad \text{ℝ}\cfrac{*}{\textcircled{a}, \|x\|^2 < \gamma^2 \vdash -2k_1^2 k_3 y - \dot{v} \ge -2k_3(k_1^2 y - v)}}{\text{cut, M}[']\cfrac{\Gamma \vdash [x' = f(x), y' = -2k_3y \, \& \, \|x\|^2 < \gamma^2] k_1^2 y - v \ge 0}{\Gamma \vdash [x' = f(x), y' = -2k_3y \, \& \, \|x\|^2 < \gamma^2] v \le k_1^2 y}}
\end{array}
$$

The resulting left premise proves by ℝ because the antecedents ⓐ and $y = (\frac{k_2}{k_1})^2\|x\|^2$ in Γ prove the chain of inequalities $v \le k_2^2\|x\|^2 = k_1^2 y$. For the resulting right premise, the Lie derivative of $k_1^2 y - v$ from the LHS of the postcondition is $-2k_1^2 k_3 y - \dot{v}$. With domain constraint $\|x\|^2 < \gamma^2$ and quantified antecedent ⓐ, this derivative provably satisfies the chain of inequalities $-2k_1^2 k_3 y - \dot{v} \ge -2k_1^2 k_3 y + 2k_3 v = -2k_3(k_1^2 y - v)$ by ℝ. □

The following global stability definitions for an equilibrium point are motivated in Section 3.4. They are used in the proof of Lemma 11.

Definition 25 (Global stability [HC08, Kha92, RHL77]). *The origin $0 \in \mathbb{R}^n$ of ODE $x' = f(x)$ is **globally asymptotically stable** if it is stable and its region of attraction is the entire state space, i.e., for all $x = x(0) \in \mathbb{R}^n$, the right-maximal ODE solution $x(t) : [0, T) \to \mathbb{R}^n$ satisfies $\lim_{t \to T} x(t) = 0$. The origin is **globally exponentially stable** if there are positive constants $\alpha, \beta > 0$ such that for all initial states $x = x(0) \in \mathbb{R}^n$, the right-maximal ODE solution $x(t) : [0, T) \to \mathbb{R}^n$ satisfies $\|x(t)\| \le \alpha\|x(0)\| \exp(-\beta t)$ for all times $0 \le t < T$.*

Proof of Lemma 11. The proof is identical to Lemmas 4 and 9, respectively, except the existential quantification over a local neighborhood of the origin $\exists \delta > 0 \, \forall x \, (\mathcal{U}_\delta(x = 0) \to \cdots)$ is replaced by universal quantification over all initial states (where $P \equiv true$), i.e., $\forall x \, (true \to \cdots)$, as required by the global stability definitions. $\square$

Proof of Lemma 12. The rules are derived in order starting with rule $\text{Lyap}_>^{\text{G}}$. First, observe that the first two premises of rule $\text{Lyap}_>^{\text{G}}$ imply the premises of $\text{Lyap}_\geq$ because if the sign conditions on v and $\dot{v}$ are true globally, then they also hold for any choice of neighborhood of the origin. Thus, the derivation starts with a cut, $\text{Lyap}_\geq$ step which proves stability of the origin. Next, the definition of $\text{Attr}^{\text{P}}(x' = f(x), true)$ is logically unfolded and axiom SAttr is used to simplify the succedent, together with unfolding steps $\forall$R, $\to$R.

$$\cfrac{\cfrac{\cfrac{\cfrac{\varepsilon > 0 \vdash \langle x' = f(x) \rangle \|x\|^2 < \varepsilon^2}{\vdash \forall \varepsilon > 0 \, \langle x' = f(x) \rangle \|x\|^2 < \varepsilon^2} \text{\small $\forall$R, $\to$R}}{\text{Stab}(x' = f(x)) \vdash \text{Asym}(x' = f(x), true)} \text{\small SAttr}}{\text{Stab}(x' = f(x)) \vdash \text{Attr}^{\text{P}}(x' = f(x), true)} \text{\small $\forall$R, $\to$R}}{\vdash \text{Stab}(x' = f(x)) \wedge \text{Attr}^{\text{P}}(x' = f(x), true)} \text{\small cut, Lyap}_\geq$$

The derivation continues with a cut, $\mathbb{R}$, $\exists$L step, introducing a fresh Skolem variable b which stores the initial value of the Lyapunov function v. Next, a cut adds the box modality formula $[x' = f(x)] \, v \leq b$ to the antecedents. This cut proves by $\text{dI}_{\succcurlyeq}$ because formula $v \leq b$ is true initially and the premises of rule $\text{Lyap}_>^{\text{G}}$ prove the formula $\dot{v} \leq 0$.[8] The subsequent $\text{M}[']$ step strengthens the postcondition $v \leq b$ of the antecedent box modality to $\|x\|^2 < \gamma^2$ using the (Skolemized) rightmost premise of rule $\text{Lyap}_>^{\text{G}}$ (i.e., v is radially unbounded [HC08, Kha92]).

$$\cfrac{\cfrac{\cfrac{\varepsilon > 0, [x' = f(x)] \|x\|^2 < \gamma^2 \vdash \langle x' = f(x) \rangle \|x\|^2 < \varepsilon^2}{\varepsilon > 0, [x' = f(x)] v \leq b \vdash \langle x' = f(x) \rangle \|x\|^2 < \varepsilon^2} \text{\small M[']}}{\varepsilon > 0, v = b \vdash \langle x' = f(x) \rangle \|x\|^2 < \varepsilon^2} \text{\small cut, dI}_{\succcurlyeq}}{\varepsilon > 0 \vdash \langle x' = f(x) \rangle \|x\|^2 < \varepsilon^2} \text{\small cut, $\mathbb{R}$, $\exists$L}$$

Like the derivation of rule $\text{Lyap}_>$ in Lemma 6, the remaining open premise is an ODE liveness property which is proved using rule SP_c with the choice of compact staging set $S \equiv \varepsilon^2 \leq \|x\|^2 \leq \gamma^2$ and $p \equiv v$. The resulting left premise proves with a differential cut dC of the antecedent and dW. The resulting right premise proves using $\mathbb{R}$ from the middle premise of rule $\text{Lyap}_>^{\text{G}}$ and antecedents $\varepsilon > 0$, S.

$$\cfrac{\cfrac{*}{[x' = f(x)] \, \|x\|^2 < \gamma^2 \vdash [x' = f(x) \, \& \, \|x\|^2 \geq \varepsilon^2] S} \text{\small dC, dW} \qquad \cfrac{*}{\varepsilon > 0, S \vdash \dot{v} < 0} \text{\small $\mathbb{R}$}}{\varepsilon > 0, [x' = f(x)] \|x\|^2 < \gamma^2 \vdash \langle x' = f(x) \rangle \|x\|^2 < \varepsilon^2} \text{\small SP}_c$$

The derivation of rule $\text{Lyap}_{\text{E}}^{\text{G}}$ is similar to the derivation of rule Lyap_{E} from Lemma 10. The proof steps are repeated briefly. The derivation starts by instantiating (using $\exists$R) the existentially quantified variables in succedent $\text{EStab}^{\text{P}}(x' = f(x), true)$ with $\alpha = \frac{k_2}{k_1}$ and decay rate $\beta = k_3$, followed by logical unfolding of the sequent.

$$\cfrac{\cfrac{\cfrac{y = (\frac{k_2}{k_1})^2 \|x\|^2 \vdash [x' = f(x), y' = -2k_3 y] \, \|x\|^2 \leq y}{\vdash [y := (\frac{k_2}{k_1})^2 \|x\|^2; x' = f(x), y' = -2k_3 y] \, \|x\|^2 \leq y} \text{\small [:=]}}{\vdash \forall x \, \left(true \to [y := (\frac{k_2}{k_1})^2 \|x\|^2; x' = f(x), y' = -2k_3 y] \, \|x\|^2 \leq y \right)} \text{\small $\forall$R, $\to$R}}{\vdash \text{EStab}^{\text{P}}(x' = f(x), true)} \text{\small $\exists$R}$$

The proof continues with a differential cut of the formula $v \leq k_1^2 y$, which is proved invariant with its equivalent rephrasing $k_1^2 y - v \geq 0$ and rule $\text{dbx}_{\succcurlyeq}$ using cofactor $g = -2k_3$. Similar to Lemma 10, the cut formula is true initially because the antecedent $y = (\frac{k_2}{k_1})^2 \|x\|^2$ and the premise of $\text{Lyap}_{\text{E}}^{\text{G}}$ imply the chain of inequalities $v \leq k_2^2 \|x\|^2 = k_1^2 y$.

---

[8]When $x = 0$, the premise $f(0) = 0$ implies $\dot{v} = 0$.

The premise of $\text{Lyap}_\text{E}^\text{G}$ are also used to show that the Lie derivative of $k_1^2 y - v$ provably satisfies the chain of inequalities $-2k_1^2 k_3 y - \dot{v} \geq -2k_1^2 k_3 y + 2k_3 v = -2k_3(k_1^2 y - v)$. The proof is completed by dW, $\mathbb{R}$ using the premise of rule $\text{Lyap}_\text{E}^\text{G}$.

$$
\begin{array}{ll}
\mathbb{R} & \dfrac{*}{\vdash k_1^2 \|x\|^2 \leq v} \\[2pt]
\mathbb{R} & \dfrac{v \leq k_1^2 y \vdash \|x\|^2 \leq y}{} \\[2pt]
\text{dW} & \dfrac{}{\vdash [x' = f(x), y' = -2k_3 y \,\&\, v \leq k_1^2 y]\, \|x\|^2 \leq y} \\[2pt]
\text{dC} & \dfrac{}{y = (\frac{k_2}{k_1})^2 \|x\|^2 \vdash [x' = f(x), y' = -2k_3 y]\, \|x\|^2 \leq y}
\end{array}
$$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

Proof of Corollary 14. The two axioms are derived in order, starting with axiom EStabStab. The derivation of axiom EStabStab starts by Skolemizing the existential quantifiers in $\text{EStab}(x' = f(x))$ with $\exists \text{L}$, then Skolemizing the succedent ($\forall \text{R}$) and instantiating ($\exists \text{R}$) the existentially quantified $\delta > 0$ in the succedent with $\gamma = \min(\frac{\varepsilon}{\alpha}, \delta)$ (note $\gamma > 0$). The sequent is then simplified, noting that $\gamma \leq \delta$ so that assumption $\|x\|^2 < \gamma^2$ proves the implication LHS $\forall x\left(\|x\|^2 < \delta^2 \to \cdots\right)$ in the antecedents. The subformula with discrete assignment to y in the antecedent is abbreviated with $R_y \equiv [y := \alpha^2 \|x\|^2; x' = f(x), y' = -2\beta y]\,\|x\|^2 \leq y$.

$$
\begin{array}{ll}
 & \dfrac{\alpha > 0, \beta > 0, \delta > 0, \varepsilon > 0, R_y, \|x\|^2 < \gamma^2 \vdash [x' = f(x)]\,\|x^2\| < \varepsilon^2}{} \\[2pt]
\to\text{R}, \to\text{L} & \dfrac{\alpha > 0, \beta > 0, \delta > 0, \varepsilon > 0, \forall x\left(\|x\|^2 < \delta^2 \to R_y\right) \vdash \forall x\left(\|x\|^2 < \gamma^2 \to [x' = f(x)]\,\|x^2\| < \varepsilon^2\right)}{} \\[2pt]
\exists\text{R} & \dfrac{\alpha > 0, \beta > 0, \delta > 0, \varepsilon > 0, \forall x\left(\|x\|^2 < \delta^2 \to R_y\right) \vdash \exists \delta > 0\, \forall x\left(\|x\|^2 < \delta^2 \to [x' = f(x)]\,\|x\|^2 < \varepsilon^2\right)}{} \\[2pt]
\forall\text{R} & \dfrac{\alpha > 0, \beta > 0, \delta > 0, \forall x\left(\|x\|^2 < \delta^2 \to R_y\right) \vdash \text{Stab}(x' = f(x))}{} \\[2pt]
\exists\text{L} & \dfrac{\text{EStab}(x' = f(x)) \vdash \text{Stab}(x' = f(x))}{}
\end{array}
$$

The discrete assignment in antecedent R_y is unfolded with $[:=]$, similar to the proof of Lemma 10, yielding the antecedent $y = \alpha^2 \|x\|^2$ and abbreviated antecedent $P_y \equiv [x' = f(x), y' = -2\beta y]\,\|x\|^2 \leq y$. Axiom DG adds differential ghost $y' = -2\beta y$ to the succedent ODE and the postcondition is strengthened to $y < \varepsilon^2$ by K using assumption P_y. The proof is completed with a $\text{dbx}_\succcurlyeq$ step with cofactor term -2β because the (rephrased) postcondition $\varepsilon^2 - y > 0$ is proved by $\mathbb{R}$ from the antecedents with the chain of inequalities $y = \alpha^2 \|x\|^2 < \alpha^2 \gamma^2 \leq \alpha^2 (\frac{\varepsilon}{\alpha})^2 = \varepsilon^2$. The Lie derivative of $\varepsilon^2 - y$ is $2\beta y$ which provably satisfies the inequality $2\beta y \geq 2\beta y - 2\beta\varepsilon^2 = -2\beta(\varepsilon^2 - y)$ for $\beta > 0$.

$$
\begin{array}{ll}
\text{dbx}_\succcurlyeq & \dfrac{*}{\alpha > 0, \beta > 0, \delta > 0, \varepsilon > 0, y = \alpha^2 \|x\|^2, \|x\|^2 < \gamma^2 \vdash [x' = f(x), y' = -2\beta y]\, \varepsilon^2 - y > 0} \\[2pt]
\text{M}['] & \dfrac{\alpha > 0, \beta > 0, \delta > 0, \varepsilon > 0, y = \alpha^2 \|x\|^2, \|x\|^2 < \gamma^2 \vdash [x' = f(x), y' = -2\beta y]\, y < \varepsilon^2}{} \\[2pt]
\text{K} & \dfrac{\alpha > 0, \beta > 0, \delta > 0, \varepsilon > 0, y = \alpha^2 \|x\|^2, P_y, \|x\|^2 < \gamma^2 \vdash [x' = f(x), y' = -2\beta y]\, \|x^2\| < \varepsilon^2}{} \\[2pt]
\text{DG} & \dfrac{\alpha > 0, \beta > 0, \delta > 0, \varepsilon > 0, y = \alpha^2 \|x\|^2, P_y, \|x\|^2 < \gamma^2 \vdash [x' = f(x)]\, \|x^2\| < \varepsilon^2}{} \\[2pt]
[:=] & \dfrac{\alpha > 0, \beta > 0, \delta > 0, \varepsilon > 0, R_y, \|x\|^2 < \gamma^2 \vdash [x' = f(x)]\, \|x^2\| < \varepsilon^2}{}
\end{array}
$$

The derivation of axiom EStabAttr starts by unfolding and Skolemizing the existential quantifiers for the antecedent, with abbreviated ODE $\alpha_{xy} \equiv x' = f(x), y' = -2\beta y$ and subformula $R_y \equiv [y := \alpha^2 \|x\|^2; \alpha_{xy}]\,\|x\|^2 \leq y$ (identically to the preceding derivation for axiom EStabStab). The succedent is logically unfolded and the resulting antecedent P proves the implication LHS in the antecedent $\forall x\,(P \to R_y)$. Succedent $\text{Asym}(x' = f(x), x = 0)$ is then Skolemized with $\forall \text{R}$.[9] The subsequent step uses axioms DG, $\text{DG}_\forall$ to add the linear differential ghost $y' = -2\beta y$ to both ODEs in the succedent. The postcondition of the succedent diamond modality is monotonically strengthened with $\text{M}\langle'\rangle$ and postcondition $(y < \varepsilon^2 \wedge [\alpha_{xy}]\,\|x\|^2 \leq y)$. The two resulting premises are abbreviated ① and ②; they are shown and proved further below.

$$
\begin{array}{ll}
 & \qquad\qquad ① \qquad\quad ② \\[2pt]
\text{M}\langle'\rangle & \dfrac{\alpha > 0, \beta > 0, R_y \vdash \langle\alpha_{xy}\rangle[\alpha_{xy}]\,\|x\|^2 < \varepsilon^2}{} \\[2pt]
\text{DG}, \text{DG}_\forall & \dfrac{\alpha > 0, \beta > 0, R_y \vdash \langle x' = f(x)\rangle[x' = f(x)]\,\|x\|^2 < \varepsilon^2}{} \\[2pt]
\forall\text{R} & \dfrac{\alpha > 0, \beta > 0, R_y, P \vdash \text{Asym}(x' = f(x), x = 0)}{} \\[2pt]
\forall\text{L}, \to\text{L} & \dfrac{\alpha > 0, \beta > 0, \forall x\left(P \to R_y\right), P \vdash \text{Asym}(x' = f(x), x = 0)}{} \\[2pt]
\forall\text{R}, \to\text{R} & \dfrac{\alpha > 0, \beta > 0, \forall x\left(P \to R_y\right) \vdash \text{Attr}^\text{P}(x' = f(x), P)}{} \\[2pt]
\exists\text{L} & \dfrac{\text{EStab}^\text{P}(x' = f(x), P) \vdash \text{Attr}^\text{P}(x' = f(x), P)}{}
\end{array}
$$

---

[9]Unlike earlier proofs, the formula is *not* simplified using a stability assumption because the generalized formula $\text{EStab}^\text{P}(x' = f(x), P)$ does not directly imply stability of the origin unless formula P provably contains a neighborhood of the origin.

From premise ①, a differential cut dC proves formula $y < \varepsilon^2$ invariant for the succedent ODE α_{xy} using rule $\text{dbx}_{\succcurlyeq}$. The subsequent dC adds the postcondition of the antecedent to the domain constraint before dW, $\mathbb{R}$ finish the derivation.

$$
\begin{array}{ll}
\mathbb{R} & \dfrac{*}{y < \varepsilon^2 \wedge \|x\|^2 \le y \vdash \|x\|^2 < \varepsilon^2} \\[2pt]
\text{dW} & \dfrac{}{\vdash [\alpha_{xy} \,\&\, y < \varepsilon^2 \wedge \|x\|^2 \le y] \, \|x\|^2 < \varepsilon^2} \\[2pt]
\text{dC} & \dfrac{}{[\alpha_{xy}] \|x\|^2 \le y \vdash [\alpha_{xy} \,\&\, y < \varepsilon^2] \, \|x\|^2 < \varepsilon^2} \\[2pt]
\text{dC, dbx}_{\succcurlyeq} & \dfrac{}{\beta > 0,\, y < \varepsilon^2,\, [\alpha_{xy}] \|x\|^2 \le y \vdash [\alpha_{xy}] \, \|x\|^2 < \varepsilon^2}
\end{array}
$$

From premise ②, the antecedent R_y is unfolded with $[:=]$, then $\text{K}\langle\&\rangle$, $\text{D}[;]$ remove the right conjunct of the postcondition because postcondition $[\alpha_{xy}] \|x\|^2 \le y$ is true after all runs of α_{xy}. Axiom BDG removes the ODEs for x in the succedent because $\|x\|^2$ is bounded using antecedent $[\alpha_{xy}] \|x\|^2 \le y$.

$$
\begin{array}{ll}
\text{BDG} & \dfrac{\beta > 0 \vdash \langle y' = -2\beta y \rangle y < \varepsilon^2}{\beta > 0,\, [\alpha_{xy}] \|x\|^2 \le y \vdash \langle \alpha_{xy} \rangle y < \varepsilon^2} \\[2pt]
\text{K}\langle\&\rangle,\, \text{D}[;] & \dfrac{}{\beta > 0,\, [\alpha_{xy}] \|x\|^2 \le y \vdash \langle \alpha_{xy} \rangle \big(y < \varepsilon^2 \wedge [\alpha_{xy}] \|x\|^2 \le y \big)} \\[2pt]
[:=] & \dfrac{}{\beta > 0,\, R_y \vdash \langle \alpha_{xy} \rangle \big(y < \varepsilon^2 \wedge [\alpha_{xy}] \|x\|^2 \le y \big)}
\end{array}
$$

The remaining open premise is an ODE liveness property for variable y. Its proof starts by introducing a fresh variable y_0 storing the initial value of y. Then, rule SP_c is used with $S \equiv \big(\varepsilon^2 \le y \le y_0 \big)$. The resulting left premise is an invariance property of the ODE which proves using $\text{M}[']$, $\text{dI}_{\succcurlyeq}$, while the right premise proves by $\mathbb{R}$.

$$
\begin{array}{ll}
\text{dI}_{\succcurlyeq} & \dfrac{*}{\beta > 0,\, y = y_0 \vdash [y' = -2\beta y \,\&\, y \ge \varepsilon^2] y \le y_0} \\[2pt]
\text{M}['] & \dfrac{}{\beta > 0,\, y = y_0 \vdash [y' = -2\beta y \,\&\, y \ge \varepsilon^2] S} \qquad \mathbb{R}\dfrac{*}{\beta > 0,\, S \vdash -2\beta y < 0} \\[2pt]
\text{SP}_c & \dfrac{}{\beta > 0,\, y = y_0 \vdash \langle y' = -2\beta y \rangle y < \varepsilon^2} \\[2pt]
\text{cut, } \exists\text{L} & \dfrac{}{\beta > 0 \vdash \langle y' = -2\beta y \rangle y < \varepsilon^2}
\end{array} \qquad \square
$$

B.2 Proofs for General Stability

This section derives proof rules for general stability and its specialized instances which are introduced and motivated in Section 4.

Proof of Lemma 15. The derivation of rule GLyap generalizes the ideas behind the derivation of rule $\text{Lyap}_{\ge}$. The derivation starts with an $\forall\text{R}$ step, followed by a cut and Skolemization $\exists\text{L}$ of the second (bottom) premise of rule GLyap. The resulting assumptions (for Skolem variables γ, δ, k) are abbreviated with: ⓐ $\equiv \forall x \, (\partial(\mathcal{U}_\gamma(R)) \to v \ge k)$, ⓑ $\equiv \forall x \, (\mathcal{U}_\delta(P) \to R \vee v < k)$, and ⓒ $\equiv \forall x \, \big(R \vee v < k \to [x' = f(x) \,\&\, \overline{\mathcal{U}_\gamma(R)}](R \vee v < k)\big)$. A subsequent $\text{M}[']$ step strengthens the postcondition monotonically since the formula $\mathcal{U}_\gamma(R) \to \mathcal{U}_\varepsilon(R)$ is provable by $\mathbb{R}$ for $\gamma \le \varepsilon$.

$$
\begin{array}{ll}
\text{M}['],\, \mathbb{R} & \dfrac{0 < \gamma,\, 0 < \delta \le \gamma,\, ⓐ,\, ⓑ,\, ⓒ \vdash \exists \delta > 0 \, \forall x \, \big(\mathcal{U}_\delta(P) \to [x' = f(x)] \mathcal{U}_\gamma(R)\big)}{0 < \gamma \le \varepsilon,\, 0 < \delta \le \gamma,\, ⓐ,\, ⓑ,\, ⓒ \vdash \exists \delta > 0 \, \forall x \, \big(\mathcal{U}_\delta(P) \to [x' = f(x)] \mathcal{U}_\varepsilon(R)\big)} \\[2pt]
\text{cut, } \exists\text{L} & \dfrac{}{\varepsilon > 0 \vdash \exists \delta > 0 \, \forall x \, \big(\mathcal{U}_\delta(P) \to [x' = f(x)] \mathcal{U}_\varepsilon(R)\big)} \\[2pt]
\forall\text{R} & \dfrac{}{\vdash \text{Stab}_\text{R}^\text{P}(x' = f(x), P, R)}
\end{array}
$$

The existentially quantified δ in the succedent is witnessed with the Skolem variable δ in the antecedents and the sequent is simplified with $\forall\text{R}$, $\to\text{R}$, $\to\text{L}$, where the implication LHS in ⓑ is proved.

$$
\begin{array}{ll}
\forall\text{R},\, \to\text{R},\, \to\text{L} & \dfrac{0 < \gamma,\, 0 < \delta \le \gamma,\, ⓐ,\, ⓒ,\, \mathcal{U}_\delta(P),\, R \vee v < k \vdash [x' = f(x)] \mathcal{U}_\gamma(R)}{0 < \gamma,\, 0 < \delta \le \gamma,\, ⓐ,\, ⓑ,\, ⓒ \vdash \forall x \, \big(\mathcal{U}_\delta(P) \to [x' = f(x)] \mathcal{U}_\gamma(R)\big)} \\[2pt]
\exists\text{R} & \dfrac{}{0 < \gamma,\, 0 < \delta \le \gamma,\, ⓐ,\, ⓑ,\, ⓒ \vdash \exists \delta > 0 \, \forall x \, \big(\mathcal{U}_\delta(P) \to [x' = f(x)] \mathcal{U}_\gamma(R)\big)}
\end{array}
$$

The derivation continues with rule Enc to assume the closure formula $\overline{\mathcal{U}_\gamma(R)}$ in the domain constraint. This step uses the first premise of rule GLyap, i.e., precondition P implies postcondition R, so that the neighborhood formula

$\mathcal{U}_\delta(P)$ provably implies neighborhood formula $\mathcal{U}_\gamma(R)$ initially by $\mathbb{R}$ for $\delta \leq \gamma$. The subsequent dC step uses the antecedent ⓒ to prove the invariance of formula $R \vee v{<}k$ for the ODE $x' = f(x) \,\&\, \overline{\mathcal{U}_\gamma(R)} \wedge (R \vee v{<}k)$ and adds it to the domain constraint. The derivation is completed using dW, $\mathbb{R}$, where the arithmetic premise is justified below.

$$
\begin{array}{c}
\mathbb{R} \dfrac{*}{0{<}\gamma, ⓐ, \overline{\mathcal{U}_\gamma(R)}, (R \vee v{<}k) \vdash \mathcal{U}_\gamma(R)} \\
\text{dW} \dfrac{}{0{<}\gamma, ⓐ, R \vee v{<}k \vdash [x' = f(x) \,\&\, \overline{\mathcal{U}_\gamma(R)} \wedge (R \vee v{<}k)]\,\mathcal{U}_\gamma(R)} \\
\text{dC} \dfrac{}{0{<}\gamma, ⓐ, ⓒ, R \vee v{<}k \vdash [x' = f(x) \,\&\, \overline{\mathcal{U}_\gamma(R)}]\,\mathcal{U}_\gamma(R)} \\
\text{Enc} \dfrac{}{0{<}\gamma, 0{<}\delta{\leq}\gamma, ⓐ, ⓒ, \mathcal{U}_\delta(P), R \vee v{<}k \vdash [x' = f(x)]\,\mathcal{U}_\gamma(R)}
\end{array}
$$

To prove arithmetical premise $0{<}\gamma, ⓐ, \overline{\mathcal{U}_\gamma(R)}, R \vee v{<}k \vdash \mathcal{U}_\gamma(R)$, note that the left disjunct R in the antecedent implies its neighborhood formula $\mathcal{U}_\gamma(R)$ in real arithmetic for $\gamma > 0$. Thus, it suffices to justify the premise for the right disjunct, i.e., $ⓐ, \overline{\mathcal{U}_\gamma(R)}, v{<}k \vdash \mathcal{U}_\gamma(R)$. Antecedent ⓐ is instantiated to obtain assumption $\partial(\mathcal{U}_\gamma(R)) \to v \geq k$. This assumption says that the right disjunct $v < k$ does *not* occur on the boundary of $\partial(\mathcal{U}_\gamma(R))$ which, together with antecedent $\overline{\mathcal{U}_\gamma(R)}$ implies succedent $\mathcal{U}_\gamma(R)$ in real arithmetic. $\square$

The following set stability definitions are standard [HC08, Kha92], except (compared to the literature) the following definitions do *not* assume any topological properties of the set characterized by formula P. The motivation for additional topological restrictions is explained in Corollary 18.

Definition 26 (Set stability [HC08, Kha92]). *Let* $\mathrm{dist}(x, P)$ *denote the distance of a point* $x \in \mathbb{R}^n$ *to the set characterized by formula* P. *The set characterized by formula* P *is*

- ***stable*** *if, for all* $\varepsilon{>}0$, *there exists* $\delta{>}0$ *such that for all initial states* $x = x(0)$ *with* $\mathrm{dist}(x, P) < \delta$, *the right-maximal ODE solution* $x(t) : [0, T) \to \mathbb{R}^n$ *satisfies* $\mathrm{dist}(x(t), P) < \varepsilon$ *for all times* $0 \leq t < T$,

- ***attractive*** *if there exists* $\delta{>}0$ *such that for all initial states* $x = x(0)$ *with* $\mathrm{dist}(x, P) < \delta$, *the right-maximal ODE solution* $x(t) : [0, T) \to \mathbb{R}^n$ *satisfies the limit* $\lim_{t \to T} \mathrm{dist}(x(t), P) = 0$,

- ***asymptotically stable*** *if it is stable and attractive,*

- ***globally asymptotically stable*** *if it is stable and for all initial states* $x = x(0) \in \mathbb{R}^n$, *the right-maximal ODE solution* $x(t) : [0, T) \to \mathbb{R}^n$ *satisfies the limit* $\lim_{t \to T} \mathrm{dist}(x(t), P) = 0$.

The set stability definitions are formalized in dL in Lemma 16.

Proof of Lemma 16. Like Lemma 4, the correctness of these definitions is immediate from the semantics of dL formulas because these definitions directly syntactically express the definitions in dL. For $\varepsilon > 0$, the neighborhood formula $\mathcal{U}_\varepsilon(P)$ characterizes the set of points $x \in \mathbb{R}^n$ within distance ε from P, i.e., $\mathrm{dist}(x, P) < \varepsilon$. Formula $\mathrm{Asym}(x' = f(x), P)$ syntactically expresses the limit $\lim_{t \to T} \mathrm{dist}(x(t), P) = 0$ for the right-maximal ODE solution $x(t) : [0, T) \to \mathbb{R}^n$, as shown in the proof of Lemma 4. $\square$

Proof of Corollary 18. The three axioms are derived in order.

SetSAttr The two directions of the inner equivalence of SetSAttr are proved separately. The easier "$\to$" direction follows by Skolemizing ε in the succedent with $\forall$R, choosing the same ε in the antecedent with $\forall$L, and then by M$\langle' \rangle$ because the resulting postcondition $[x' = f(x)]\,\mathcal{U}_\varepsilon(P)$ monotonically implies postcondition $\mathcal{U}_\varepsilon(P)$ by differential skip DX.

$$
\begin{array}{c}
\text{DX} \dfrac{*}{[x' = f(x)]\,\mathcal{U}_\varepsilon(P) \vdash \mathcal{U}_\varepsilon(P)} \\
\text{M}\langle'\rangle \dfrac{}{\langle x' = f(x)\rangle [x' = f(x)]\,\mathcal{U}_\varepsilon(P) \vdash \langle x' = f(x)\rangle \mathcal{U}_\varepsilon(P)} \\
\forall\text{R}, \forall\text{L} \dfrac{}{\mathrm{Asym}(x' = f(x), P) \vdash \forall\varepsilon{>}0 \,\langle x' = f(x)\rangle \mathcal{U}_\varepsilon(P)}
\end{array}
$$

The more interesting "←" direction uses the stability assumption. The first step Skolemizes the succedent with ∀R, then the stability antecedent is instantiated with ∀L and Skolemized with ∃L (yielding fresh Skolem variable δ). Using the resulting quantified assumption $\forall x \left(\mathcal{U}_\delta(P) \to [x' = f(x)]\mathcal{U}_\varepsilon(P)\right)$, the postcondition of the succedent is monotonically strengthened to $\mathcal{U}_\delta(P)$ with M⟨′⟩. The derivation is completed by ∀L instantiating the remaining quantified antecedent with δ.

$$
\begin{array}{ll}
\forall \text{L} & \cfrac{\cfrac{*}{\delta > 0, \forall \varepsilon > 0 \langle x' = f(x)\rangle \mathcal{U}_\varepsilon(P) \vdash \langle x' = f(x)\rangle \mathcal{U}_\delta(P)}}{\begin{array}{l}
\text{M}\langle'\rangle \quad \cfrac{\delta > 0, \forall x \left(\mathcal{U}_\delta(P) \to [x' = f(x)]\mathcal{U}_\varepsilon(P)\right), \forall \varepsilon > 0 \langle x' = f(x)\rangle \mathcal{U}_\varepsilon(P) \vdash \langle x' = f(x)\rangle [x' = f(x)]\mathcal{U}_\varepsilon(P)}{\begin{array}{l}
\forall \text{L}, \exists \text{L} \quad \cfrac{\text{Stab}_\text{R}^\text{P}(x' = f(x), P, P), \forall \varepsilon > 0 \langle x' = f(x)\rangle \mathcal{U}_\varepsilon(P), \varepsilon > 0 \vdash \langle x' = f(x)\rangle [x' = f(x)]\mathcal{U}_\varepsilon(P)}{\forall \text{R} \quad \text{Stab}_\text{R}^\text{P}(x' = f(x), P, P), \forall \varepsilon > 0 \langle x' = f(x)\rangle \mathcal{U}_\varepsilon(P) \vdash \text{Asym}(x' = f(x), P)}}
\end{array}}
\end{array}
$$

SClosure This axiom is derived immediately by equivalently rewriting with arithmetic equivalences because for $\delta > 0$ the open neighborhood formulas $\mathcal{U}_\delta(P)$ and $\mathcal{U}_\delta(\overline{P})$ are provably equivalent in real arithmetic by ℝ.

SClosed This axiom is proved by contradiction so its derivation starts by negating the invariance succedent using ⟨·⟩.

$$
\begin{array}{ll}
\langle\cdot\rangle, \neg\text{R} & \cfrac{\text{Stab}_\text{R}^\text{P}(x' = f(x), P, P), P, \langle x' = f(x)\rangle \neg P \vdash \textit{false}}{\cfrac{\text{Stab}_\text{R}^\text{P}(x' = f(x), P, P), P \vdash [x' = f(x)]P}{\forall\text{R}, \to\text{R} \quad \text{Stab}_\text{R}^\text{P}(x' = f(x), P, P) \vdash \forall x \left(P \to [x' = f(x)]P\right)}}
\end{array}
$$

Since formula P characterizes a closed set, every point satisfying $\neg P$ must be contained in some $\varepsilon > 0$ ball in the interior of the open set characterized by $\neg P$. Accordingly, these points are $\varepsilon > 0$ distance away from the set characterized by P and therefore, the formula $\neg P \leftrightarrow \exists \varepsilon > 0 \neg \mathcal{U}_\varepsilon(P)$ is provable in real arithmetic. This equivalence is used to rewrite the postcondition of the diamond modality antecedent before the resulting existentially quantified variable ε is commuted with the diamond modality and Skolemized with B′, ∃L and V to extract the constant assumption $\varepsilon > 0$.

$$
\begin{array}{ll}
\langle\cdot\rangle & \cfrac{\cfrac{*}{[x' = f(x)]\mathcal{U}_\varepsilon(P), \langle x' = f(x)\rangle \neg \mathcal{U}_\varepsilon(P) \vdash \textit{false}}}{\begin{array}{l}
\forall\text{L}, \to\text{L} \cfrac{\delta > 0, \forall x \left(\mathcal{U}_\delta(P) \to [x' = f(x)]\mathcal{U}_\varepsilon(P)\right), P, \langle x' = f(x)\rangle \neg \mathcal{U}_\varepsilon(P) \vdash \textit{false}}{\begin{array}{l}
\forall\text{L}, \exists\text{L} \cfrac{\text{Stab}_\text{R}^\text{P}(x' = f(x), P, P), P, \varepsilon > 0, \langle x' = f(x)\rangle \neg \mathcal{U}_\varepsilon(P) \vdash \textit{false}}{\begin{array}{l}
\text{V} \cfrac{\text{Stab}_\text{R}^\text{P}(x' = f(x), P, P), P, \langle x' = f(x)\rangle \left(\varepsilon > 0 \wedge \neg \mathcal{U}_\varepsilon(P)\right) \vdash \textit{false}}{\begin{array}{l}
\text{B}', \exists\text{L} \cfrac{\text{Stab}_\text{R}^\text{P}(x' = f(x), P, P), P, \langle x' = f(x)\rangle \exists \varepsilon > 0 \neg \mathcal{U}_\varepsilon(P) \vdash \textit{false}}{\text{M}\langle'\rangle, \mathbb{R} \quad \text{Stab}_\text{R}^\text{P}(x' = f(x), P, P), P, \langle x' = f(x)\rangle \neg P \vdash \textit{false}}
\end{array}}
\end{array}}
\end{array}}
\end{array}
$$

The stability assumption is instantiated with ε using ∀L and Skolemized with ∃L. Since the formula $P \to \mathcal{U}_\delta(P)$ is provable in real arithmetic for $\delta > 0$, the implication LHS in the antecedents is proved with ∀L, →L. The proof is completed using ⟨·⟩ since the resulting box and diamond modality antecedents are contradictory. □

Proof of Lemma 19. Rule SLyap$^*_\geq$ is derived first before SLyap$_\geq$ and SLyap$_>$ are derived from SLyap$^*_\geq$ as corollaries further below. The derivation of rule SLyap$^*_\geq$ starts with a GLyap step. The (left) resulting premise $\overline{P} \to P$ proves trivially and is not shown below. For the (right) resulting premise, the first two conjuncts under the nested quantifiers prove trivially from a cut of the second (bottom) premise of rule SLyap$^*_\geq$. It remains to prove the final conjunct for fresh Skolem variable k with antecedent abbreviated ⓐ $\equiv \forall x \left(\overline{\mathcal{U}_\gamma(P)} \wedge \neg P \to \dot{v} \leq 0\right)$ from the premise of SLyap$^*_\geq$.

$$
\begin{array}{ll}
\text{cut} & \cfrac{\text{ⓐ}, P \vee v < k \vdash [x' = f(x) \,\&\, \overline{\mathcal{U}_\gamma(P)}](P \vee v < k)}{\begin{array}{l}
\vdash \forall \varepsilon > 0 \, \exists 0 < \gamma \leq \varepsilon \, \exists k \left(\begin{array}{l}
\forall x \left(\partial(\mathcal{U}_\gamma(P)) \to v \geq k\right) \wedge \\
\exists 0 < \delta \leq \gamma \, \forall x \left(\mathcal{U}_\delta(P) \to P \vee v < k\right) \wedge \\
\forall x \left(P \vee v < k \to [x' = f(x) \,\&\, \overline{\mathcal{U}_\gamma(P)}](P \vee v < k)\right)
\end{array}\right)
\end{array}}
\\
\text{GLyap} & \cfrac{}{\vdash \text{Stab}_\text{R}^\text{P}(x' = f(x), P, P)}
\end{array}
$$

The derivation continues using rule DCC to prove that $v < k$ is true along ODE solutions until the invariant P is entered; the first step uses an equivalent propositional rephrasing of $P \vee v < k$ as $\neg P \to v < k$. The two resulting premises are abbreviated ① and ② and continued below.

$$\text{DCC} \frac{\text{①} \qquad \text{②}}{\text{ⓐ}, \neg P \to v < k \vdash [x' = f(x) \,\&\, \overline{\mathcal{U}_\gamma(P)}](\neg P \to v < k)}$$
$$\text{cut, M[}'\text{]} \frac{}{\text{ⓐ}, P \vee v{<}k \vdash [x' = f(x) \,\&\, \overline{\mathcal{U}_\gamma(P)}](P \vee v{<}k)}$$

From premise ①, a DX step strengthens the antecedent to $v < k$ using the domain constraint $\neg P$. Rule $\text{dI}_{\succcurlyeq}$ completes the proof because formula $\dot{v} \le 0$ proves from antecedent ⓐ with domain $\overline{\mathcal{U}_\gamma(P)} \wedge \neg P$.

$$\frac{*}{\text{ⓐ}, \overline{\mathcal{U}_\gamma(P)} \wedge \neg P \vdash \dot{v} \le 0}$$
$$\text{dI}_{\succcurlyeq} \frac{}{\text{ⓐ}, v < k \vdash [x' = f(x) \,\&\, \overline{\mathcal{U}_\gamma(P)} \wedge \neg P]v < k}$$
$$\text{DX} \frac{}{\text{ⓐ}, \neg P \to v < k \vdash [x' = f(x) \,\&\, \overline{\mathcal{U}_\gamma(P)} \wedge \neg P]v < k}$$

From premise ②, a dW step reduces the premise to an invariance question for formula P (since $\neg\neg P$ is equivalent to P). The DMP step weakens the domain constraint, which proves using the first premise of rule $\text{SLyap}^*_{\ge}$.

$$\frac{*}{P \vdash [x' = f(x)]P}$$
$$\text{DMP} \frac{}{P \vdash [x' = f(x) \,\&\, \overline{\mathcal{U}_\gamma(P)}]P}$$
$$\text{dW} \frac{}{\vdash [x' = f(x) \,\&\, \overline{\mathcal{U}_\gamma(P)}](\neg\neg P \to [x' = f(x) \,\&\, \overline{\mathcal{U}_\gamma(P)}]\neg\neg P)}$$

Rule $\text{SLyap}_{\ge}$ derives from $\text{SLyap}^*_{\ge}$ because the two rules share the invariance premise on P and the latter two premises of rule $\text{SLyap}_{\ge}$ imply the latter premise of $\text{SLyap}^*_{\ge}$ in real arithmetic when P characterizes a compact set. The variable γ is witnessed by ε in the premise after $\text{SLyap}^*_{\ge}$. The proof of the arithmetic premise is explained below.

$$\mathbb{R} \frac{*}{\varepsilon > 0 \vdash \left(\exists k \left(\begin{array}{c} \forall x\, (\partial(\mathcal{U}_\varepsilon(P)) \to v \ge k) \wedge \\ \exists 0 < \delta \le \varepsilon\, \forall x\, (\mathcal{U}_\delta(P) \wedge \neg P \to v < k) \end{array} \right) \wedge \\ \forall x\, (\overline{\mathcal{U}_\varepsilon(P)} \wedge \neg P \to \dot{v} \le 0) \right)}$$
$$\forall\text{R},\ \exists\text{R} \frac{}{\vdash \forall \varepsilon > 0\, \exists 0 < \gamma \le \varepsilon \left(\exists k \left(\begin{array}{c} \forall x\, (\partial(\mathcal{U}_\gamma(P)) \to v \ge k) \wedge \\ \exists 0 < \delta \le \gamma\, \forall x\, (\mathcal{U}_\delta(P) \wedge \neg P \to v < k) \end{array} \right) \wedge \\ \forall x\, (\overline{\mathcal{U}_\gamma(P)} \wedge \neg P \to \dot{v} \le 0) \right)}$$
$$\text{SLyap}^*_{\ge} \frac{}{\vdash \text{Stab}^P_R(x' = f(x), P, P)}$$

The conjunct $\forall x\, (\overline{\mathcal{U}_\varepsilon(P)} \wedge \neg P \to \dot{v} \le 0)$ proves logically from the right conjunct of the middle premise of rule $\text{SLyap}_{\ge}$. For the existentially quantified conjunct, $\exists k\, (\cdots)$, since formula P characterizes a compact set, the boundary $\partial(\mathcal{U}_\varepsilon(P))$ is also compact and therefore the continuous Lyapunov function v must attain its minimum k on that set. This k witnesses the quantifier $\exists k$, and note that $k > 0$ from the left conjunct of the middle premise of rule $\text{SLyap}_{\ge}$. From the rightmost premise of rule $\text{SLyap}_{\ge}$, the Lyapunov function satisfies $v \le 0$ for all points $x \in \mathbb{R}^n$ on the boundary characterized by formula ∂P. For each such point on the boundary, by continuity, there is a radius $\delta > 0$ where points in the open ball $\|x\| < \delta$ satisfy $v < k$ because $k > 0$. The union of all such balls over all points on the boundary is an open cover of the compact boundary which therefore has a finite subcover. The minimum radius $\delta > 0$ of balls in this finite subcover witnesses the formula $\exists 0 < \delta \le \varepsilon\, \forall x\, (\mathcal{U}_\delta(P) \wedge \neg P \to v < k)$, justifying the use of $\mathbb{R}$.

Rule $\text{SLyap}_{>}$ is derived from rule $\text{SLyap}_{\ge}$ similar to the derivation of $\text{Lyap}_{>}$ from $\text{Lyap}_{\ge}$. The derivation starts with a cut of the set stability formula $\text{Stab}^{\overline{P}}_R(x' = f(x), P, P)$ which proves by $\text{SLyap}_{\ge}$ because rules $\text{SLyap}_{>}$

and $\text{SLyap}_\geq$ have identical premises except for a strict inequality on $\dot{v}$.

$$\text{cut, SLyap}_\geq \frac{\text{Stab}_R^P(x' = f(x), P, P) \vdash \exists\delta{>}0\ \text{Attr}_R^P(x' = f(x), \mathcal{U}_\delta(P), P)}{\vdash \text{Stab}_R^P(x' = f(x), P, P) \wedge \exists\delta{>}0\ \text{Attr}_R^P(x' = f(x), \mathcal{U}_\delta(P), P)}$$

The stability antecedent is instantiated with $\varepsilon = 1$; the positive constant 1 is chosen arbitrarily to obtain a neighborhood in which solutions are trapped. After Skolemization, this yields an initial disturbance $\delta > 0$ and the antecedent $\forall x \left(\mathcal{U}_\delta(P) \to [x' = f(x)]\,\mathcal{U}_1(P) \right)$. The succedent is witnessed with δ, and the resulting sequent is simplified with $\forall$R, $\to$R, $\to$L. Then, axiom SetSAttr simplifies the succedent using the stability antecedent.

$$
\begin{array}{c}
\text{SetSAttr} \cfrac{\delta{>}0, [x' = f(x)]\,\mathcal{U}_1(P), \mathcal{U}_\delta(P) \vdash \forall\varepsilon{>}0\ \langle x' = f(x)\rangle\,\mathcal{U}_\varepsilon(P)}{\text{Stab}_R^P(x' = f(x), P, P), \delta{>}0, [x' = f(x)]\,\mathcal{U}_1(P), \mathcal{U}_\delta(P) \vdash \text{Asym}(x' = f(x), P)} \\
\forall\text{R}, \to\text{R}, \to\text{L}\ \cfrac{}{\text{Stab}_R^P(x' = f(x), P, P), \delta{>}0, \forall x\left(\mathcal{U}_\delta(P) \to [x' = f(x)]\,\mathcal{U}_1(P)\right) \vdash \text{Attr}_R^P(x' = f(x), \mathcal{U}_\delta(P), P)} \\
\exists\text{R}\ \cfrac{}{\text{Stab}_R^P(x' = f(x), P, P), \delta{>}0, \forall x\left(\mathcal{U}_\delta(P) \to [x' = f(x)]\,\mathcal{U}_1(P)\right) \vdash \exists\delta{>}0\ \text{Attr}_R^P(x' = f(x), \mathcal{U}_\delta(P), P)} \\
\text{cut, }\exists\text{L}\ \cfrac{}{\text{Stab}_R^P(x' = f(x), P, P) \vdash \exists\delta{>}0\ \text{Attr}_R^P(x' = f(x), \mathcal{U}_\delta(P), P)}
\end{array}
$$

The proof of the liveness property in the open premise uses rule SP_c with the choice of compact staging set $S \equiv \overline{\mathcal{U}_1(P)} \wedge \neg\mathcal{U}_\varepsilon(P)$ and $p \equiv v$. Note that formula S characterizes a compact set because P is compact so conjuncts $\overline{\mathcal{U}_1(P)}$ and $\neg\mathcal{U}_\varepsilon(P)$ are both closed and $\overline{\mathcal{U}_1(P)}$ is bounded.

$$
\begin{array}{c}
\text{dC, dW}\cfrac{*}{[x' = f(x)]\,\mathcal{U}_1(P) \vdash [x' = f(x)\,\&\,\neg\mathcal{U}_\varepsilon(P)]\,S} \qquad \mathbb{R}\cfrac{*}{\varepsilon{>}0, S \vdash \dot{v} < 0} \\
\text{SP}_c\ \cfrac{}{\delta{>}0, [x' = f(x)]\,\mathcal{U}_1(P), \mathcal{U}_\delta(P), \varepsilon{>}0 \vdash \langle x' = f(x)\rangle\,\mathcal{U}_\varepsilon(P)} \\
\forall\text{R}\ \cfrac{}{\delta{>}0, [x' = f(x)]\,\mathcal{U}_1(P), \mathcal{U}_\delta(P) \vdash \forall\varepsilon{>}0\ \langle x' = f(x)\rangle\,\mathcal{U}_\varepsilon(P)}
\end{array}
$$

The left premise proves with a cut dC of the antecedent and dW. The right premise proves by real arithmetic $\mathbb{R}$ using the middle premise of rule $\text{SLyap}_>$ because the antecedents imply $\neg P$. $\square$

The following definition of ε-stability is standard [GKD$^+$19], except the first quantification over $\gamma > \varepsilon$ is strict whereas in the original definition [GKD$^+$19] it is $\gamma \geq \varepsilon$. This difference is immaterial for the purpose of ε-stability as ε is a numerical parameter for the radius of a ball around which disturbances to the origin are to be ignored. In particular, an ODE ε-stable by the following definition is $\alpha\varepsilon$-stable for any $\alpha \in (0, 1)$ by its original definition [GKD$^+$19].

Definition 27 (Epsilon-Stability [GKD$^+$19])**.** *The origin* $0 \in \mathbb{R}^n$ *of ODE* $x' = f(x)$ *is* ε-***stable*** *for a positive constant* $\varepsilon > 0$ *if for all* $\gamma > \varepsilon$, *there exists* $\delta > 0$ *such that for points* $x = x(0)$ *with* $\|x\| < \delta$, *the right-maximal ODE solution* $x(t) : [0, T) \to \mathbb{R}^n$ *satisfies* $\|x(t)\| < \gamma$ *for all times* $0 \leq t < T$.

Proof of Lemma 21. The formula $\text{Stab}_R^P(x' = f(x), x = 0, \mathcal{U}_\varepsilon(x = 0))$ is valid iff for all $\gamma > 0$, there exists $\delta > 0$ such that for points $x = x(0)$ with $\|x\| < \delta$, the right-maximal ODE solution $x(t) : [0, T) \to \mathbb{R}^n$ satisfies $\|x(t)\| < \varepsilon + \gamma$ for all times $0 \leq t < T$, where the neighborhood $\mathcal{U}_\gamma(\mathcal{U}_\varepsilon(x = 0))$ is equivalently characterized by $\|x\|^2 < \gamma + \varepsilon$. This unfolded semantics is equivalent to the mathematical definition of ε-stability in Def. 27 by reindexing the universal quantifier with $\gamma \mapsto \gamma + \varepsilon$ instead. $\square$

C   Counterexamples

This appendix provides counterexamples for the soundness issues highlighted in Sections 4 and 5. The first counterexample illustrates the need to assume compactness, i.e., formula P is closed *and bounded* in rule $\text{SLyap}_\geq$. The remark after [Kha92, Definition 8.1] suggests that the following variant of $\text{SLyap}_\geq$ is sound for formulas P that characterize a closed, invariant set:

$$\text{SLyap}_\geq \text{\Lightning}\ \frac{P \vdash v = 0 \qquad \neg P \vdash v > 0 \wedge \dot{v} \leq 0}{\vdash \text{Stab}_R^P(x' = f(x), P, P)}$$

The rule $\text{SLyap}_\geq\text{\Lightning}$ is unsound (indicated by $\text{\Lightning}$); indeed, the rule $\text{SLyap}_\geq$ from Lemma 19 is also unsound if the assumption that formula P characterizes a bounded set is omitted.
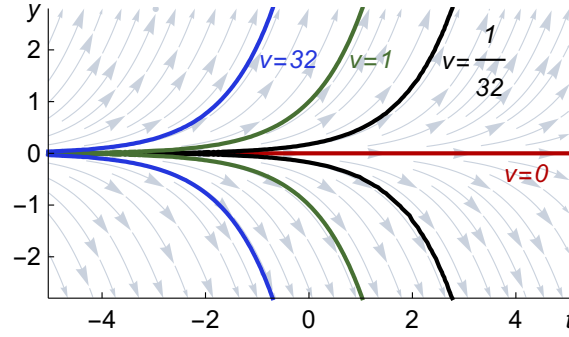
Figure 4: An illustration of α_c and the Lyapunov function v from Counterexample 28, with level curves (where $v = k$ for various k) shown in color.

Counterexample 28. Consider the ODE $\alpha_c \equiv y' = y, t' = 1$ and the formula $P \equiv y = 0$ which characterizes a closed invariant set of α_c that is *not bounded*. The Lyapunov function $v = y^2 \exp(-2t)$, satisfies all of the premises of rule SLyap$_\geq$⚡ because $v = 0$ when $y = 0$, $v > 0$ for $y \neq 0$, and $\dot{v} = 0$. However, P is not stable for ODE α_c, as can be seem from Fig. 4. The norm of the right-maximal solution from all initial states that satisfy $y \neq 0$ approach ∞.

This counterexample also illustrates the importance of the boundedness assumption for formula P in Lemma 19 for rule SLyap$_\geq$ since all other premises of the rule are satisfied by the above example.

The second counterexample below shows that rule Lyap$_\geq$ crucially needs the premise $v(0) = 0$. This premise is unsoundly omitted from the arithmetical conditions in [APA20, Equation 1].

Counterexample 29. Consider the ODE $y' = y$ with solution $y(t) = y_0 \exp(t)$ from initial value $y(0) = y_0$. For all perturbed initial states $y_0 \neq 0$, $\|y(t)\|$ approaches ∞ as $t \to \infty$ so this ODE is not stable (nor attractive). However, the Lyapunov function $v = 1$ trivially satisfies all of the premises of rule Lyap$_\geq$ except the omitted premise $v(0) = 0$.