

# Verifying Switched System Stability With Logic

Anonymous Author(s)

## ABSTRACT

Switched systems are known to exhibit subtle (in)stability behaviors requiring system designers to carefully analyze the stability of closed-loop systems that arise from their proposed switching control laws. This paper presents a formal approach for verifying switched system stability that blends classical ideas from the controls and verification literature using differential dynamic logic (dL), a logic for deductive verification of hybrid systems. From controls, we use standard stability notions for various classes of switching mechanisms and their corresponding Lyapunov function-based analysis techniques. From verification, we use dL's ability to verify quantified properties of hybrid systems and dL models of switched systems as looping hybrid programs whose stability can be formally specified and proven by finding appropriate *loop invariants*, i.e., properties that are preserved across each loop iteration. This blend of ideas enables a trustworthy implementation of switched system stability verification in the KeYmaera X prover based on dL. For standard classes of switching mechanisms, the implementation provides fully automated stability proofs, including searching for suitable Lyapunov functions. Moreover, the generality of the deductive approach also enables verification of switching control laws that require non-standard stability arguments through the design of loop invariants that suitably express specific intuitions behind those control laws. This flexibility is demonstrated on three case studies: a model for longitudinal flight control by Branicky, an automatic cruise controller, and Brockett's nonholonomic integrator.

## CCS CONCEPTS

• **Theory of computation** → **Logic and verification**; **Timed and hybrid models**; • **Computing methodologies** → *Computational control theory*; • **Computer systems organization** → *Embedded systems*.

## KEYWORDS

switched system stability, loop invariants, differential dynamic logic

## ACM Reference Format:

Anonymous Author(s). 2021. Verifying Switched System Stability With Logic. In *Proceedings of ACM Conference (Conference'17)*. ACM, New York, NY, USA, 19 pages. <https://doi.org/10.1145/nnnnnnnn.nnnnnnnn>

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](mailto:permissions@acm.org).

Conference'17, July 2017, Washington, DC, USA

© 2021 Association for Computing Machinery.

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM...\$15.00

<https://doi.org/10.1145/nnnnnnnn.nnnnnnnn>

## 1 INTRODUCTION

Switched systems provide a powerful mathematical paradigm for the design and analysis of discontinuous (or nondifferentiable) control mechanisms [10, 22, 28, 44]. Examples of such mechanisms include: bang-bang controllers that switch between on/off modes; gain schedulers that switch between a family of locally valid linear controllers; and supervisory control, where a supervisor switches between candidate controllers based on logical criteria [22, 28]. However, switched systems are known to exhibit subtle (in)stability behaviors, e.g., switching between stable subsystems can lead to instability [22], so it is important for system designers to adequately justify the stability of their proposed switching designs. Verification and validation are complementary approaches for such justifications: *validation* approaches, such as system simulations or lab experiments, allow designers to check that their models and controllers conform to real world behavior; *verification* approaches yield formal mathematical proofs that the stability properties hold for *all* possible switching decisions everywhere in the model's infinite state space, not just for finitely-many simulated trajectories.

This paper presents a logic-based, deductive approach for verifying switched system stability under various classes of switching mechanisms. The key insight is that control-theoretic stability arguments for switching control can be formally justified by blending techniques from discrete program verification with continuous differential equations analysis using differential dynamic logic (dL), a logic for deductive verification of hybrid systems [33, 34]. Intuitively, switched systems are modeled in dL as looping *hybrid programs* [46], as in the following snippet ( $\{\cdot\}^*$  denotes repetition):

```
{    u := ctrl(x);    // switching controller (discrete dynamics)
    x' = f_u(x)      // actuate decision (continuous dynamics)
}*@invariant( ... ) // switching loop with invariant annotation
```

Accordingly, switched system stability is formally specified in dL as first-order quantified safety properties of such loops (Section 2.2), and these safety properties can then be proved rigorously by combining fundamental ideas from verification and control, namely: *i*) identification of *loop invariants* (@invariant above), i.e., properties of the (discrete) loop that are preserved across all executions of the loop body, *ii*) *compositional verification* for separately analyzing the discrete and continuous dynamics of the loop body, and *iii*) *Lyapunov functions*, i.e., auxiliary energy functions that enable stability analysis for the continuous dynamics.

Section 3 identifies key loop invariants underlying stability arguments for various classes of switching mechanisms and derives sound stability proof rules for those mechanisms. Crucially, these *syntactic derivations* are built from dL's sound foundations for hybrid program reasoning [33, 34], *without* the need to introduce new mathematical concepts such as non-classical weak solutions or nondifferentiable Lyapunov functions [9, 16]. Section 4 uses these derivations to implement support for switched systems in the KeYmaera X prover based on dL [12], including a modeling interface

for switched systems, automatic search for Lyapunov function candidates, and sound verification of switched system stability specifications. Notably, the implementation requires *no extensions* to KeYmaera X's soundness-critical core and thereby directly inherits all of KeYmaera X's correctness guarantees [12, 25]. This trustworthiness is necessary for computer-aided verification of complex, controlled switching designs, where the number of correctness conditions on their Lyapunov functions scales quadratically with the number of switching modes (Section 3.2), making pen-and-paper proofs error-prone or infeasible. Section 5 further applies the deductive approach on three case studies, chosen because each require subtle twists to standard switched system stability arguments:

- *Longitudinal flight control* [4]: This model is parametric (5 parameters, 2 state variables) and its stability justification due to Branicky [4] uses a “noncustomary” Lyapunov function [10], whose correctness requires intricate arithmetic reasoning. The proof is enabled through the use of *ghost switching* where virtual switching modes are introduced for the sake of the stability analysis, similar to the use of ghost variables in program verification [30, 34, 35].
- *Automatic cruise control* [29]: This hybrid automaton switches between several operating modes, e.g., standard/emergency braking, accelerating, and PI control, based on specific guard conditions. Lyapunov function candidates can be numerically generated [26], but must be corrected for soundness.
- *Brockett's nonholonomic integrator* [7]: A large class of control systems can be transformed to the nonholonomic integrator but this system is not stabilizable by continuous feedback [7, 22]. Instead, the system must be initially controlled into a suitable region where a stabilizing control law can be applied. The stability argument must show that the initial control mode does not destabilize the system.

These case studies are verified semi-automatically in KeYmaera X, with user guidance to design and prove modified loop invariants that suitably capture the specific intuitions behind their respective control laws. The flexibility and generality of this paper's deductive approach enables such modifications while ensuring that the overall stability argument remains valid. In fact, these modified stability proofs enjoy exactly the same, strong correctness guarantees thanks to their formalization within the uniform dL logical foundations.

All proofs are in the appendix. The KeYmaera X implementation, examples, and case studies are available at:<sup>1</sup>

<https://figshare.com/s/00b273eb0a5fc61c175d>

## 2 BACKGROUND

This section briefly recalls switched systems and their hybrid program models introduced by Tan and Platzer [46]. The section then explains how stability for these models can be formally specified and verified using differential dynamic logic (dL) [33, 34].

### 2.1 Switched Systems as Hybrid Programs

**2.1.1 Hybrid Programs.** The language of *hybrid programs* is generated by the following grammar, where  $x$  is a variable,  $e$  is a dL

<sup>1</sup>While an artifact will be submitted for artifact evaluation if this paper is accepted according to the guidelines for regular papers, we already provide a double-blind anonymized link to a prototype implementation for interested reviewers now.

term, and  $Q$  is a formula of first-order real arithmetic [33, 34].

$$\alpha, \beta ::= x' = f(x) \ \& \ Q \mid x := e \mid ?Q \mid \alpha; \beta \mid \alpha \cup \beta \mid \alpha^*$$

Continuous dynamics are modeled using systems of ordinary differential equations (ODEs)  $x' = f(x) \ \& \ Q$  evolving within domain  $Q$ ; the ODE is written as  $x' = f(x)$  when there is no domain constraint, i.e.,  $Q \equiv \text{true}$ . Discrete dynamics are modeled using assignments ( $x := e$  assigns the value of term  $e$  to  $x$ ) and tests ( $?Q$  checks whether condition  $Q$  is true in the current state). The program combinators are used to piece together sub-programs to form programs with hybrid dynamics; the combinators are: sequential composition ( $\alpha; \beta$  runs  $\alpha$  followed by  $\beta$ ), nondeterministic choice ( $\alpha \cup \beta$  runs  $\alpha$  or  $\beta$  nondeterministically), and nondeterministic repetition ( $\alpha^*$  repeats  $\alpha$  for any number of iterations).

Throughout this paper,  $x = (x_1, \dots, x_n)$  denotes the vector of continuous state variables for the system under consideration. Other variables are used for program auxiliaries, e.g., to describe memory and timing components of switching controllers.

**2.1.2 Switched systems.** A *switched system* is described by a finite family  $\mathcal{P}$  of ODEs  $x' = f_p(x)$ ,  $p \in \mathcal{P}$  and a set of *switching signals*  $\sigma : [0, \infty) \rightarrow \mathcal{P}$  that prescribe the ODE  $x' = f_{\sigma(t)}(x)$  to follow at time  $t$  along the system's evolution. Tan and Platzer [46] use hybrid programs as formal models for various classes of switching mechanisms; one example is *arbitrary switching* [22], where the system is allowed to follow *any* switching signal, i.e., it switches arbitrarily (at any time) between the ODEs  $x' = f_p(x)$ ,  $p \in \mathcal{P}$ . This can be used to model real world systems whose switching behavior is uncontrolled or *a priori* unknown. Arbitrary switching is modeled by the hybrid program  $\alpha_{\text{arb}}$  [46, Proposition 1]:

$$\alpha_{\text{arb}} \equiv \left( \bigcup_{p \in \mathcal{P}} x' = f_p(x) \right)^* \quad (1)$$

The behavior of program  $\alpha_{\text{arb}}$  is analogous to a computer simulation of arbitrary switching: on each iteration, the program makes a (discrete) nondeterministic choice of switching decision  $\bigcup_{p \in \mathcal{P}} (\cdot)$  to select an ODE  $x' = f_p(x)$  which it then follows continuously for some duration before repeating the simulation loop.

The hybrid programs language can be used to model various other classes of switching mechanisms [22, 46], including general *controlled switching*, as illustrated in Section 1, where a (discrete) control law  $u := \text{ctrl}(x)$  decides the ODE  $x' = f_u(x)$  to switch to on each loop iteration. Stability for these models is explained next.

### 2.2 Stability as Quantified Loop Safety

This paper studies *uniform global pre-asymptotic stability* (UGpAS) for switched systems [16, 17, 22], defined as follows:

**Definition 1** (UGpAS [16, 17]). Let  $\Phi(x)$  denote the set of all (domain-obeying) solutions<sup>2</sup>  $\varphi : [0, T_\varphi] \rightarrow \mathbb{R}^n$  for a switched system from state  $x \in \mathbb{R}^n$ . The origin  $0 \in \mathbb{R}^n$  is:

- **uniformly globally pre-asymptotically stable** if the system is uniformly stable and uniformly globally pre-attractive,
- **uniformly stable** if, for all  $\varepsilon > 0$ , there exists  $\delta > 0$  such that from all initial states  $x \in \mathbb{R}^n$  with  $\|x\| < \delta$ , all solutions  $\varphi \in \Phi(x)$  satisfy  $\|\varphi(t)\| < \varepsilon$  for all times  $0 \leq t \leq T_\varphi$ , and

<sup>2</sup>A formal construction of the (right-maximal) solution  $\phi$  for a given switching signal  $\sigma$  is available elsewhere [46, Appendix A].

- **uniformly globally pre-attractive** if, for all  $\varepsilon > 0, \delta > 0$ , there exists  $T \geq 0$  such that from all initial states  $x \in \mathbb{R}^n$  with  $\|x\| < \delta$ , all solutions  $\varphi \in \Phi(x)$  satisfy  $\|\varphi(t)\| < \varepsilon$  for all times  $T \leq t \leq T_\varphi$ .

The UGpAS definition can be understood intuitively for a system with a switching control mechanism:

- *stability* means the mechanism keeps the system close to the origin if the system is initially perturbed close to the origin,
- *global pre-attractivity* means the mechanism drives the system to the origin asymptotically as  $t \rightarrow \infty$ , and
- *uniform* means the stability and pre-attractivity properties are independent of both the nondeterminism in the switching mechanism (e.g., arbitrary switching) and the choice of initial states satisfying  $\|x\| < \delta$ ; for brevity in subsequent sections, “uniform” is elided when describing stability properties.

*Remark 1.* Switched systems whose solutions are all uniformly bounded in time, i.e., there exists  $T_m$  such that for all solutions  $\varphi$ ,  $T_\varphi \leq T_m$ , are trivially pre-attractive. Goebel et al. [16, 17] introduce the notion of *pre-attractivity* as opposed to *attractivity* for hybrid systems because it separates considerations about whether a hybrid system’s solutions are *complete*, i.e., solutions exist for all (forward) time, from conditions for stability and attractivity. Indeed, it is common in the hybrid and switched systems literature to either *ignore* incomplete solutions or *assume* the models under consideration only have complete solutions [22, 26, 49]. Instead of predicating proofs on these hypotheses, this paper formalizes the (weaker) notion of UGpAS for switched systems directly.

The definition of UGpAS nests alternating quantification over real numbers with temporal quantification over the solutions  $\varphi$  of switched systems. This combination of quantifiers can be expressed formally using the formula language of dL [33, 34], whose grammar is shown below,  $\sim \in \{=, \neq, \geq, >, \leq, <\}$  is a comparison operator between dL terms  $e, \tilde{e}$  and  $\alpha$  is a hybrid program:

$$\phi, \psi ::= e \sim \tilde{e} \mid \phi \wedge \psi \mid \phi \vee \psi \mid \neg \phi \mid \forall v \phi \mid \exists v \phi \mid [\alpha] \phi \mid \langle \alpha \rangle \phi$$

This grammar extends the first-order language of real arithmetic ( $\text{FOL}_{\mathbb{R}}$ ) with the box  $[\alpha]\phi$  and diamond  $\langle \alpha \rangle \phi$  modality formulas which express that all or some runs of hybrid program  $\alpha$  satisfy postcondition  $\phi$ , respectively. Real arithmetic  $\text{FOL}_{\mathbb{R}}$  is decidable by quantifier elimination [47] and serves as a useful base specification language. Various specifications are equivalently definable in  $\text{FOL}_{\mathbb{R}}$ , e.g., Euclidean norm bounds  $\|x\| \sim \varepsilon \stackrel{\text{def}}{=} \|x\|^2 \sim \varepsilon^2$  (for  $\varepsilon \geq 0$ ) and topological operations such as the boundary  $\partial \phi$  and closure  $\bar{\phi}$  of the set characterized by formula  $\phi$  [3].

The box modality formula  $[\alpha]\phi$  expresses *safety* properties  $\phi$  of program  $\alpha$  that must hold along all of its executions [34]. When  $\alpha$  models a switched system, the box modality quantifies (uniformly) over all times for all solutions arising from the switching mechanism. Accordingly, UGpAS for switched systems is formally specified by nesting the box modality with the first-order quantifiers.

**LEMMA 2 (UGPAS IN DIFFERENTIAL DYNAMIC LOGIC).** *The origin  $0 \in \mathbb{R}^n$  for a switched system modeled by program  $\alpha$  is UGpAS iff the dL formula  $\text{UGPAS}(\alpha)$  is valid. Variables  $\varepsilon, \delta, T, t$  are fresh in  $\alpha$ :*

$$\text{UGPAS}(\alpha) \equiv \text{UStab}(\alpha) \wedge \text{UGpAttr}(\alpha)$$

$$\text{UStab}(\alpha) \equiv \forall \varepsilon > 0 \exists \delta > 0 \forall x (\|x\| < \delta \rightarrow [\alpha] \|x\| < \varepsilon)$$

$$\text{UGpAttr}(\alpha) \equiv \forall \varepsilon > 0 \forall \delta > 0 \exists T \geq 0 \forall x (\|x\| < \delta \rightarrow$$

$$[t := 0; \alpha, t' = 1] (t \geq T \rightarrow \|x\| < \varepsilon))$$

Here,  $\text{UStab}(\alpha)$  and  $\text{UGpAttr}(\alpha)$  characterize stability and global pre-attractivity of  $\alpha$ , respectively. In  $\text{UGpAttr}(\alpha)$ ,  $\alpha, t' = 1$  denotes the hybrid program obtained from  $\alpha$  by augmenting its continuous dynamics so that variable  $t$  tracks the progression of time.

Formulas  $\text{UStab}(\alpha)$  and  $\text{UGpAttr}(\alpha)$  syntactically formalize in dL the corresponding quantifiers in Def. 1. In  $\text{UGpAttr}(\alpha)$ , the fresh clock variable  $t$  is initialized to 0 and syntactically tracks the progression of time along switched system solutions. The program  $\alpha, t' = 1$  can, e.g., be constructed by adding a clock ODE  $t' = 1$  to all ODEs in the switched system model  $\alpha$ . Accordingly, the postcondition  $t \geq T \rightarrow \|x\| < \varepsilon$  expresses that the system state norm is bounded by  $\varepsilon$  after  $T$  time units along any switching trajectory, as required in Def. 1. Various other stability notions are of interest in the continuous and hybrid systems literature [13, 17, 22, 29, 36, 44, 45]. These variations can also be formally specified in dL [45] but are left out of scope for this paper.

## 2.3 Proof Calculus

The dL proof calculus enables formal, deductive verification of UGpAS stability specifications through compositional reasoning principles for hybrid programs [33, 34] and a complete axiomatization for ODE invariants [35]. For example, an important syntactic tool for differential equations reasoning is the *Lie derivative* of term  $e$  along ODE  $x' = f(x)$ , defined as  $\mathcal{L}_f(e) \stackrel{\text{def}}{=} \nabla e \cdot f$ . The sound calculation and manipulation of Lie derivatives is enabled in dL through the use of syntactic differentials [33].

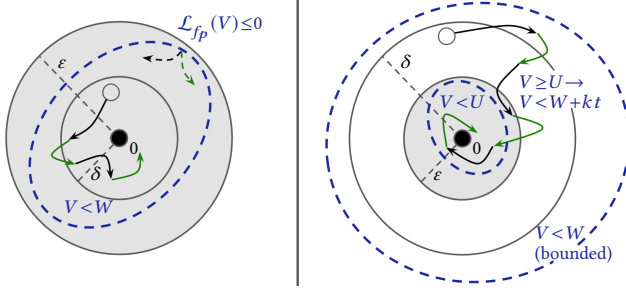
All proofs are presented in a classical sequent calculus with the usual rules for manipulating logical connectives and sequents. The semantics of *sequent*  $\Gamma \vdash \phi$  is equivalent to the formula  $(\bigwedge_{\psi \in \Gamma} \psi) \rightarrow \phi$  and a sequent is *valid* iff its corresponding formula is valid. The key (derived) dL proof rule used in this paper is:

$$\text{loop} \frac{\Gamma \vdash \text{Inv} \quad \text{Inv} \vdash [\alpha] \text{Inv} \quad \text{Inv} \vdash \phi}{\Gamma \vdash [\alpha^*] \phi}$$

The loop rule says that, in order to prove validity of the conclusion (below the rule bar), it suffices to prove the three premises (above the rule bar), respectively from left to right: *i*) the initial assumptions  $\Gamma$  imply  $\text{Inv}$ , *ii*)  $\text{Inv}$  is preserved across the loop body  $\alpha$ , i.e.,  $\text{Inv}$  is a *loop invariant* for  $\alpha^*$ , and *iii*)  $\text{Inv}$  implies the postcondition  $\phi$ . The identification of loop invariants  $\text{Inv}$  is crucial for formal proofs of UGpAS, as illustrated by the following deductive proof skeleton for stability (a similar skeleton is used for pre-attractivity):

$$\text{Deduction} \quad \frac{\begin{array}{c} \vdots \\ \Gamma \vdash \text{Inv} \end{array} \quad \frac{\begin{array}{c} \vdots \\ \text{Inv} \vdash [\alpha] \text{Inv} \end{array} \quad \frac{\begin{array}{c} \vdots \\ \text{Inv} \vdash \|x\| < \varepsilon \end{array}}{\Gamma \vdash [\alpha^*] \|x\| < \varepsilon} \quad \frac{\begin{array}{c} \vdots \\ \vdots \end{array} \quad \frac{\begin{array}{c} \vdots \\ \vdots \end{array}}{\vdash \text{UStab}(\alpha^*)}}{\vdash \text{UStab}(\alpha^*)}$$





**Figure 1: Loop invariants for UGPAS (arbitrary switching), stability (left) and pre-attractivity (right). Switching trajectories are illustrated by alternating black and green arrows.**

Proofs proceed upwards by deduction, where each reasoning step is justified by sound dL axioms and rules of inference, e.g., the loop rule. The skeleton above syntactically *derives* a proof rule that reduces a stability proof for  $\alpha^*$  to proofs of the top-most premises,  $\Gamma_1 \vdash \phi_1 \cdots \Gamma_k \vdash \phi_k$ , which corresponding to required logical and arithmetical conditions on Lyapunov functions for various switching mechanisms. The loop invariant step (highlighted in red) crucially ties together these conditions on Lyapunov functions and hybrid program reasoning for switched systems.

### 3 LOOP INVARIANTS FOR SWITCHED SYSTEM STABILITY

This section identifies loop invariants for proving UGPAS under various classes of switching mechanisms with Lyapunov functions [5, 21, 22]; relevant mathematical arguments are presented briefly, see Appendix A for more details. Throughout the section, loop invariants are progressively tweaked to account for new design insights behind increasingly complex switching mechanisms.

#### 3.1 Arbitrary and State-Dependent Switching

**3.1.1 Arbitrary Switching.** Stability for the arbitrary switching model  $\alpha_{arb}$  from (1) can be verified by finding a so-called *common Lyapunov function*  $V$  for all of the ODEs  $x' = f_p(x), p \in \mathcal{P}$  satisfying the following arithmetical conditions [22, 44]:

- i)  $V(0) = 0$  and  $V(x) > 0$  for all  $\|x\| > 0$ ,
- ii)  $V$  is *radially unbounded*, i.e., for all  $b$ , there exists  $\gamma > 0$  such that  $\|x\| < \gamma$  for all  $V(x) \leq b$ , and
- iii) for each ODE  $x' = f_p(x), p \in \mathcal{P}$ , the Lie derivative  $\mathcal{L}_{f_p}(V)$  satisfies:  $\mathcal{L}_{f_p}(V)(0) = 0$  and  $\mathcal{L}_{f_p}(V)(x) < 0$  for all  $\|x\| > 0$ .

Conditions i)–iii) are generalizations of well-known conditions for stability of ODEs [8, 21] to arbitrary switching. Intuitively, conditions i) and iii) ensure that  $V$  acts as an auxiliary energy function whose value decreases asymptotically to zero (at the origin) along all switching trajectories of the system; the radial unboundedness condition ii) ensures that this argument applies to all system states for *global* pre-attractivity [21]. Correctness of these conditions can be proved in dL using loop invariants, see Fig. 1 (explained below).

**Stability.** The specification  $\text{UStab}(\alpha_{arb})$  requires that all trajectories of  $\alpha_{arb}$  stay in the grey ball  $\|x\| < \varepsilon$ , starting from a chosen ball  $\|x\| < \delta$ , see Fig. 1 (left). Condition i) guarantees that the ball

$\|x\| < \varepsilon$  contains a sublevel set of the Lyapunov function satisfying  $V < W$  (dashed blue curve) and this sublevel set contains a smaller ball  $\|x\| < \delta$  [8, 21]. Condition iii) shows that this sublevel set is invariant for each ODE  $x' = f_p(x), p \in \mathcal{P}$  because  $\mathcal{L}_{f_p}(V)(x) \leq 0$ , as illustrated by the dashed black and green arrows for two different switching choices  $p \in \mathcal{P}$  both locally pointing inwards to the boundary of the sublevel set. Thus, the formula  $\text{Inv}_s \equiv \|x\| < \varepsilon \wedge V < W$ , which characterizes the blue sublevel set, is an invariant for all possible switching choices in the loop body of  $\alpha_{arb}$ , which makes  $\text{Inv}_s$  a suitable loop invariant for  $\text{UStab}(\alpha_{arb})$ .

**Pre-attractivity.** The specification  $\text{UGPAttr}(\alpha_{arb})$  requires that all trajectories of  $\alpha_{arb}$  stay in the grey ball  $\|x\| < \varepsilon$  after a chosen time  $T$ , starting from the initial ball  $\|x\| < \delta$ , see Fig. 1 (right). The ball  $\|x\| < \delta$  is compact, i.e., contained in a sublevel set satisfying  $V < W$  for some  $W > 0$  (outer dashed blue curve); this sublevel set is bounded by condition ii). Like the stability argument, condition i) guarantees that there is a sublevel set  $V < U$  (inner dashed blue curve) contained in the ball  $\|x\| < \varepsilon$ , and condition iii) shows that both sublevel sets characterized by  $V < W$  and  $V < U$  are invariants for every ODE in the loop body of  $\alpha_{arb}$ . The set characterized by formula  $V \geq U \wedge V \leq W$  is compact and bounded away from the origin, which implies by condition iii) that there is a uniform bound  $k < 0$  on this set, where for each ODE  $x' = f_p(x), p \in \mathcal{P}$ ,  $\mathcal{L}_{f_p}(V)(x) \leq k$ . Thus, the value of Lyapunov function  $V$  decreases at rate  $k$ , regardless of switching choices in the loop body of  $\alpha_{arb}$ , as long as it has not entered  $V < U$ . The loop invariant for  $\text{UGPAttr}(\alpha_{arb})$  syntactically expresses this intuition:  $\text{Inv}_a \equiv V < W \wedge (V \geq U \rightarrow V < W + kt)$ . For a sufficiently large choice of  $T$  with  $W + kT \leq U$ , trajectories at time  $t \geq T$  satisfy  $V < U$  so they are contained in the  $\|x\| < \varepsilon$  ball.

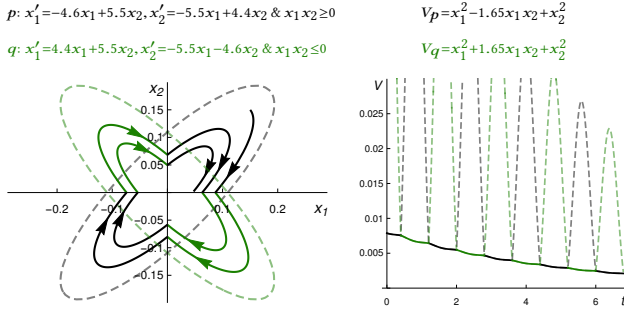
The loop invariants identified above enable derivation of a formal dL stability proof rule for  $\alpha_{arb}$  (deferred to a more general version in Corollary 3 below). In fact, since arbitrary switching is the most permissive form of switching [22], UGPAS for any switching mechanism can be soundly justified using the loop invariants above in case a suitable common Lyapunov function can be found.

**3.1.2 State-dependent Switching.** The state-dependent switching mechanism [22] constrains arbitrary switching by allowing execution of (and switching to) an ODE  $x' = f_p(x), p \in \mathcal{P}$  only when the system state is in domain  $Q_p$ . This is modeled by the hybrid program  $\alpha_{state} \equiv \left( \bigcup_{p \in \mathcal{P}} x' = f_p(x) \ \& \ Q_p \right)^*$  [46, Proposition 2], where arbitrary switching  $\alpha_{arb}$  corresponds to the special case with  $Q_p \equiv \text{true}$  for all  $p \in \mathcal{P}$ .

The same loop invariants for  $\alpha_{arb}$  are used for  $\alpha_{state}$  to derive the following proof rule. For brevity, premises of all derived stability proof rules are implicitly conjunctively quantified over  $p \in \mathcal{P}$ .

**COROLLARY 3 (UGPAS FOR STATE-DEPENDENT SWITCHING, CLF).** *The following proof rule for common Lyapunov function  $V$  with three stacked premises is derivable in dL.*

$$\text{CLF} \frac{\begin{array}{l} \vdash V(0) = 0 \wedge \forall x (\|x\| > 0 \rightarrow V(x) > 0) \\ \vdash \forall b \exists \gamma \forall x (V(x) \leq b \rightarrow \|x\| \leq \gamma) \\ \vdash \mathcal{L}_{f_p}(V)(0) = 0 \wedge \forall x (\|x\| > 0 \wedge \overline{Q_p} \rightarrow \mathcal{L}_{f_p}(V)(x) < 0) \end{array}}{\vdash \text{UGPAS}(\alpha_{state})}$$



**Figure 2: A switching trajectory for Example 7 from Section 4.2 with state-dependent switching (left) and the value of two Lyapunov functions along that trajectory (right). Solid lines indicate the active Lyapunov function at time  $t$ . Two sublevel sets  $V_p, V_q < W = 0.012$  are shown dashed on the left within which the switching trajectory is respectively trapped at any given time.**

Corollary 3 syntactically derives a slight generalization of conditions i)–iii) from Section 3.1.1 for  $\alpha_{\text{state}}$ , where the Lie derivatives  $\mathcal{L}_{f_p}(V)(x)$  for each  $p \in \mathcal{P}$  are required to be negative on their respective domain closures<sup>3</sup>  $\overline{Q_p}$ . This generalization is justified by the same loop invariants in Section 3.1.1 because the ODE invariance properties are only required to hold in their respective domains.

The domain asymmetry in  $\alpha_{\text{state}}$  suggests another way of generalizing the stability arguments, namely, through the use of *multiple Lyapunov functions*, where a (possibly) different Lyapunov function  $V_p$  is associated to each  $p \in \mathcal{P}$  [5]. Here, the function  $V_p$  is responsible for justifying stability within domain  $Q_p$ , i.e., its value decreases along system trajectories whenever the system is within  $Q_p$ , as illustrated in Fig. 2. Constraints on these functions are obtained by modifying the loop invariants to account for this intuition.

**Stability.** The stability loop invariant is modified by case splitting disjunctively on the domains  $Q_p, p \in \mathcal{P}$ , and requiring that the sublevel set characterized by  $V_p < W$  is invariant within its respective domain:  $\text{Inv}_s \equiv \|x\| < \varepsilon \wedge \bigvee_{p \in \mathcal{P}} (Q_p \wedge V_p < W)$ . Similar to Section 3.1.1, the bound  $W$  is chosen so that each sublevel set characterized by  $V_p < W$  is contained in the ball  $\|x\| < \varepsilon$ .

**Pre-attractivity.** The pre-attractivity loop invariant is similarly modified by disjunctively requiring that  $V_p$  decreases along system trajectories when the system is in their respective domains  $Q_p$ :  $\text{Inv}_a \equiv \bigvee_{p \in \mathcal{P}} (Q_p \wedge V_p < W \wedge (V_p \geq U \rightarrow V_p < W + kt))$ . The constants  $U, W, k, T$  are chosen as appropriate lower or upper bounds for all the Lyapunov functions (see proof of Corollary 4).

Arithmetical conditions for the Lyapunov functions  $V_p, p \in \mathcal{P}$  are derived from the modified invariants in the following rule.

**COROLLARY 4 (UGPAS FOR STATE-DEPENDENT SWITCHING, MLF).** *The following proof rule for multiple Lyapunov functions  $V_p, p \in \mathcal{P}$  with four stacked premises is derivable in dL.*

<sup>3</sup>The topological closure  $\overline{Q}$  of domain  $Q$  is needed for soundness of a technical compactness argument used in the pre-attractivity proof, see Appendix A for details.

$$\begin{array}{l}
 \vdash V_p(0) = 0 \wedge \forall x (\|x\| > 0 \rightarrow V_p(x) > 0) \\
 \vdash \forall b \exists \gamma \forall x (V_p(x) \leq b \rightarrow \|x\| \leq \gamma) \\
 \vdash \mathcal{L}_{f_p}(V_p)(0) = 0 \wedge \forall x (\|x\| > 0 \wedge \overline{Q_p} \rightarrow \mathcal{L}_{f_p}(V_p)(x) < 0) \\
 \vdash \bigwedge_{q \in \mathcal{P}} (Q_p \wedge Q_q \rightarrow V_p = V_q) \\
 \hline
 \text{MLF} \quad \vdash \text{UGPAS}(\alpha_{\text{state}})
 \end{array}$$

The top three premises of Corollary 4 are similar to those of Corollary 3, but are now required to hold for each Lyapunov function  $V_p, p \in \mathcal{P}$  separately. The (new) bottom premise corresponds to a compatibility condition between the Lyapunov functions arising from the loop invariants. For example, consider the stability loop invariant (similarly for pre-attractivity) and suppose the system currently satisfies disjunct  $Q_p \wedge V_p < w$  with  $V_p$  justifying stability in domain  $Q_p$ . If the system switches to the ODE  $x' = f_q(x)$  within domain  $Q_q$ , then Lyapunov function  $V_q$  becomes the active Lyapunov function which must satisfy  $V_q < w$  to preserve the stability loop invariant. The premise  $Q_p \wedge Q_q \rightarrow V_p = V_q$  says that the Lyapunov functions  $V_p, V_q$  are equal whenever such a switch is possible (in either direction), i.e., when their domains overlap.

### 3.2 Controlled Switching

This section turns to *controlled switching* models [46], where an explicit controller program is responsible for making logical switching decisions between the ODEs  $x' = f_p(x), p \in \mathcal{P}$ . This is in contrast to earlier models  $\alpha_{\text{arb}}, \alpha_{\text{state}}$  which exhibit *autonomous switching*, i.e., without an explicit control logic [6, 22]. General controlled switching is modeled by the hybrid program  $\alpha_{\text{ctrl1}}$ :

$$\alpha_{\text{ctrl1}} \equiv \alpha_i; \left( \begin{array}{c} \text{switching controller} \quad \alpha_p \text{ (plant, actuate decision)} \\ \uparrow \\ \alpha_u: \bigcup_{p \in \mathcal{P}} (?u = p; x' = f_p(x, y), y' = g_p(x, y) \& Q_p) \end{array} \right)^* \downarrow \text{initialization}$$

The model  $\alpha_{\text{ctrl1}}$  uses three subprograms:  $\alpha_i$  initializes the system, then  $\alpha_u$  (modeling the switching controller) and  $\alpha_p$  (modeling the continuous plant dynamics) are run in a switching loop. The discrete programs  $\alpha_i, \alpha_u$  decide on values for the control output  $u = p, p \in \mathcal{P}$  and the program  $\alpha_p$  responds to this output by evolving the corresponding ODE  $x' = f_p(x, y), y' = g_p(x, y) \& Q_p$ . The programs  $\alpha_i, \alpha_u$  must not modify the system state variables  $x$ , but they may modify other auxiliaries, including *auxiliary continuous state variables*  $y$  used to model timers or integral terms used in controllers, see Section 5.2. This control-plant loop is a typical structure for hybrid systems modeled in dL [32, 34], e.g., the controller  $\alpha_u$  below models the discrete switching logic present in hybrid automata [6, 18, 32] (without jumps in the system state):

$$\begin{aligned}
 \alpha_u &\equiv \bigcup_{p \in \mathcal{P}} (?u = p; \bigcup_{q \in \mathcal{P}} (?G_{p,q}; R_{p,q}; u := q)) \\
 R_{p,q} &\equiv y_1 := e_1; y_2 := e_2; \dots; y_k := e_k
 \end{aligned} \tag{2}$$

For each mode  $p \in \mathcal{P}$ , the switching controller may decide to transition to mode  $q \in \mathcal{P}$ . This transition can only be taken if the *guard* formula  $G_{p,q}$  is true in the current state<sup>4</sup>; if the transition is taken, the *reset map*  $R_{p,q}$  sets the values of auxiliary state variables  $y_1, \dots, y_k$  respectively to the value of terms  $e_1, \dots, e_k$ .

<sup>4</sup>The controller can allow trivial self-transitions with  $G_{p,p} \equiv \text{true}$ .

Stability analysis for controlled switching proceeds by identifying suitable loop invariants  $Inv$  for  $\alpha_{ctrl}$ . A powerful proof technique applied here is *compositional reasoning* [32, 34] which separately analyses the discrete ( $\alpha_i, \alpha_u$ ) and continuous ( $\alpha_p$ ) dynamics, and then lifts those results to the full hybrid dynamics. This idea is exemplified by the following derived variation of the loop rule:

$$\text{loopT} \frac{\Gamma \vdash [\alpha_i]Inv \quad Inv \vdash [\alpha_u]Inv \quad Inv \vdash [\alpha_p]Inv \quad Inv \vdash \phi}{\Gamma \vdash [\alpha_i; (\alpha_u; \alpha_p)^*]\phi}$$

The premises of rule loopT say that system initialization  $\alpha_i$  puts the system in a state satisfying the invariant  $Inv$ , and that  $Inv$  is compositionally preserved by *both* the discrete switching logic  $\alpha_u$  and the continuous dynamics  $\alpha_p$ . This rule is applied to analyze stability for two important special instances of  $\alpha_{ctrl}$  next.

**3.2.1 Guarded State-dependent Switching.** The instance  $\alpha_{guard}$  corresponds to the automata controller from (2) with  $\alpha_i \equiv \bigcup_{p \in \mathcal{P}} u := p$  and guard formulas  $G_{p,q}$ . It does not use auxiliaries  $y$  nor the reset map  $R_{p,q}$ . This model adds *hysteresis* [19] to the state-dependent switching model from Section 3.1.2, so that switching decisions at each  $G_{p,q}$  depend explicitly on the current discrete mode  $u$  in addition to the continuous state. This design change is reflected in the loop invariants and in the corresponding proof rule below.

**Stability.** The stability loop invariant is modified (cf. Section 3.1.2) to case split on the possible discrete modes  $u = p$  rather than the ODE domains:  $Inv_s \equiv \|x\| < \varepsilon \wedge \bigvee_{p \in \mathcal{P}} (u = p \wedge V_p < W)$ .

**Pre-attractivity.** The pre-attractivity loop invariant is modified similarly:  $Inv_a \equiv \bigvee_{p \in \mathcal{P}} (u = p \wedge V_p < W \wedge (V_p \geq U \rightarrow V_p < W + kt))$ .

**COROLLARY 5 (UGPAS FOR GUARDED STATE-DEPENDENT SWITCHING, MLF).** *The following proof rule for multiple Lyapunov functions  $V_p, p \in \mathcal{P}$  with four stacked premises is derivable in dL.*

$$\text{MLF}_G \frac{\begin{array}{l} \vdash V_p(0) = 0 \wedge \forall x (\|x\| > 0 \rightarrow V_p(x) > 0) \\ \vdash \forall b \exists y \forall x (V_p(x) \leq b \rightarrow \|x\| \leq y) \\ \vdash \mathcal{L}_{f_p}(V_p)(0) = 0 \wedge \forall x (\|x\| > 0 \wedge \overline{Q_p} \rightarrow \mathcal{L}_{f_p}(V_p)(x) < 0) \\ \vdash \bigwedge_{q \in \mathcal{P}} (G_{p,q} \rightarrow V_q \leq V_p) \end{array}}{\vdash \text{UGPAS}(\alpha_{guard})}$$

The premises of rule  $\text{MLF}_G$  are identical to those from MLF except the bottom premise, which derives from loopT and unfolding the controller  $\alpha_u$  with dL's hybrid program axioms, e.g., the following proof skeleton shows the unfolding for the stability loop invariant  $Inv_s$  corresponding to a switch from mode  $p$  to mode  $q$ :

$$\begin{array}{c} \text{Arithmetic} \\ \frac{\vdash G_{p,q} \rightarrow V_q \leq V_p}{V_p < W \wedge G_{p,q} \rightarrow V_q < W} \uparrow \\ \text{Unfold} \quad \frac{\uparrow}{u = p \wedge V_p < W \wedge [?G_{p,q}; u := q](u = q \wedge V_q < W)} \\ \text{Inv}_s \vdash [\alpha_u]Inv_s \end{array}$$

Unlike rule MLF, the bottom premise of rule  $\text{MLF}_G$  only uses an inequality, because the guards  $G_{p,q}$  determine permissible switching.

**3.2.2 Time-dependent Switching.** The instance  $\alpha_{time}$  shown below models *time-dependent switching*, where the controller  $\alpha_u$  makes

switching decisions based on the time  $\tau$  elapsed in each mode.

$$\alpha_{time} \equiv \begin{cases} \alpha_i \equiv \tau := 0; \bigcup_{p \in \mathcal{P}} u := p \\ \alpha_u \equiv \bigcup_{p \in \mathcal{P}} \left( ?u = p; \bigcup_{q \in \mathcal{P}} (? \theta_{p,q} \leq \tau; \tau := 0; u := q) \right) \\ \alpha_p \equiv \bigcup_{p \in \mathcal{P}} (?u = p; x' = f_p(x), \tau' = 1 \wedge \tau \leq \Theta_p) \end{cases}$$

The controller  $\alpha_u$  enables switching from mode  $p$  to  $q$  when a *minimum* dwell time  $0 \leq \theta_{p,q} \leq \tau$  has elapsed and resets the timer whenever such a switch occurs. Conversely, the plant  $\alpha_p$  restricts modes with a *maximum* dwell time  $\tau \leq \Theta_p$ ,  $\Theta_p > 0$ ; an unbounded dwell time  $\Theta_p = \infty$  is represented by the domain constraint *true*. Dwell time restrictions can be used to stabilize systems that switch between *stable* and *unstable* modes [48]. Intuitively, the system should stay in stable modes for sufficient duration ( $\theta_{p,q} \leq \tau$ ) while it should avoid staying in unstable modes for too long ( $\tau \leq \Theta_p$ ).

To reason about stability for  $\alpha_{time}$ , consider Lyapunov function conditions  $\mathcal{L}_{f_p}(V_p)(x) \leq -\lambda_p V_p$ , where  $\lambda_p$  is a constant associated with each mode  $p \in \mathcal{P}$ . This condition bounds the value of  $V_p$  along the solution of  $x' = f_p(x)$  by either a decaying exponential for stable modes ( $\lambda_p > 0$ ) or a growing exponential for unstable modes ( $\lambda_p \leq 0$ ). Let  $\mathcal{S} = \{p \in \mathcal{P}, \lambda_p > 0\}$  and  $\mathcal{U} = \{p \in \mathcal{P}, \lambda_p \leq 0\}$  be the indexes of the stable and unstable modes in the loop invariants below, and let  $e^{(\cdot)}$  denote the real exponential function, which is definable in dL by differential axiomatization [32, 35].

**Stability.** The stability loop invariant expresses the required exponential bounds with a case split depending if  $p \in \mathcal{S}$  or  $p \in \mathcal{U}$ :

$$Inv_s \equiv \tau \geq 0 \wedge \|x\| < \varepsilon \wedge \left( \bigvee_{p \in \mathcal{S}} (u = p \wedge V_p < W e^{-\lambda_p \tau}) \vee \bigvee_{p \in \mathcal{U}} (u = p \wedge V_p < W e^{-\lambda_p (\tau - \Theta_p)} \wedge \tau \leq \Theta_p) \right)$$

For  $p \in \mathcal{S}$ ,  $e^{-\lambda_p \tau}$  is the accumulated decay factor for  $V_p$  after staying in the stable mode for time  $\tau$ . For  $p \in \mathcal{U}$ ,  $e^{-\lambda_p (\tau - \Theta_p)}$  is a buffer factor for the growth of  $V_p$  in the unstable mode so that  $V_p < W$  still holds at the maximum dwell time  $\tau = \Theta_p$ . In both cases, the internal timer variable is non-negative ( $\tau \geq 0$ ).

**Pre-attractivity.** The pre-attractivity loop invariant has similar exponential decay and growth bounds for each  $p \in \mathcal{P}$  in the current mode. In addition, it has an overall exponential decay term  $e^{-\sigma(t-\tau)}$  for some  $\sigma > 0$ , which ensures that the value of  $V_p$  tends to 0 as  $t \rightarrow \infty$  for all switching trajectories; recall  $t$  is the global clock introduced in the specification of pre-attractivity in Lemma 2.

$$Inv_a \equiv \tau \geq 0 \wedge t \geq \tau \wedge \left( \bigvee_{p \in \mathcal{S}} (u = p \wedge V_p < W e^{-\sigma(t-\tau)} e^{-\lambda_p \tau}) \vee \bigvee_{p \in \mathcal{U}} (u = p \wedge V_p < W e^{-\sigma(t-\tau)} e^{-\lambda_p (\tau - \Theta_p)} \wedge \tau \leq \Theta_p) \right)$$

Intuitively,  $e^{-\sigma(t-\tau)}$  is the accumulated *overall* decay factor for  $V_p$  until the previous switch, which occurred at time  $t - \tau$ .



COROLLARY 6 (UGPAS FOR TIME-DEPENDENT SWITCHING, MLF).  
The following proof rule for multiple Lyapunov functions  $V_p, p \in \mathcal{P}$  with five stacked premises is derivable in dL.

$$\begin{aligned} & \vdash V_p(0) = 0 \wedge \forall x (\|x\| > 0 \rightarrow V_p(x) > 0) \\ & \vdash \forall b \exists \gamma \forall x (V_p(x) \leq b \rightarrow \|x\| \leq \gamma) \\ & \vdash \mathcal{L}_{f_p}(V_p) \leq -\lambda_p V_p \end{aligned}$$

$$\text{MLF}_\tau \frac{\text{Inv}_s \vdash [\alpha_u] \text{Inv}_s \quad \text{Inv}_a \vdash [\alpha_u] \text{Inv}_a}{\vdash \text{UGPAS}(\alpha_{\text{time}})}$$

The two red premises on the bottom row are expanded to arithmetical conditions on  $V_p$  in Appendix A.

The bottom premises of  $\text{MLF}_\tau$  and  $\text{MLF}_G$  exemplify a key benefit of dL stability reasoning: arithmetical conditions on  $V_p$  that arise from  $\alpha_u, \text{Inv}_s, \text{Inv}_a$  are derived in a *correct-by-construction* manner by systematically unfolding the discrete dynamics of  $\alpha_u$  with sound dL axioms. This is especially important for controlled switching, where the number of possible transitions scales quadratically with the number of switching modes.

## 4 KEYMAERA X IMPLEMENTATION

This section presents a prototype implementation of switched systems support in the KeYmaera X prover based on dL [12]. The implementation consists of  $\approx 2700$  lines and, crucially, does not require any extension to KeYmaera X's existing soundness-critical core. Accordingly, verification results for switched systems obtained through this implementation directly inherit the strong correctness properties guaranteed by KeYmaera X's design [12, 25].

### 4.1 Modeling and Proof Interface

The implementation builds on KeYmaera X's proof IDE [24] to provide a convenient interface for modeling switching mechanisms, as shown in Fig. 3. The interface allows users to express switching mechanisms intuitively by rendering automaton plots while abstracting away the underlying hybrid programs. It provides templates for switched systems following the switching mechanisms of Section 3: state-dependent, guarded, timed, and general controlled switching (tabs "Autonomous", "Timed", "Guarded", "Generic" in Fig. 3). From these templates, KeYmaera X automatically generates programs and stability specifications, ensuring that they have the correct structure. This saves user effort from having to manually expand switching designs to correctly structured hybrid programs. Moreover, the generated programs and specifications follow a uniform structure that the proof tactics discussed below can rely on.

Switched systems are represented internally with a common interface `SwitchedSystem` which is currently implemented by four classes: `StateDependent`  $\alpha_{\text{state}}$ , `Guarded`  $\alpha_{\text{guard}}$ , `Timed`  $\alpha_{\text{time}}$ , and `Controlled`  $\alpha_{\text{ctrl}}$ . The `SwitchedSystem` interface provides default stability and pre-attractivity specifications, which can be adapted by users on the UI if needed. Corollaries 3–6 are implemented as UGPAS proof tactics in KeYmaera X's Bellerophon tactic language [11]. These tactics automate all of the reasoning steps underlying stability proofs for their respective switching mechanisms, so that users only need to input candidate Lyapunov functions for KeYmaera X to (attempt to) complete their proofs. Additionally, when candidates are not provided by the user, the implementation uses sum-of-squares programming [31, 38] to automatically generate

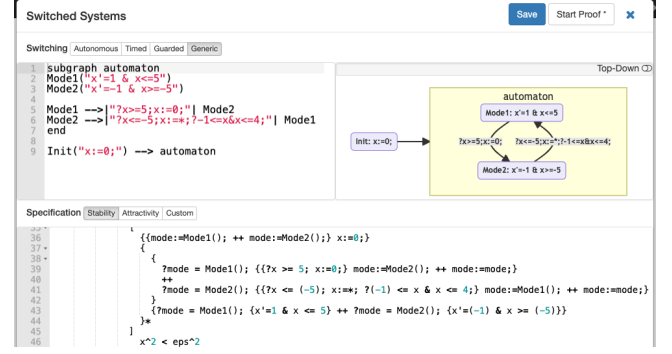


Figure 3: Screenshot of the KeYmaera X switched systems modeling editor: automata input on top-left, rendered automaton top-right, generated hybrid program and specification(s) in dL at the bottom

Table 1: Available tactics in KeYmaera X for switched systems stability proofs and Lyapunov function generation.

SwitchedSystem	Common Lyap.		Multiple Lyap.	
	Proof	Gen.	Proof	Gen.
StateDependent $\alpha_{\text{state}}$	✓	✓	✓	✓
Guarded $\alpha_{\text{guard}}$	✓	✓	✓	✓
Timed $\alpha_{\text{time}}$	✓	✓	✓	—
Controlled $\alpha_{\text{ctrl}}$	✓	✓	—	—

candidate Lyapunov functions for a subset of switching designs. The generated candidates are checked for correctness by KeYmaera X so the generator does not need to be trusted for correctness of the resulting proofs. Table 1 summarizes the available proof tactics and Lyapunov function generation for classes of switching mechanisms.

### 4.2 Examples

The implementation is tested on a suite of examples drawn from the literature [5, 19, 38, 44] featuring various switching mechanisms. These examples have a 2 dimensional state space and switch between 2 modes except Example 6 (3 dimensions, 2 modes) and Example 4 (2 dimensions, 4 modes). Results are summarized in Table 2; Lyapunov functions from the literature were used (if available) in cases where generation failed or is inapplicable.

The proof tactics successfully prove most of the examples across various switching mechanisms. For Example 6, a suitable Lyapunov function (without numerical errors) could not be found. For the time-dependent switching models (Examples 8–10), KeYmaera X internally uses verified polynomial Taylor approximations to the exponential function for decidability of arithmetic [3, 47]. Example 10 requires a high degree approximation (15 terms) and its attractivity proof could not be completed in reasonable time.

## 5 CASE STUDIES

This section presents three case studies applying the deductive verification approach to justify various non-standard stability arguments in KeYmaera X.

**Table 2: Stability proofs for examples drawn from the literature. The “Time” columns indicate time (in seconds) to run the KeYmaera X proofs, × indicates incomplete proof. A ✓ in the “Gen.” column indicates successful Lyapunov function(s) generation, ? indicates that a candidate was generated but with numerical issues, and – indicates inapplicability.**

Example	Model	Time (Stab.)	Time (Attr.)	Gen.
1 [5, Ex. 2.1]	$\alpha_{\text{state}}$	2.6	3.0	✓
2 [19, Motiv. ex.]	$\alpha_{\text{state}}$	2.2	2.3	✓
3 [19, Ex. 1]	$\alpha_{\text{state}}$	3.3	4.1	✓
4 [19, Ex. 2 & 3]	$\alpha_{\text{guard}}$	2.8	3.8	?
5 [38, Ex. 6]	$\alpha_{\text{guard}}$	×	×	?
6 [44, Ex. 2.45]	$\alpha_{\text{arb}}$	19.4	11.1	✓
7 [44, Ex. 3.25]	$\alpha_{\text{state}}$	2.4	2.9	✓
8 [44, Ex. 3.49]	$\alpha_{\text{time}}$	4.4	5.6	–
9 [48, Ex. 1]	$\alpha_{\text{time}}$	4.7	5.3	–
10 [48, Ex. 2]	$\alpha_{\text{time}}$	256.9	×	–

## 5.1 Canonical Max System

Branicky [4] investigates the longitudinal dynamics of an aircraft with an elevator controller that mediates between two control objectives: *i*) tracking potentially unsafe pilot input and *ii*) respecting safety constraints on the aircraft’s angle of attack. Assuming a state feedback control law, the model is transformed to the following *canonical max system* [4, Remark 5], with state variables  $x, y$  and parameters  $a, b, f, g, \gamma$  satisfying  $a, b, a - f, b - g > 0$  and  $\gamma \leq 0$ .

$$x' = y, y' = -ax - by + \max(fx + gy + \gamma, 0) \quad (3)$$

The right-hand side of system (3) is non-differentiable but the equations can be equivalently rewritten as a family of two ODEs corresponding to either possibility for the  $\max(fx + gy + \gamma, 0)$  term in the equation for  $y'$  as follows, where the system follows ODE (A) in domain  $fx + gy + \gamma \leq 0$  and ODE (B) in domain  $fx + gy + \gamma \geq 0$ .

$$(A) \equiv x' = y, y' = -ax - by$$

$$(B) \equiv x' = y, y' = -(a - f)x - (b - g)y + \gamma$$

Stability of this parametric system is *not* directly provable using standard techniques for state-dependent switching presented in Section 3.1.2. For example, the ODE (A) stabilizes the system to the origin but the ODE (B) stabilizes to the point  $(-\frac{\gamma}{a-f}, 0)$  (away from the origin for  $\gamma < 0$ ). Branicky proves global asymptotic stability of (3) with the following “noncustomary” [10] Lyapunov function involving a nondifferentiable integrand:

$$V = \frac{1}{2}y^2 + \int_0^x a\xi - \max(f\xi + \gamma, 0)d\xi \quad (4)$$

Instead, the key idea used to prove stability in this paper is *ghost switching*: analogous to ghost variables in program verification which are added for the sake of program proofs [30, 34, 35], ghost switching modes do not change the physical dynamics of the system but are introduced for the purposes of the stability analysis. Here, ghost switching between  $fx + \gamma \leq 0$  and  $fx + \gamma \geq 0$  is used to obtain closed form representations for the integral in (4). This yields an instance of state-dependent switching  $\alpha_{\text{state}}$  with 4 switching

modes and the corresponding stability specification  $P_m$ :

$$(A)_1 \equiv (A) \& fx + gy + \gamma \leq 0 \wedge fx + \gamma \leq 0$$

$$(A)_2 \equiv (A) \& fx + gy + \gamma \leq 0 \wedge fx + \gamma \geq 0$$

$$(B)_1 \equiv (B) \& fx + gy + \gamma \geq 0 \wedge fx + \gamma \leq 0$$

$$(B)_2 \equiv (B) \& fx + gy + \gamma \geq 0 \wedge fx + \gamma \geq 0$$

$$\alpha_m \equiv ((A)_1 \cup (A)_2 \cup (B)_1 \cup (B)_2)^*$$

$$P_m \equiv a > 0 \wedge b > 0 \wedge a - f > 0 \wedge b - g > 0 \wedge f \neq 0 \wedge \gamma \leq 0 \rightarrow \text{UGpAS}(\alpha_m)$$

The ghost switching modes enable a multiple Lyapunov function argument for stability using the following modified closed-form representations of Branicky’s Lyapunov function (4), with  $V_1 = \frac{1}{2}(bcx^2 + 2cxy + y^2) + \frac{a}{2}x^2$  for  $(A)_1, (B)_1$  and  $V_2 = \frac{1}{2}(bcx^2 + 2cxy + y^2) + \frac{a}{2}x^2 - \frac{(fx + \gamma)^2}{2f}$  for  $(A)_2, (B)_2$ .<sup>5</sup> The sub-terms highlighted in red for  $V_1, V_2$  are closed form expressions for  $\int_0^x a\xi - \max(f\xi + \gamma, 0)d\xi$  where  $f\xi + \gamma \leq 0$  and  $f\xi + \gamma \geq 0$  respectively. The Lyapunov functions  $V_1, V_2$  are modified from (4) to use a quadratic form with an additional constant  $c$  satisfying constraints  $0 < c < b, c < b - g, c < \frac{(a-f)(b-g)}{a-f+g^2}, c < \frac{a(b-g)}{a+g^2}$  (such a constant always exists under the assumptions on  $a, b, f, g$ ). This technical modification is required to prove UGpAS for  $\alpha_m$  directly with the Lyapunov functions. Branicky’s earlier proof requires LaSalle’s principle [4].

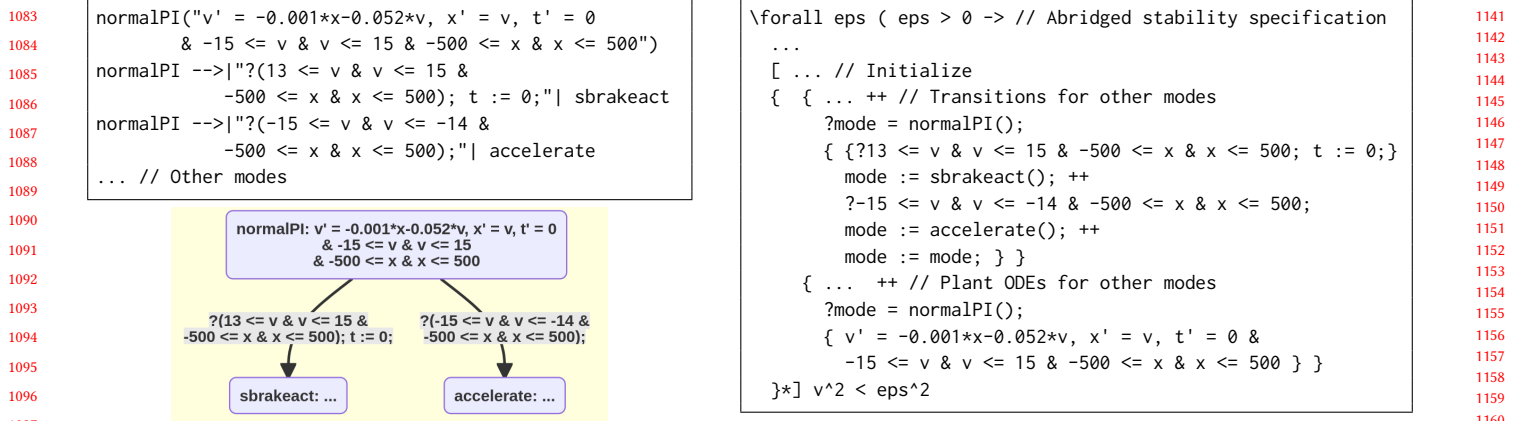
Another challenging aspect of this case study is verification of the *parametric* arithmetical conditions for  $V_1, V_2$ , i.e., stability is verified for *all* possible parameter values  $a, b, f, g, \gamma$  that satisfy the assumptions in  $P_m$ . Such questions are decidable in theory [3, 47], but are difficult for automated solvers in practice (even out of reach of solvers that require numerically bounded parameters [14]). KeYmaera X enables a user-aided proof of the required arithmetic conditions. For example, the Lie derivative of the Lyapunov function  $V_1$  for  $(B)_1$  is given by  $V_1' = -(b - c)y^2 - acx^2 + (cx + y)(fx + gy + \gamma)$ , where  $V_1'$  is required to be strictly negative away from the origin for stability. The arithmetical argument is as follows: if  $cx + y \leq 0$ , then by constraint  $fx + gy + \gamma \geq 0$ ,  $V_1'$  satisfies  $V_1' \leq -(b - c)y^2 - acx^2$ . Otherwise,  $cx + y > 0$ , then by constraint  $fx + \gamma \leq 0$ ,  $V_1'$  satisfies  $V_1' \leq -(b - c)y^2 - acx^2 + gcxy$ . In either case, the RHS bound is a negative definite quadratic form by the earlier choice of parameter  $c$  and therefore,  $V_1'$  is negative away from the origin.

## 5.2 Automated Cruise Control

Oehlerking [29, Sect. 4.6] verifies the stability of an automatic cruise controller modeled as a hybrid automaton with 6 operating modes and 11 transitions between them: normal proportional-integral (PI) control, acceleration, service braking (2 modes), and emergency braking (2 modes). Figure 4 shows an abridged version of the corresponding KeYmaera X model (using  $\alpha_{\text{ctrl}}$ ) with the PI control mode, where  $v$  is the relative velocity to be controlled to  $v = 0$  and  $x, t$  are auxiliary integral and timer variables used in the controller. Briefly, this controller is designed to use the PI controller near  $v = 0$  for stability, while its other control modes drive the system toward  $v = 0$  by accelerating or braking.

<sup>5</sup>An important technical requirement for  $V_2$  to be well-defined is  $f \neq 0$ . The case with  $f = 0$  is also verified in KeYmaera X but the details are omitted here for brevity. It does not require ghost switching and uses only  $V_1$  as its common Lyapunov function.





**Figure 4: Snippets of an automated cruise controller [29] modeled as a (switching) hybrid automaton. Users express the automaton within the description language (top left) and KeYmaera X visualizes the automaton on-the-fly (bottom left). The implementation automatically generates the appropriate hybrid program representation and UGPAS specification (right); ++, &, () denote choice, conjunction, and constants in KeYmaera X's ASCII syntax respectively.**

Lyapunov function candidates for this model can be successfully generated using the Stabhyli [26] stability tool for hybrid automata. However, Stabhyli (with default configurations) outputs a Lyapunov function candidate for the PI control mode that is numerically unsound, see Appendix B for the output and a counterexample; this is a known issue with Stabhyli for control modes at the origin [26]. For this case study, the issue is manually resolved by truncating terms with very small magnitude coefficients in the generated output and then checking in KeYmaera X that the arithmetical conditions for the PI mode are satisfied *exactly* for the truncated candidate.

Further insights from the controller design are used in the UGPAS proof in KeYmaera X. Briefly, stability only concerns states and modes that are active near the origin. Hence, the stability argument and loop invariant only need to mention a single Lyapunov function for the PI control mode, while choosing  $\delta$  (in Def. 1) sufficiently small so that none of the other modes can be entered.<sup>6</sup> Similarly, pre-attractivity only requires reasoning about *asymptotic* convergence to the origin for the PI control mode, hence it suffices to show that the system leaves all other modes in finite time.

### 5.3 Brockett's Nonholonomic Integrator

Verification of stabilizing control laws for Brockett's nonholonomic integrator [7] is of significant interest because stability for a large class of models can be reduced to that of the integrator via coordinate transformations, e.g., Liberzon [22] transforms a unicycle model to the integrator and provides a stabilizing switching control law corresponding to parking of the unicycle. The non-holonomic integrator is described by the system of differential equations  $x' = u$ ,  $y' = v$ ,  $z' = xv - yu$ , with state variables  $x, y, z$  and state feedback control inputs  $u = u(x, y, z)$ ,  $v = v(x, y, z)$  (to be determined below). Notably, this is a classical example of a system

that is not stabilizable by purely continuous feedback control. Intuitively, no choice of controls  $u, v$  can produce motion along the  $z$ -axis ( $x = y = 0$ ). Thus, to stabilize the system to the origin, the controller must first drive the system away from the  $z$ -axis before switching to a control law that stabilizes the system from states away from the  $z$ -axis. This intuition can be realized using two different switching strategies that are analogous to the event-triggered and time-triggered CPS design paradigms respectively [34].

**5.3.1 Event-triggered Controller.** Bloch and Drakunov [2] use the switching controller  $u = -x + ay \operatorname{sign}(z)$ ,  $v = -y - ax \operatorname{sign}(z)$  to asymptotically stabilize the integrator in the region  $\frac{a}{2}(x^2 + y^2) \geq |z|$  for any given constant  $a > 0$ . This controller first drives the system towards the plane  $z = 0$  and, once it reaches the plane, *slides* along the plane towards the origin. The closed-loop system is modeled as an instance of state-dependent switching  $\alpha_{\text{state}}$  with 3 modes depending on the sign of  $z$  and specification  $P_e$ :

$$\textcircled{A} \equiv x' = -x + ay, y' = -y - ax, z' = -a(x^2 + y^2) \ \& \ z \geq 0$$

$$\textcircled{B} \equiv x' = -x - ay, y' = -y + ax, z' = a(x^2 + y^2) \ \& \ z \leq 0$$

$$\textcircled{C} \equiv x' = -x, y' = -y, z' = 0 \ \& \ z = 0$$

$$\alpha_e \equiv (\textcircled{A} \cup \textcircled{B} \cup \textcircled{C})^*$$

$$P_e \equiv a > 0 \rightarrow \text{UStab}(\alpha) \wedge$$

$$\forall \delta > 0 \ \forall \epsilon > 0 \ \exists T \geq 0 \ \forall x, y, z \left( \|x, y, z\| < \delta \wedge \frac{a}{2}(x^2 + y^2) \geq |z| \rightarrow [t := 0; \alpha_e, t' = 1](t \geq T \rightarrow \|x, y, z\| < \epsilon) \right)$$

The specification  $P_e$  is identical to UGPAS except it restricts pre-attractivity to the applicable region  $\frac{a}{2}(x^2 + y^2) \geq |z|$  for the controller.<sup>7</sup> Its verification uses the squared norm  $V = x^2 + y^2 + z^2$  as a common Lyapunov function. The key modification to the pre-attractivity proof, cf. Section 3.1, is to use (and verify) the fact that

<sup>6</sup>In fact, the PI controller equations are exactly those of a linearized pendulum, which has known Lyapunov functions [21, 45]. It could be interesting to modify Stabhyli to accept user-provided Lyapunov function hints for certain modes.

<sup>7</sup>The applicable region is equivalently characterized by the real arithmetic formula  $(z \geq 0 \rightarrow \frac{a}{2}(x^2 + y^2) \geq z) \wedge (z \leq 0 \rightarrow \frac{a}{2}(x^2 + y^2) \geq -z)$  but this is omitted for brevity.

$\frac{a}{2}(x^2 + y^2) \geq |z|$  is a loop invariant of  $\alpha_e$ . This additional invariant corresponds to the fact that the controller keeps the system within its applicable region (if the system is initially within that region).

In fact,  $\alpha_e$  can be extended to a globally stabilizing controller, as modeled by  $\alpha_{\hat{e}}$  below (**if, else** branching is supported as an abbreviation in KeYmaera X [34]):

$$\begin{aligned} \textcircled{D} &\equiv x' = u, y' = v, z' = xv - yu \ \& \ \frac{a}{2}(x^2 + y^2) \leq |z| \\ \textcircled{E} &\equiv x' = u, y' = v, z' = xv - yu \ \& \ \frac{a}{2}(x^2 + y^2) \geq |z| \\ \alpha_{\hat{e}} &\equiv \left( \text{if} \left( \frac{a}{2}(x^2 + y^2) \geq |z| \right) \{ \textcircled{A} \cup \textcircled{B} \cup \textcircled{C} \} \right. \\ &\quad \text{else} \left\{ \begin{array}{l} \text{if}((x - y)z \leq 0) \{ u := c; v := c \} \\ \text{else} \{ u := -c; v := -c \}; \\ \left. \{ \textcircled{D} \cup \textcircled{E} \} \right\}^* \end{array} \right. \end{aligned}$$

If the system is in the applicable region (outer **if** branch), then the previous controller from  $\alpha_e$  is used. Otherwise, outside the applicable region (outer **else** branch), the system applies a constant control  $c > 0$  chosen to drive the system into the applicable region. The pair of ODEs  $\textcircled{D}$  and  $\textcircled{E}$  model an event-trigger in dL [34], where the switching controller is triggered to make its next decision when the system reaches the switching surface  $\frac{a}{2}(x^2 + y^2) = |z|$ .

The specification  $P_{\hat{e}} \equiv a > 0 \wedge c > 0 \rightarrow \text{UGpAS}(\alpha_{\hat{e}})$  is proved by modifying the loop invariants to account for the initial period where the system is outside the applicable region, e.g., the stability loop invariant  $\text{Inv}_s \equiv (\neg \frac{a}{2}(x^2 + y^2) \geq |z| \rightarrow |z| < \delta) \wedge (\frac{a}{2}(x^2 + y^2) \geq |z| \rightarrow \|x, y, z\| < \varepsilon)$  expresses that the controller keeps  $|z|$  sufficiently small to preserve stability outside the applicable region.

**5.3.2 Time-triggered Controller.** The time-triggered switching strategy [34], modeled by  $\alpha_\tau$  below, is similar to that proposed by Liberzon [22, Section 4.2]. If the system is on the  $z$ -axis and away from the origin  $\textcircled{A}$ , the controller sets an internal stopwatch  $\tau$  and drives the system away from the axis for maximum duration  $T_0 > 0$  with  $u = z, v = z$ . Otherwise  $\textcircled{B}$ , the controller drives the system towards the origin along a parabolic curve of the form  $\frac{a}{2}(x^2 + y^2) = z$ .

$$\begin{aligned} \alpha_\tau &\equiv \left( \text{if}(x = 0 \wedge y = 0 \wedge z \neq 0) \{ \right. \\ \textcircled{A} \quad &\quad \tau := 0; x' = z, y' = z, z' = xz - yz \ \& \ \tau \leq T_0 \} \\ &\quad \text{else} \left\{ a := \frac{2z}{x^2 + y^2}; \right. \\ \textcircled{B} \quad &\quad \left. x' = -x + ay, y' = -y - ax, z' = -a(x^2 + y^2) \right\}^* \end{aligned}$$

The specification  $P_\tau \equiv T_0 > 0 \rightarrow \text{UGpAS}(\alpha_\tau)$  is again proved by analyzing both cases of the controller in the loop invariants, e.g., with the pre-attractivity invariant  $\text{Inv}_a$ :

$$\begin{aligned} (x = 0 \wedge y = 0 \wedge z \neq 0 \rightarrow |z| < \delta \wedge t = 0) \wedge \\ (\neg(x = 0 \wedge y = 0 \wedge z \neq 0) \rightarrow \\ \|x, y, z\| > \varepsilon \rightarrow \|x, y, z\|^2 < \delta^2(2T_0^2 + 1) - \varepsilon^2(t - T_0)) \end{aligned}$$

The left conjunct says the system may start transiently on the  $z$ -axis (away from  $z = 0$ ) at time  $t = 0$ . The right conjunct gives explicit bounds on  $\|x, y, z\|$ , which, for sufficiently large  $t \geq T$  implies that the system enters  $\|x, y, z\| < \varepsilon$  as required for pre-attractivity.

The transient term  $\delta^2(2T_0^2 + 1)$  upper bounds the (squared) norm of the system state after starting on the  $z$ -axis in ball  $\|x, y, z\| < \delta$  and following mode  $\textcircled{A}$  for the maximum stopwatch duration  $\tau = T_0$ .

## 6 RELATED WORK

**Switched Systems.** Comprehensive introductions to the analysis and design of switching control can be found in the literature [10, 22, 44]. An important design consideration (which this paper sidesteps, cf. Remark 1) is whether a given switched or hybrid system has complete solutions [16, 17, 23, 49]. Justification of such design considerations, and other stability notions of interest for switching designs, e.g., quadratic, region, or set-based stability [16, 17, 22, 36, 44], can be done in dL with appropriate formal specifications of the desired properties from the literature [32, 34, 45, 46]. Another complementary question is how to design a switching control law that *stabilizes* a given system. Switching design approaches are often guided by underlying stability arguments [22, 39, 44]; the loop invariants from Section 3 are expected to help guide correct-by-construction synthesis of such controllers.

**Stability Analysis and Verification.** Corollaries 3–6 formalize various Lyapunov function-based stability arguments from the literature [5, 48] using loop invariants, yielding trustworthy, computer-checked stability proofs in KeYmaera X [11, 12]. Other computer-aided approaches for switched system stability analysis are based on finding Lyapunov functions that satisfy the requisite arithmetical conditions [20, 26, 29, 38, 41, 42]. Although the search for such functions can often be done efficiently with numerical techniques [26, 31, 38], various authors have emphasized the need to check that their outputs satisfy the arithmetical conditions *exactly*, i.e., without numerical errors compromising the resulting stability claims [1, 20, 40] (see, e.g., Section 5.2). This paper's deductive approach goes further as it comprehensively verifies *all* steps of the stability argument down to its underlying discrete and continuous reasoning steps [33, 34]. The generality of this approach is precisely what enables verification of various classes of switching mechanisms all within a common logical framework (Section 3) and verification of non-standard stability arguments (Section 5). Alternative approaches to stability verification are based on abstraction [15, 43] and model checking [36].

## 7 CONCLUSION

This paper shows how to deductively verify switched system stability, using dL's nested quantification over hybrid programs to specify stability, and dL's axiomatics to prove those specifications. Loop invariants—a classical technique from verification—are used to succinctly capture the desired properties of a given switching design; through deductive proofs, these invariants yield systematic, correct-by-construction derivation of the requisite arithmetical conditions on Lyapunov functions for stability arguments in implementations. An interesting direction for future work is to use other Lyapunov function generation techniques [20, 26, 29, 42], which—thanks to the presented approach—do not have to be trusted since their results can be checked independently by KeYmaera X. This would enable fully automated, yet sound and trustworthy verification of switched system stability based on dL's parsimonious hybrid program reasoning principles.

## REFERENCES

- [1] Daniele Ahmed, Andrea Peruffo, and Alessandro Abate. 2020. Automated and Sound Synthesis of Lyapunov Functions with SMT Solvers. In *TACAS (LNCS)*, Armin Biere and David Parker (Eds.), Vol. 12078. Springer, 97–114. [https://doi.org/10.1007/978-3-030-45190-5\\_6](https://doi.org/10.1007/978-3-030-45190-5_6)
- [2] Anthony Bloch and Sergey Drakunov. 1996. Stabilization and tracking in the nonholonomic integrator via sliding modes. *Systems & Control Letters* 29, 2 (1996), 91–99. [https://doi.org/10.1016/S0167-6911\(96\)00049-7](https://doi.org/10.1016/S0167-6911(96)00049-7)
- [3] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. 1998. *Real Algebraic Geometry*. Springer, Heidelberg. <https://doi.org/10.1007/978-3-662-03718-8>
- [4] Michael S. Branicky. 1994. Analyzing continuous switching systems: theory and examples. In *ACC*, Vol. 3. 3110–3114. <https://doi.org/10.1109/ACC.1994.735143>
- [5] Michael S. Branicky. 1998. Multiple Lyapunov functions and other analysis tools for switched and hybrid systems. *IEEE Trans. Autom. Control* 43, 4 (1998), 475–482. <https://doi.org/10.1109/9.664150>
- [6] Michael S. Branicky. 2005. Introduction to Hybrid Systems. In *Handbook of Networked and Embedded Control Systems*, Dimitrios Hristu-Varsakelis and William S. Levine (Eds.). Birkhäuser, 91–116. [https://doi.org/10.1007/0-8176-4404-0\\_5](https://doi.org/10.1007/0-8176-4404-0_5)
- [7] R. W. Brockett. 1983. Asymptotic stability and feedback stabilization. In *Differential Geometric Control Theory*. Birkhäuser, 181–191.
- [8] Carmen Chicone. 2006. *Ordinary Differential Equations with Applications, Second Edition*. Springer-Verlag New York. <https://doi.org/10.1007/0-387-35794-7>
- [9] Jorge Cortes. 2008. Discontinuous dynamical systems. *IEEE Control Systems Magazine* 28, 3 (2008), 36–73. <https://doi.org/10.1109/MCS.2008.919306>
- [10] Raymond A. Decarlo, Michael S. Branicky, Stefan Pettersson, and Bengt Lennartson. 2000. Perspectives and results on the stability and stabilizability of hybrid systems. *Proc. IEEE* 88, 7 (2000), 1069–1082. <https://doi.org/10.1109/5.871309>
- [11] Nathan Fulton, Stefan Mitsch, Brandon Bohrer, and André Platzer. 2017. Bellerophon: Tactical Theorem Proving for Hybrid Systems. In *ITP (LNCS)*, Mauricio Ayala-Rincón and César A. Muñoz (Eds.), Vol. 10499. Springer, 207–224. [https://doi.org/10.1007/978-3-319-66107-0\\_14](https://doi.org/10.1007/978-3-319-66107-0_14)
- [12] Nathan Fulton, Stefan Mitsch, Jan-David Quesel, Marcus Völz, and André Platzer. 2015. KeYmaera X: An Axiomatic Tactical Theorem Prover for Hybrid Systems. In *CADE (LNCS)*, Amy P. Felty and Aart Middeldorp (Eds.), Vol. 9195. Springer, Cham, 527–538. [https://doi.org/10.1007/978-3-319-21401-6\\_36](https://doi.org/10.1007/978-3-319-21401-6_36)
- [13] Sicun Gao, James Kapinski, Jyotirmoy V. Deshmukh, Nima Roohi, Armando Solar-Lezama, Nikos Aréchiga, and Soonho Kong. 2019. Numerically-Robust Inductive Proof Rules for Continuous Dynamical Systems. In *CAV (LNCS)*, Isil Dillig and Serdar Tasiran (Eds.), Vol. 11562. Springer, 137–154. [https://doi.org/10.1007/978-3-030-25543-5\\_9](https://doi.org/10.1007/978-3-030-25543-5_9)
- [14] Sicun Gao, Soonho Kong, and Edmund M. Clarke. 2013. dReal: An SMT Solver for Nonlinear Theories over the Reals. In *CADE (LNCS)*, Maria Paola Bonacina (Ed.), Vol. 7898. Springer, 208–214. [https://doi.org/10.1007/978-3-642-38574-2\\_14](https://doi.org/10.1007/978-3-642-38574-2_14)
- [15] Miriam García Soto and Pavithra Prabhakar. 2020. Abstraction based verification of stability of polyhedral switched systems. *Nonlinear Analysis: Hybrid Systems* 36 (2020), 100856. <https://doi.org/10.1016/j.nahs.2020.100856>
- [16] Rafal Goebel, Ricardo G. Sanfelice, and Andrew R. Teel. 2009. Hybrid dynamical systems. *IEEE Control Systems Magazine* 29, 2 (2009), 28–93. <https://doi.org/10.1109/MCS.2008.931718>
- [17] Rafal Goebel, Ricardo G. Sanfelice, and Andrew R. Teel. 2012. *Hybrid Dynamical Systems: Modeling, Stability, and Robustness*. Princeton University Press.
- [18] Thomas A. Henzinger. 1996. The Theory of Hybrid Automata. In *LICS*. IEEE Computer Society, 278–292.
- [19] Martin Johansson and Anders Rantzer. 1998. Computation of piecewise quadratic Lyapunov functions for hybrid systems. *IEEE Trans. Autom. Control* 43, 4 (1998), 555–559. <https://doi.org/10.1109/9.664157>
- [20] James Kapinski, Jyotirmoy V. Deshmukh, Sriram Sankaranarayanan, and Nikos Aréchiga. 2014. Simulation-guided Lyapunov analysis for hybrid dynamical systems. In *HSCC*, Martin Fränzle and John Lygeros (Eds.), ACM, 133–142. <https://doi.org/10.1145/2562059.2562139>
- [21] Hassan K. Khalil. 1992. *Nonlinear systems*. Macmillan Publishing Company, New York. xii+564 pages.
- [22] Daniel Liberzon. 2003. *Switching in Systems and Control*. Birkhäuser. <https://doi.org/10.1007/978-1-4612-0017-8>
- [23] John Lygeros, Karl Henrik Johansson, Slobodan N. Simic, Jun Zhang, and Shankar S. Sastry. 2003. Dynamical properties of hybrid automata. *IEEE Trans. Autom. Control* 48, 1 (2003), 2–17. <https://doi.org/10.1109/TAC.2002.806650>
- [24] Stefan Mitsch and André Platzer. 2016. The KeYmaera X proof IDE: Concepts on usability in hybrid systems theorem proving. In *3rd Workshop on Formal Integrated Development Environment (EPTCS)*, Catherine Dubois, Paolo Masci, and Dominique Méry (Eds.), Vol. 240. 67–81. <https://doi.org/10.4204/EPTCS.240.5>
- [25] Stefan Mitsch and André Platzer. 2020. A Retrospective on Developing Hybrid Systems Provers in the KeYmaera Family - A Tale of Three Provers. In *Deductive Software Verification: Future Perspectives - Reflections on the Occasion of 20 Years of KeY*, Wolfgang Ahrendt, Bernhard Beckert, Richard Bubel, Reiner Hähnle, and Matthias Ulbrich (Eds.). LNCS, Vol. 12345. Springer, 21–64. [https://doi.org/10.1007/978-3-030-64354-6\\_2](https://doi.org/10.1007/978-3-030-64354-6_2)
- [26] Eike Möhlmann and Oliver E. Theel. 2013. Stabbyli: a tool for automatic stability verification of non-linear hybrid systems. In *HSCC*, Calin Belta and Franjo Ivancic (Eds.). ACM, 107–112. <https://doi.org/10.1145/2461328.2461347>
- [27] Eike Möhlmann and Oliver E. Theel. 2021. Stabbyli. <https://uol.de/svs/forschung/avacs/stabbyli> [Online; accessed 27-October-2021].
- [28] A. S. Morse. 1995. Control Using Logic-Based Switching. In *Trends in Control*, Alberto Isidori (Ed.). Springer London, London, 69–113. [https://doi.org/10.1007/978-1-4471-3061-1\\_4](https://doi.org/10.1007/978-1-4471-3061-1_4)
- [29] Jens Oehlerking. 2011. *Decomposition of stability proofs for hybrid systems*. Ph.D. Dissertation. Carl von Ossietzky University of Oldenburg. <https://oops.uni-oldenburg.de/id/eprint/1375>
- [30] Susan S. Owicki and David Gries. 1976. Verifying Properties of Parallel Programs: An Axiomatic Approach. *Commun. ACM* 19, 5 (1976), 279–285. <https://doi.org/10.1145/360051.360224>
- [31] A. Papachristodoulou, J. Anderson, G. Valmorbida, S. Prajna, P. Seiler, P. A. Parrilo, M. M. Peet, and D. Jagt. 2021. SOSTOOLS: Sum of squares optimization toolbox for MATLAB. <http://arxiv.org/abs/1310.4716>. Available from <https://github.com/oxfordcontrol/SOSTOOLS>.
- [32] André Platzer. 2010. *Logical Analysis of Hybrid Systems - Proving Theorems for Complex Dynamics*. Springer. <https://doi.org/10.1007/978-3-642-14509-4>
- [33] André Platzer. 2017. A Complete Uniform Substitution Calculus for Differential Dynamic Logic. *J. Autom. Reasoning* 59, 2 (2017), 219–265. <https://doi.org/10.1007/s10817-016-9385-1>
- [34] André Platzer. 2018. *Logical Foundations of Cyber-Physical Systems*. Springer, Cham. <https://doi.org/10.1007/978-3-319-63588-0>
- [35] André Platzer and Yong Kiam Tan. 2020. Differential Equation Invariance Axiomatization. *J. ACM* 67, 1, Article 6 (2020), 66 pages. <https://doi.org/10.1145/3380825>
- [36] Andreas Podelski and Silke Wagner. 2006. Model Checking of Hybrid Systems: From Reachability Towards Stability. In *HSCC (LNCS)*, João P. Hespanha and Ashish Tiwari (Eds.), Vol. 3927. Springer, 507–521. [https://doi.org/10.1007/11730637\\_38](https://doi.org/10.1007/11730637_38)
- [37] Stephen Prajna, Ali Jadbabaie, and George J. Pappas. 2007. A Framework for Worst-Case and Stochastic Safety Verification Using Barrier Certificates. *IEEE Trans. Automat. Contr.* 52, 8 (2007), 1415–1428. <https://doi.org/10.1109/TAC.2007.902736>
- [38] S. Prajna and A. Papachristodoulou. 2003. Analysis of switched and hybrid systems - beyond piecewise quadratic methods. In *ACC*, Vol. 4. 2779–2784 vol.4. <https://doi.org/10.1109/ACC.2003.1243743>
- [39] Hadi Ravanbakhsh and Sriram Sankaranarayanan. 2015. Counter-Example Guided Synthesis of control Lyapunov functions for switched systems. In *CDC*. IEEE, 4232–4239. <https://doi.org/10.1109/CDC.2015.7402879>
- [40] Pierre Roux, Yuen-Lam Voronin, and Sriram Sankaranarayanan. 2018. Validating numerical semidefinite programming solvers for polynomial invariants. *Formal Methods Syst. Des.* 53, 2 (2018), 286–312. <https://doi.org/10.1007/s10703-017-0302-y>
- [41] Sriram Sankaranarayanan, Xin Chen, and Erika Ábrahám. 2013. Lyapunov Function Synthesis Using Handelman Representations. In *NOLCOS*, Sophie Tarbouriech and Miroslav Krstic (Eds.). International Federation of Automatic Control, 576–581. <https://doi.org/10.3182/20130904-3-FR-2041.00198>
- [42] Zhikun She and Bai Xue. 2014. Discovering Multiple Lyapunov Functions for Switched Hybrid Systems. *SIAM J. Control. Optim.* 52, 5 (2014), 3312–3340. <https://doi.org/10.1137/130934313>
- [43] Miriam García Soto and Pavithra Prabhakar. 2018. Averist: Algorithmic Verifier for Stability of Linear Hybrid Systems. In *HSCC*, Maria Prandini and Jyotirmoy V. Deshmukh (Eds.). ACM, 259–264. <https://doi.org/10.1145/3178126.3178154>
- [44] Zhendong Sun and Shuzhi Sam Ge. 2011. *Stability Theory of Switched Dynamical Systems*. Springer. <https://doi.org/10.1007/978-0-85729-256-8>
- [45] Yong Kiam Tan and André Platzer. 2021. Deductive Stability Proofs for Ordinary Differential Equations. In *TACAS (LNCS)*, Jan Friso Groote and Kim Guldstrand Larsen (Eds.), Vol. 12652. Springer, 181–199. [https://doi.org/10.1007/978-3-030-72013-1\\_10](https://doi.org/10.1007/978-3-030-72013-1_10)
- [46] Yong Kiam Tan and André Platzer. 2021. Switched Systems as Hybrid Programs. In *ADHS (IFAC-PapersOnLine)*, Raphaël M. Jurgers, Necmiye Ozay, and Alessandro Abate (Eds.), Vol. 54. Elsevier, 247–252. <https://doi.org/10.1016/j.ifacol.2021.08.506>
- [47] Alfred Tarski. 1951. *A Decision Method for Elementary Algebra and Geometry*. RAND Corporation, Santa Monica, CA.
- [48] Guisheng Zhai, Bo Hu, Kazunori Yasuda, and Anthony N. Michel. 2001. Stability analysis of switched systems with stable and unstable subsystems: An average dwell time approach. *Int. J. Syst. Sci.* 32, 8 (2001), 1055–1061. <https://doi.org/10.1080/002071701106692>
- [49] Jun Zhang, Karl Henrik Johansson, John Lygeros, and Shankar Sastry. 2001. Zeno hybrid systems. *Int. J. Robust Nonlinear Control* 11, 5 (2001), 435–451. <https://doi.org/10.1002/rnc.592>



## A PROOFS

This appendix provides proofs for the results presented in the main paper. Relevant background for dL's semantics and axiomatics is given, expanding on the material in Section 2. Full definitions are available in the literature [33, 34].

A dL state  $\omega : \mathcal{V} \rightarrow \mathbb{R}$  assigns a real value to each variable in  $\mathcal{V}$ . The set of variables  $\mathcal{V}$  consists of the continuously evolving state variables  $x = (x_1, \dots, x_n)$  of a switched system model and additional variables  $\mathcal{V} \setminus \{x\}$  used as program auxiliaries for those models. Following Tan and Platzer [46], dL states are projected on the state variables  $x$  and the (projected) dL states  $\omega$  are equivalently treated as points in  $\mathbb{R}^n$ . The semantics of program auxiliaries is as usual [34]. The axioms and proof rules of dL used in the proofs are as follows.

$$\begin{aligned}
& [:=] [x := e]P(x) \leftrightarrow P(e) \quad (e \text{ free for } x \text{ in } P) \\
& [?] [?Q]P \leftrightarrow (Q \rightarrow P) \quad [\cup] [\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P \\
& [;] [\alpha; \beta]P \leftrightarrow [\alpha][\beta]P \quad [*] [\alpha^*]P \leftrightarrow P \wedge [\alpha][\alpha^*]P \\
& \text{loop} \frac{\Gamma \vdash \text{Inv} \quad \text{Inv} \vdash [\alpha] \text{Inv} \quad \text{Inv} \vdash \phi}{\Gamma \vdash [\alpha^*]\phi} \\
& \text{loopT} \frac{\Gamma \vdash [\alpha_i] \text{Inv} \quad \text{Inv} \vdash [\alpha_u] \text{Inv} \quad \text{Inv} \vdash [\alpha_p] \text{Inv} \quad \text{Inv} \vdash \phi}{\Gamma \vdash [\alpha_i; (\alpha_u; \alpha_p)^*]\phi} \\
& \text{G} \frac{\vdash P \quad M[\cdot] \quad R \vdash P \quad \Gamma \vdash [\alpha]R}{\Gamma \vdash [\alpha]P} \\
& \text{dI}_{\succsim} \frac{\Gamma, Q \vdash p \succsim q \quad Q \vdash \mathcal{L}_{f(x)}(p) \geq \mathcal{L}_{f(x)}(q)}{\Gamma \vdash [x' = f(x) \& Q]p \succsim q} \quad (\succsim \text{ is either } \geq \text{ or } >) \\
& \text{dC} \frac{\Gamma \vdash [x' = f(x) \& Q]C \quad \Gamma \vdash [x' = f(x) \& Q \wedge C]P}{\Gamma \vdash [x' = f(x) \& Q]P} \\
& \text{dW} \frac{Q \vdash P}{\Gamma \vdash [x' = f(x) \& Q]P} \\
& \text{dbx}_{\succsim} \frac{Q \vdash \mathcal{L}_{f(x)}(p) \geq gp}{p \succsim 0 \vdash [x' = f(x) \& Q]p \succsim 0} \quad (\succsim \text{ is either } \geq \text{ or } >) \\
& \text{Barr} \frac{Q, p \succsim 0 \vdash \mathcal{L}_{f(x)}(p) > 0}{\Gamma, p \succsim 0 \vdash [x' = f(x) \& Q]p \succsim 0} \quad (\succsim \text{ is either } \geq \text{ or } >) \\
& \text{DCC} \frac{[x' = f(x) \& Q \wedge P]R \wedge [x' = f(x) \& Q](\neg P \rightarrow [x' = f(x) \& Q]\neg P)}{\rightarrow [x' = f(x) \& Q](P \rightarrow R)} \\
& \text{DX} [x' = f(x) \& Q]P \leftrightarrow (Q \rightarrow P \wedge [x' = f(x) \& Q]P) \quad (x' \notin P, Q)
\end{aligned}$$

Axioms  $[:=]$ ,  $[?]$ ,  $[;]$ ,  $[\cup]$ ,  $[*]$  unfold box modalities of their respective hybrid programs according to their semantics [33, 34]. These equivalences are especially useful for obtaining correct-by-construction arithmetical conditions on Lyapunov functions in derivations and implementations (see Corollaries 5 and 6). The derived loop induction rules  $\text{loop}$ ,  $\text{loopT}$  are used to prove stability properties of switched system models with suitably chosen loop invariants  $\text{Inv}$  (see Section 3). Rule  $\text{G}$  is Gödel generalization, and rule  $M[\cdot]$  is the derived monotonicity rule for box modality postconditions; antecedents that have no free variables bound in  $\alpha$  are soundly kept across uses of rules  $\text{loop}$ ,  $\text{loopT}$ ,  $\text{G}$ ,  $M[\cdot]$  [33, 34].

The remaining axioms and proof rules are used in dL to reason about differential equations  $x' = f(x) \& Q$  [33–35, 45]. Differential

invariants  $\text{dI}_{\succsim}$  proves ODE invariance for an inequality  $p \succsim q$  if their Lie derivatives satisfy  $\mathcal{L}_{f(x)}(p) \geq \mathcal{L}_{f(x)}(q)$ . Differential cuts  $\text{dC}$  say that if one can separately prove that formula  $C$  is always satisfied along the solution, then  $C$  may be assumed in the domain constraint when proving the same for formula  $P$ . Differential weakening  $\text{dW}$  says that postcondition  $P$  is always satisfied along solutions if it is already implied by the domain constraint. Rule  $\text{dbx}_{\succsim}$  is the Darboux inequality proof rule for the invariance of  $p \succsim 0$ , where  $g$  is an arbitrary cofactor term [35]. Rule  $\text{Barr}$  is a dL rendition of the strict barrier certificates proof rule [37] for invariance of  $p \succsim 0$ . Axiom  $\text{DCC}$  says that 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 [45]. Differential skip  $\text{DX}$  unfolds the effect of a differential equation on the initial state in the box modality.

To improve readability in the proofs below, formula and premises are often abbreviated, e.g., with  $\textcircled{a}$ ,  $\textcircled{1}$ . To avoid confusion, the scope of these abbreviations always extend to the end of each *paragraph* label, i.e., the abbreviations used in the *Stability* proofs should not be confused with those used in the *Pre-attractivity* proofs.

**PROOF OF LEMMA 2.** Let  $\Phi(x)$  denote the set of all domain-obeying solutions  $\varphi : [0, T_\varphi] \rightarrow \mathbb{R}^n$  for a given switched system from state  $x \in \mathbb{R}^n$  as in Def. 1. Hybrid program  $\alpha$  models this switched system if for any initial state  $\omega \in \mathbb{R}^n$ , the state  $v$  is reachable from  $\omega$ , i.e.,  $(\omega, v) \in \llbracket \alpha \rrbracket$ , iff  $v = \varphi(\tau)$  for some  $\varphi \in \Phi(\omega)$  and  $\tau \in [0, T_\varphi]$ . For the augmented program  $\alpha, t' = 1$ , in particular,  $t$  syntactically tracks the progression of time so that  $(\omega, v) \in \llbracket \alpha, t' = 1 \rrbracket$  iff  $v = \varphi(\tau)$  for some  $\varphi \in \Phi(\omega)$  and  $\tau = v(t) - \omega(t)$ . Tan and Platzer [46] prove the adequacy of hybrid program models for several switching designs.

The formulas  $\text{UStab}(\alpha)$  and  $\text{UGpAttr}(\alpha)$  syntactically express their respective quantifiers from Def. 1, where the box modality  $[\cdot]$  is used in both formulas to quantify over all reachable states of  $\alpha$  (and  $\alpha, t' = 1$ ), i.e., all times  $\tau \in [0, T_\varphi]$  along all solutions  $\varphi \in \Phi$ . Thus, the correctness of these specifications follows directly from the definition of dL's formula semantics [33, 34]. In  $\text{UGpAttr}(\alpha)$ , variable  $t$  is set to 0 initially, so the implication  $t \geq T \rightarrow \dots$  in the postcondition of the box modality further restricts temporal quantification to all times  $\omega(T) \leq \tau \leq T_\varphi$  for  $\varphi \in \Phi(\omega)$ , as required in the definition of uniform pre-attractivity.  $\square$

**PROOF OF COROLLARY 3.** The proof rule  $\text{CLF}$  is an instance of rule  $\text{MLF}$  from Corollary 4 where the Lyapunov functions for all modes  $p \in \mathcal{P}$  are chosen identically with  $V_p = V$ . Nevertheless, a full derivation of  $\text{CLF}$  is given here because it provides the building blocks used in later derivations. The stability and pre-attractivity conjuncts of  $\text{UGpAS}(\alpha_{\text{state}})$  are proved separately with  $\wedge \text{R}$ :

$$\wedge \text{R} \frac{\vdash \text{UStab}(\alpha_{\text{state}}) \quad \vdash \text{UGpAttr}(\alpha_{\text{state}})}{\vdash \text{UGpAS}(\alpha_{\text{state}})}$$

**Stability.** The derivation for stability begins by Skolemizing the succedent with  $\forall \text{R}$ ,  $\rightarrow \text{R}$ , followed by two arithmetic cuts which are justified as follows. For any  $\varepsilon > 0$ , the Lyapunov function  $V$  attains a minimum value on the compact set characterized by  $\|x\| = \varepsilon$ . From the first (topmost) premise of rule  $\text{CLF}$ , this minimum is attained away from the origin so it is positive, which proves the first cut of formula  $\exists W > 0 \textcircled{a}$  where  $\textcircled{a} \equiv \forall x (\|x\| = \varepsilon \rightarrow V \geq W)$ . After Skolemizing  $W$  with  $\exists \text{L}$ , the premise  $V(0) = 0$  implies, by continuity

of dL term semantics [33], that the sublevel set characterized by  $V < W$  with  $W > 0$  (see Fig. 1) contains a sufficiently small  $\delta$  ball around the origin. This proves the second arithmetic cut with the formula  $\exists \delta (0 < \delta \leq \varepsilon \wedge \textcircled{B})$  where  $\textcircled{B} \equiv \forall x (\|x\| < \delta \rightarrow V < W)$ . After both cuts, the antecedent  $\delta$  is used to witness the succedent by  $\exists R$ .

$$\frac{\begin{array}{c} \textcircled{A}, \delta \leq \varepsilon, \textcircled{B} \vdash \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon) \\ \exists R \frac{\textcircled{A}, 0 < \delta \leq \varepsilon, \textcircled{B} \vdash \exists \delta > 0 \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon)}{\textcircled{A}, 0 < \delta \leq \varepsilon, \textcircled{B} \vdash \exists \delta > 0 \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon)} \\ \text{cut, } \mathbb{R}, \exists L \frac{\varepsilon > 0, W > 0, \textcircled{A} \vdash \exists \delta > 0 \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon)}{\textcircled{A}, \varepsilon > 0 \vdash \exists \delta > 0 \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon)} \\ \text{cut, } \mathbb{R}, \exists L \frac{\varepsilon > 0 \vdash \exists \delta > 0 \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon)}{\textcircled{A}, \varepsilon > 0 \vdash \exists \delta > 0 \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon)} \\ \text{VR, } \rightarrow R \frac{}{\vdash \text{UStab}(\alpha_{\text{state}})} \end{array}$$

The derivation continues from the open premise by Skolemizing with  $\forall R, \rightarrow R$  and proving the LHS of the implication in  $\textcircled{B}$  with  $\forall L, \rightarrow L$ . Then, the loop rule is used with the stability loop invariant  $\text{Inv}_s \equiv \|x\| < \varepsilon \wedge V < W$ . This results in three premises,  $\textcircled{1}$  which shows that the invariant is implied by the initial antecedent assumptions,  $\textcircled{2}$ , the crucial premise, which shows that the invariant  $\text{Inv}_s$  is preserved across the loop body of  $\alpha_{\text{state}}$ , and  $\textcircled{3}$  which shows that the invariant implies the postcondition. These premises are shown and proved further below.

$$\frac{\begin{array}{c} \textcircled{1} \quad \textcircled{2} \quad \textcircled{3} \\ \text{loop} \frac{\textcircled{A}, \delta \leq \varepsilon, \|x\| < \delta, V < W \vdash [\alpha_{\text{state}}] \|x\| < \varepsilon}{\textcircled{A}, \delta \leq \varepsilon, \textcircled{B} \vdash \|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon} \\ \forall L, \rightarrow L \frac{}{\textcircled{A}, \delta \leq \varepsilon, \textcircled{B} \vdash \|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon} \\ \text{VR, } \rightarrow R \frac{}{\textcircled{A}, \delta \leq \varepsilon, \textcircled{B} \vdash \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon)} \end{array}$$

Premise  $\textcircled{1}$  proves by  $\mathbb{R}$  from the antecedents using the inequality  $\|x\| < \delta$  and  $\delta \leq \varepsilon$ .

$$\frac{}{\mathbb{R} \delta \leq \varepsilon, \|x\| < \delta, V < W \vdash \text{Inv}_s} *$$

Premise  $\textcircled{3}$  proves trivially since the postcondition  $\|x\| < \varepsilon$  is part of the loop invariant:

$$\frac{}{\mathbb{R} \text{Inv}_s \vdash \|x\| < \varepsilon} *$$

The derivation continues from premise  $\textcircled{2}$  by unfolding the loop body of  $\alpha_{\text{state}}$  with  $[\cup], \wedge R$ . This results in one premise for each switching choice  $p \in \mathcal{P}$ , indexed below by  $p$ .

$$\frac{\textcircled{A}, \text{Inv}_s \vdash [x' = f_p(x) \& Q_p] \text{Inv}_s}{[\cup], \wedge R \textcircled{A}, \text{Inv}_s \vdash [\bigcup_{p \in \mathcal{P}} x' = f_p(x) \& Q_p] \text{Inv}_s}$$

Each of these  $p \in \mathcal{P}$  premises is an ODE invariance question, which is decidable in dL [35]. The derivation below shows how to derive arithmetical conditions on  $V$  from these premises. The right conjunct of  $\text{Inv}_s$ ,  $V < W$ , is added to the domain constraint with a dC step; the cut premise is labeled  $\textcircled{4}$  and proved below. A subsequent dC step adds  $\|x\| \neq \varepsilon$  to the domain constraint using the contrapositive of antecedent  $\textcircled{A}$  and the derivation is completed with rule Barr since the resulting assumptions are contradictory.

$$\frac{\begin{array}{c} \mathbb{R} \frac{}{\|x\| \neq \varepsilon, \|x\| = \varepsilon \vdash \text{false}} \\ \text{Barr} \frac{\|x\| < \varepsilon \vdash [x' = f_p(x) \& Q_p] \wedge V < W \wedge \|x\| \neq \varepsilon \vdash \|x\| < \varepsilon}{\textcircled{A}, \|x\| < \varepsilon \vdash [x' = f_p(x) \& Q_p] \wedge V < W \wedge \|x\| < \varepsilon} \textcircled{4} \\ \text{dC} \frac{}{\textcircled{A}, \text{Inv}_s \vdash [x' = f_p(x) \& Q_p] \text{Inv}_s} \end{array}$$

The derivation from  $\textcircled{4}$  is completed with a  $\text{dL}_{\geq}$  step whose resulting arithmetic is implied by the bottom premise of rule CLF.

$$\frac{\mathbb{R} \frac{}{Q_p \vdash \mathcal{L}_{f_p}(V) \leq 0}}{\text{dL}_{\geq} V < W \vdash [x' = f_p(x) \& Q_p] V < W} *$$

*Pre-attractivity.* The derivation for pre-attractivity begins by Skolemizing  $\delta, \varepsilon$  with  $\forall R, \rightarrow R$ , followed by a series of arithmetic cuts which are justified stepwise. First, the Lyapunov function  $V$  is bounded above on the ball characterized by  $\|x\| < \delta$ , which justifies a cut of the formula  $\exists W > 0 \textcircled{A}$  with  $\textcircled{A} \equiv \forall x (\|x\| < \delta \rightarrow V < W)$ . After Skolemizing the upper bound  $W$ , note that the set characterized by formula  $V \leq W$  is compact by radial unboundedness (middle premise of rule CLF). Therefore, the set characterized by formula  $V \leq W \wedge \|x\| \geq \varepsilon$  is an intersection of a compact and closed set, which is itself compact. Thus,  $V$  attains a minimum  $U$  on that set which, by the first (topmost) premise is positive. This justifies the next arithmetic cut of the formula  $\exists U > 0 \textcircled{B}$  with  $\textcircled{B} \equiv \forall x (V \leq W \wedge \|x\| \geq \varepsilon \rightarrow V \geq U)$ , where  $U$  is subsequently Skolemized with  $\exists L$ . The steps are shown below, with the box modality in  $\text{UGpAttr}(\alpha_{\text{state}})$  temporarily hidden with  $\dots$  as it is not relevant for this part of the derivation.

$$\frac{\begin{array}{c} \varepsilon > 0, W > 0, \textcircled{A}, U > 0, \textcircled{B} \vdash \exists T \geq 0 \forall x (\|x\| < \delta \rightarrow \dots) \\ \text{cut, } \mathbb{R}, \exists L \frac{\varepsilon > 0, W > 0, \textcircled{A} \vdash \exists T \geq 0 \forall x (\|x\| < \delta \rightarrow \dots)}{\textcircled{A}, \varepsilon > 0 \vdash \exists T \geq 0 \forall x (\|x\| < \delta \rightarrow \dots)} \\ \text{cut, } \mathbb{R}, \exists L \frac{\varepsilon > 0 \vdash \exists T \geq 0 \forall x (\|x\| < \delta \rightarrow \dots)}{\textcircled{A}, \varepsilon > 0 \vdash \exists T \geq 0 \forall x (\|x\| < \delta \rightarrow \dots)} \\ \text{VR, } \rightarrow R \frac{}{\vdash \text{UGpAttr}(\alpha_{\text{state}})} \end{array}$$

Intuitively (see Fig. 1) the next arithmetic steps syntactically determine  $T \geq 0$  such that the value of  $V$  is guaranteed to decrease from  $W$  to  $U$  along all switching trajectories within time  $T$ . Consider the set characterized by formula  $Q_p \wedge U \leq V \leq W$ , which is the set of states (before reaching  $V < U$ ) where switching to ODE  $x' = f_p(x)$  &  $Q_p, p \in \mathcal{P}$  is possible. From the third (bottom) premise of rule CLF,  $\mathcal{L}_{f_p}(V)$  is negative on the set characterized by the formula  $\overline{Q_p} \wedge U \leq V \leq W$  because conjunct  $U \leq V$  bounds the set away from the origin as  $U > 0$ . Using radial unboundedness again,  $V \leq W$  is compact, so the set characterized by  $\overline{Q_p} \wedge U \leq V \leq W$  is an intersection of closed sets and compact sets which is therefore compact. Accordingly,  $\mathcal{L}_{f_p}(V)$  attains a maximum value  $k_p < 0$  on that set, which justifies the following arithmetic cut, where the bound  $k < 0$  is chosen uniformly across all choices of  $p$ , e.g., as the maximum over all  $k_p$  for  $p \in \mathcal{P}$ :

$$\frac{\exists k < 0 \bigwedge_{p \in \mathcal{P}} \forall x (Q_p \wedge U \leq V \leq W \rightarrow \mathcal{L}_{f_p}(V) \leq k)}{\textcircled{C}}$$

After Skolemizing  $k$ , it suffices to pick  $T \geq 0$  for the succedent such that  $W + kT \leq U$ . Such a  $T$  always exists since  $k < 0$ .

$$\frac{\begin{array}{c} \textcircled{A}, \textcircled{B}, k < 0, \textcircled{C}, W + kT \leq U \vdash \forall x (\|x\| < \delta \rightarrow \dots) \\ \exists R \frac{\varepsilon > 0, W > 0, \textcircled{A}, U > 0, \textcircled{B}, k < 0, \textcircled{C} \vdash \exists T \geq 0 \forall x (\|x\| < \delta \rightarrow \dots)}{\textcircled{A}, \varepsilon > 0 \vdash \exists T \geq 0 \forall x (\|x\| < \delta \rightarrow \dots)} \\ \text{cut, } \mathbb{R}, \exists L \frac{}{\textcircled{A}, \varepsilon > 0 \vdash \exists T \geq 0 \forall x (\|x\| < \delta \rightarrow \dots)} \end{array}$$

The derivation continues by Skolemizing with  $\forall R, \rightarrow R$  and proving the LHS of the implication in  $\textcircled{A}$  with  $\forall L, \rightarrow L$ . The assignment  $t := 0$  is unfolded with axioms  $[\cdot], [\cdot := \cdot]$ , then the loop rule is used with the pre-attractivity loop invariant  $\text{Inv}_a \equiv V < W \wedge (V \geq U \rightarrow V < W + kt)$ . Similar to the stability derivation, this results in three premises, where the crucial premise  $\textcircled{2}$  requires showing that  $\text{Inv}_a$  is preserved across the loop body, while the other premises are labeled  $\textcircled{1}$  and  $\textcircled{3}$  (all three premises are shown further below).

$$\begin{array}{c}
\text{loop} \frac{\textcircled{1} \quad \textcircled{2} \quad \textcircled{3}}{V < W, \textcircled{B}, k < 0, \textcircled{C}, W + kT \leq U, t = 0 \vdash [\alpha_{\text{state}}, t' = 1] \dots} \\
[\cdot], \vdash \frac{V < W, \textcircled{B}, k < 0, \textcircled{C}, W + kT \leq U \vdash [t := 0; \alpha_{\text{state}}, t' = 1] \dots}{V < W, \textcircled{B}, k < 0, \textcircled{C}, W + kT \leq U, \|x\| < \delta \vdash [t := 0; \alpha_{\text{state}}, t' = 1] \dots} \\
\text{VL}, \rightarrow \text{L} \frac{\textcircled{A}, \textcircled{B}, k < 0, \textcircled{C}, W + kT \leq U, \|x\| < \delta \vdash [t := 0; \alpha_{\text{state}}, t' = 1] \dots}{\textcircled{A}, \textcircled{B}, k < 0, \textcircled{C}, W + kT \leq U \vdash \forall x (\|x\| < \delta \rightarrow \dots)} \\
\text{VR}, \rightarrow \text{R}
\end{array}$$

Premise ① proves by  $\mathbb{R}$  from the antecedents.

$$\frac{*}{\mathbb{R} V < W, t = 0 \vdash \text{Inv}_a}$$

Premise ③ proves by  $\mathbb{R}$  from the loop invariant using the following arithmetic argument. Suppose for contradiction that there is a state satisfying the negation of the postcondition, i.e., assume the negation  $t \geq T \wedge \|x\| \geq \varepsilon$ . Then, using the left conjunct of  $\text{Inv}_a$  together with  $\|x\| \geq \varepsilon$  to prove the LHS of the implication in  $\textcircled{B}$  gives assumption  $V \geq U$ . The right conjunct of  $\text{Inv}_a$  then yields the chain of inequalities  $V < W + kt \leq W + kT \leq U$ , which is a contradiction. The steps are outlined below.

$$\begin{array}{c}
\textcircled{A}, \delta \leq \varepsilon, \textcircled{B} \vdash \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon) \\
\textcircled{A}, 0 < \delta \leq \varepsilon, \textcircled{B} \vdash \exists \delta > 0 \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon) \\
\text{cut, } \mathbb{R}, \exists \text{L} \frac{\varepsilon > 0, W > 0, \textcircled{A} \vdash \exists \delta > 0 \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon)}{\varepsilon > 0 \vdash \exists \delta > 0 \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon)} \\
\text{cut, } \mathbb{R}, \exists \text{L} \frac{\varepsilon > 0 \vdash \exists \delta > 0 \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon)}{\vdash \text{UStab}(\alpha_{\text{state}})} \\
\text{VR}, \rightarrow \text{R}
\end{array}$$

**Stability.** The derivation for stability similarly begins with cut and Skolemization steps. The difference compared to the derivation of rule CLF is the cut formulas are now conjunctions over all possible modes  $p \in \mathcal{P}$  for the Lyapunov functions  $V_p$ . The first cut is  $\exists W > 0$   $\textcircled{A}$  with  $\textcircled{A} \equiv \bigwedge_{p \in \mathcal{P}} \forall x (\|x\| = \varepsilon \rightarrow V_p \geq W)$ , where the upper bound  $W > 0$  is chosen to be the maximum of the respective bounds for each  $V_p$  on the compact set characterized by  $\|x\| = \varepsilon$ . After Skolemizing  $W$ , the second arithmetic cut is the formula  $\exists \delta (0 < \delta \leq \varepsilon \wedge \textcircled{B})$  with  $\textcircled{B} \equiv \bigwedge_{p \in \mathcal{P}} \forall x (\|x\| < \delta \rightarrow V_p < W)$ . Such a  $\delta$  exists by continuity for each  $V_p, p \in \mathcal{P}$  since  $V_p(0) = 0$  from the first (topmost) premise of rule MLF. After both cuts, the antecedent  $\delta$  is used to witness the succedent by  $\exists \mathbb{R}$ .

$$\begin{array}{c}
\textcircled{A}, \delta \leq \varepsilon, \textcircled{B} \vdash \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon) \\
\textcircled{A}, 0 < \delta \leq \varepsilon, \textcircled{B} \vdash \exists \delta > 0 \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon) \\
\text{cut, } \mathbb{R}, \exists \text{L} \frac{\varepsilon > 0, W > 0, \textcircled{A} \vdash \exists \delta > 0 \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon)}{\varepsilon > 0 \vdash \exists \delta > 0 \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon)} \\
\text{cut, } \mathbb{R}, \exists \text{L} \frac{\varepsilon > 0 \vdash \exists \delta > 0 \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon)}{\vdash \text{UStab}(\alpha_{\text{state}})} \\
\text{VR}, \rightarrow \text{R}
\end{array}$$

The derivation continues with logical simplification steps, Skolemizing the succedent and then proving the LHS of the implications in antecedent  $\textcircled{B}$ .

$$\begin{array}{c}
\textcircled{A}, \delta \leq \varepsilon, \|x\| < \delta, \bigwedge_{p \in \mathcal{P}} V_p < W \vdash [\alpha_{\text{state}}] \|x\| < \varepsilon \\
\text{VL}, \rightarrow \text{L} \frac{\textcircled{A}, \delta \leq \varepsilon, \textcircled{B}, \|x\| < \delta \vdash [\alpha_{\text{state}}] \|x\| < \varepsilon}{\textcircled{A}, \delta \leq \varepsilon, \textcircled{B} \vdash \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{state}}] \|x\| < \varepsilon)} \\
\text{VR}, \rightarrow \text{R}
\end{array}$$

Next, a cut,  $\forall \text{L}$  step case splits on whether the switched system is initially in its domain of definition characterized by formula  $Q \equiv \bigvee_{p \in \mathcal{P}} Q_p$ . The case where the system is *not* in its domain is labeled  $\textcircled{0}$ , and the proof of this case is deferred to the end. In case the system is in its domain, the loop rule is used with stability loop invariant  $\text{Inv}_s \equiv \|x\| < \varepsilon \wedge \bigvee_{p \in \mathcal{P}} (Q_p \wedge V_p < W)$ . This yields three premises labeled ①–③ shown and proved further below.

$$\begin{array}{c}
\textcircled{1} \quad \textcircled{2} \quad \textcircled{3} \\
\text{loop} \frac{\textcircled{A}, \delta \leq \varepsilon, \|x\| < \delta, \bigwedge_{p \in \mathcal{P}} V_p < W, Q \vdash [\alpha_{\text{state}}] \|x\| < \varepsilon}{\textcircled{A}, \delta \leq \varepsilon, \|x\| < \delta, \bigwedge_{p \in \mathcal{P}} V_p < W \vdash [\alpha_{\text{state}}] \|x\| < \varepsilon} \textcircled{0} \\
\text{cut, } \forall \text{L}
\end{array}$$

Premise ① proves by  $\mathbb{R}$  from the antecedents using the inequalities  $\|x\| < \delta$  and  $\delta \leq \varepsilon$  for the left conjunct and propositionally from antecedents  $Q$  and  $\bigwedge_{p \in \mathcal{P}} V_p < W$  for the right conjunct.

$$\frac{*}{\mathbb{R} \delta \leq \varepsilon, \|x\| < \delta, \bigwedge_{p \in \mathcal{P}} V_p < W, Q \vdash \text{Inv}_s}$$

Premise ③ proves trivially since the postcondition  $\|x\| < \varepsilon$  is part of the loop invariant:

$$\frac{*}{\mathbb{R} \text{Inv}_s \vdash \|x\| < \varepsilon}$$

The derivation continues from premise ② by unfolding the loop body of  $\alpha_{\text{state}}$  with  $[\cdot], \wedge \text{R}$ . Premises are indexed by  $p \in \mathcal{P}$  in the derivation. The  $\text{M}[\cdot]$  step propositionally strengthens the postcondition to its constituent disjunct  $\|x\| < \varepsilon \wedge V_p < W$  for the chosen mode  $p$ . Then,  $\text{DX}$  assumes domain  $Q_p$  in the antecedent and a cut step adds the assumption  $\|x\| < \varepsilon \wedge V_p < W$ . This cut corresponds to the last (bottom) premise of rule MLF. It is labeled ④ and explained below. The rest of the proof after the cut proceeds identically to the corresponding derivation for rule CLF using the respective conjunct for  $p \in \mathcal{P}$  from  $\textcircled{A}$ . The steps are omitted here.

The proof for premise ② proceeds by unfolding the loop body with  $[\cdot], \wedge \text{R}$ , yielding one premise for each switching choice  $p \in \mathcal{P}$ . A dC step proves the invariance of the left conjunct  $V < W$  of  $\text{Inv}_a$  with  $\text{dI}_{\geq}$  (see the stability proof, sublevel sets of  $V$  are invariant). The right conjunct of  $\text{Inv}_a$  is the implication abbreviated  $I \equiv V \geq U \rightarrow V < W + kt$  and this is proved below using axiom DCC, which results in premises ④ and ⑤ (shown and proved further below).

$$\begin{array}{c}
\textcircled{4} \quad \textcircled{5} \\
\text{DCC, } \wedge \text{R} \frac{\textcircled{C}, I \vdash [x' = f_p(x), t' = 1 \& Q_p \wedge V < W] I}{\textcircled{C}, \text{Inv}_a \vdash [x' = f_p(x), t' = 1 \& Q_p] \text{Inv}_a} \\
\text{dC, } \text{dI}_{\geq} \frac{\textcircled{C}, \text{Inv}_a \vdash [x' = f_p(x), t' = 1 \& Q_p] \text{Inv}_a}{[\cdot], \wedge \text{R} \textcircled{C}, \text{Inv}_a \vdash [\bigvee_{p \in \mathcal{P}} x' = f_p(x), t' = 1 \& Q_p] \text{Inv}_a}
\end{array}$$

From premise ④, the proof is completed with a  $\text{dI}_{\geq}$  step using the quantified assumption  $\textcircled{C}$  and the domain constraint. Note that the Lie derivative of the RHS  $W + kt$  is  $k$  using  $t' = 1$ .

$$\begin{array}{c}
\frac{*}{\mathbb{R} \textcircled{C}, Q_p \wedge V < W \wedge V \geq U \vdash \mathcal{L}_{f_p}(V) \leq k} \\
\text{dI}_{\geq} \frac{\textcircled{C}, I \vdash [x' = f_p(x), t' = 1 \& Q_p \wedge V < W \wedge V \geq U] V < W + kt}{\textcircled{C}, I \vdash [x' = f_p(x), t' = 1 \& Q_p \wedge V < W \wedge V \geq U] V < W + kt}
\end{array}$$

From premise ⑤, the proof is completed with a generalization G step followed by  $\text{dI}_{\geq}$  to prove the invariance of formula  $V < U$  (see the stability proof, sublevel sets of  $V$  are invariant). The ODE in the outer box modality is elided with  $\dots$  here.

$$\begin{array}{c}
\frac{*}{\text{dI}_{\geq} \frac{V < U \vdash [x' = f_p(x), t' = 1 \& Q_p \wedge V < W] V < U}{G, \rightarrow \text{R} \vdash [\dots] (V < U \rightarrow [x' = f_p(x), t' = 1 \& Q_p \wedge V < W] V < U)} \square
\end{array}$$

**PROOF OF COROLLARY 4.** The derivation of rule MLF builds on the ideas of the derivation of rule CLF so similar proof steps are explained in less detail here. The derivation starts with an  $\wedge \text{R}$  step for the stability and pre-attractivity conjuncts which are proved separately below.

$$\begin{array}{c}
\vdash \text{UStab}(\alpha_{\text{state}}) \quad \vdash \text{UGpAttr}(\alpha_{\text{state}}) \\
\wedge \text{R} \frac{\vdash \text{UStab}(\alpha_{\text{state}}) \quad \vdash \text{UGpAttr}(\alpha_{\text{state}})}{\vdash \text{UGpAS}(\alpha_{\text{state}})}
\end{array}$$





Returning to premise ①, similar to the case for stability, initial states satisfying  $\neg Q$  have no continuous motion possible so they are stuck at the initial state (with global clock  $t = 0$ ). This is proved using the loop invariant  $Inv_a^0 \equiv t = 0 \wedge \neg Q$ . The first and third premise resulting from the loop rule are proved trivially (not shown below). For the remaining premise,  $\neg Q$  is preserved (trivially) across the loop body after unfolding it with  $[\cup]$ ,  $\wedge R$  and using DX to show that the system is unable to switch to the ODE with domain  $Q_p$ .

$$\begin{array}{c} \text{DX} \quad \frac{\neg Q, Q_p \vdash \text{false}}{\neg Q \vdash [x' = f_p(x), t' = 1 \& Q_p] Inv_a^0} \\ [\cup], \wedge R \quad \frac{Inv_a^0 \vdash [\bigcup_{p \in \mathcal{P}} x' = f_p(x), t' = 1 \& Q_p] Inv_a^0}{T > 0, t = 0, \neg Q \vdash [\alpha_{\text{state}}, t' = 1](t \geq T \rightarrow \|x\| < \varepsilon)} \quad \square \end{array}$$

**PROOF OF COROLLARY 5.** The derivation of rule  $MLF_G$  is similar to MLF, but adapted to the shape of the guarded switching model  $\alpha_{\text{guard}}$  and its corresponding loop invariants. The derivation starts with an  $\wedge R$  step for the stability and pre-attractivity conjuncts which are proved separately below.

$$\frac{\vdash \text{UStab}(\alpha_{\text{guard}}) \quad \vdash \text{UGpAttr}(\alpha_{\text{guard}})}{\wedge R \quad \vdash \text{UGpAS}(\alpha_{\text{guard}})}$$

**Stability.** The derivation for stability proceeds identically to the derivation for rule MLF until the step before the stability loop invariant is used. These steps are omitted below with  $\dots$  and the resulting premise has antecedent formula abbreviated ①  $\equiv \bigwedge_{p \in \mathcal{P}} \forall x (\|x\| = \varepsilon \rightarrow V_p \geq W)$ .

$$\frac{\text{①}, \delta \leq \varepsilon, \|x\| < \delta, \bigwedge_{p \in \mathcal{P}} V_p < W \vdash [\alpha_{\text{guard}}] \|x\| < \varepsilon}{\vdash \text{UStab}(\alpha_{\text{guard}})}$$

The derivation continues using the loopT rule with stability loop invariant  $Inv_s \equiv \|x\| < \varepsilon \wedge \bigvee_{p \in \mathcal{P}} (u = p \wedge V_p < W)$ . This yields four premises labeled ①–④, shown and proved further below.

$$\text{loopT} \frac{\text{①} \quad \text{②} \quad \text{③} \quad \text{④}}{\text{①}, \delta \leq \varepsilon, \|x\| < \delta, \bigwedge_{p \in \mathcal{P}} V_p < W \vdash [\alpha_{\text{guard}}] \|x\| < \varepsilon}$$

Premise ① shows that the system state satisfies the invariant  $Inv_s$  after running the initialization program  $\alpha_i \equiv \bigcup_{p \in \mathcal{P}} u := p$ . This is proved by  $\mathbb{R}$  after unfolding  $\alpha_i$  using  $[\cup]$ ,  $[\cdot]$ .

$$\frac{\mathbb{R} \quad \delta \leq \varepsilon, \|x\| < \delta, \bigwedge_{p \in \mathcal{P}} V_p < W, u = p \vdash Inv_s}{[\cup], [\cdot] \quad \delta \leq \varepsilon, \|x\| < \delta, \bigwedge_{p \in \mathcal{P}} V_p < W \vdash [\alpha_i] Inv_s}$$

Premise ④ proves trivially since the postcondition  $\|x\| < \varepsilon$  is part of the loop invariant.

$$\frac{*}{\mathbb{R} \quad Inv_s \vdash \|x\| < \varepsilon}$$

The derivation from premise ② yields *correct-by-construction* arithmetical conditions on the Lyapunov functions from unfolding the guarded switching controller in  $\alpha_{\text{guard}}$ . recall

$$\alpha_u \equiv \bigcup_{p \in \mathcal{P}} \left( ?u = p; \bigcup_{q \in \mathcal{P}} (?G_{p,q}; u := q) \right)$$

Axiom  $[\cup]$  unfolds the outer choice  $\bigcup_{p \in \mathcal{P}} (\cdot)$ , yielding one premise for each mode  $p \in \mathcal{P}$ . Then, axioms  $[\cdot]$ ,  $[\cdot]$  add the current mode  $u = p$  (before switching) to the assumptions. The cut step propositionally unfolds antecedent loop invariant assumption  $Inv_s$  to the corresponding disjunct for  $u = p$ . The inner choice  $\bigcup_{q \in \mathcal{P}} (\cdot)$  is unfolded next with axioms  $[\cup]$ ,  $[\cdot]$ ,  $[\cdot]$ , yielding one

premise for each possible transition to mode  $q \in \mathcal{P}$  guarded by formula  $G_{p,q}$ . The assignment  $u := q$  is unfolded with  $[\cdot]$ , so the succedent simplifies to the disjunct for  $u = q$  in  $Inv_s$ . An arithmetic simplification step yields the bottom premise of rule  $MLF_G$ .

$$\begin{array}{c} \mathbb{R} \quad \frac{*}{G_{p,q} \vdash V_p \leq V_p} \\ \mathbb{R} \quad \frac{V_p < W, G_{p,q} \vdash V_p < W}{\|x\| < \varepsilon, V_p < W, G_{p,q} \vdash [u := q] Inv_s} \\ [\cdot], [\cdot], [\cdot] \quad \frac{\|x\| < \varepsilon, V_p < W \vdash [\bigcup_{q \in \mathcal{P}} (?G_{p,q}; u := q)] Inv_s}{Inv_s, u = p \vdash [\bigcup_{q \in \mathcal{P}} (?G_{p,q}; u := q)] Inv_s} \\ \text{cut} \quad \frac{Inv_s, u = p \vdash [\bigcup_{q \in \mathcal{P}} (?G_{p,q}; u := q)] Inv_s}{Inv_s \vdash [?u = p; \bigcup_{q \in \mathcal{P}} (?G_{p,q}; u := q)] Inv_s} \\ [\cdot], [\cdot] \quad \frac{Inv_s \vdash [?u = p; \bigcup_{q \in \mathcal{P}} (?G_{p,q}; u := q)] Inv_s}{Inv_s \vdash [\alpha_u] Inv_s} \\ [\cup] \end{array}$$

The derivation from premise ③ unfolds the plant model  $\alpha_p \equiv \bigcup_{p \in \mathcal{P}} (?u = p; x' = f_p(x, y) \& Q_p)$ . The choice  $\bigcup_{p \in \mathcal{P}} (\cdot)$  is unfolded first with axiom  $[\cup]$ , yielding one premise for each mode  $p \in \mathcal{P}$ . Then, axioms  $[\cdot]$ ,  $[\cdot]$  adds the mode selected by  $\alpha_u$  to the antecedent, where the antecedent loop invariant assumption  $Inv_s$  is simplified by cut to the disjunct for  $u = p$ . Similarly  $M[\cdot]$  strengthens the postcondition to the disjunct for  $u = p$ . The rest of the proof proceeds identically to the corresponding derivation for rule CLF so it is omitted here.

$$\begin{array}{c} \mathbb{M}[\cdot] \quad \frac{*}{\text{①}, \|x\| < \varepsilon, V_p < W \vdash [x' = f_p(x) \& Q_p](\|x\| < \varepsilon \wedge V_p < W)} \\ \text{cut} \quad \frac{\text{①}, \|x\| < \varepsilon, V_p < W, u = p \vdash [x' = f_p(x) \& Q_p] Inv_s}{\text{①}, Inv_s, u = p \vdash [x' = f_p(x) \& Q_p] Inv_s} \\ [\cdot], [\cdot] \quad \frac{\text{①}, Inv_s, u = p \vdash [x' = f_p(x) \& Q_p] Inv_s}{\text{①}, Inv_s \vdash [?u = p; x' = f_p(x, y) \& Q_p] Inv_s} \\ [\cup] \quad \frac{\text{①}, Inv_s \vdash [?u = p; x' = f_p(x, y) \& Q_p] Inv_s}{\text{①}, Inv_s \vdash [\alpha_p] Inv_s} \end{array}$$

**Pre-attractivity.** The derivation for pre-attractivity is also identical to MLF until the step before the pre-attractivity loop invariant is used. These steps are omitted below with  $\dots$  and the resulting premise has antecedent formulas abbreviated with:

$$\begin{array}{c} \text{⑥} \equiv \bigwedge_{p \in \mathcal{P}} \forall x (V_p \leq W \wedge \|x\| \geq \varepsilon \rightarrow V_p \geq U) \\ \text{⑦} \equiv \bigwedge_{p \in \mathcal{P}} \forall x (Q_p \wedge U \leq V_p \leq W \rightarrow \mathcal{L}_{f_p}(V_p) \leq k) \\ \bigwedge_{p \in \mathcal{P}} V_p < W, \text{⑥}, k < 0, \text{⑦}, W + kT \leq U, t = 0 \vdash [\alpha_{\text{guard}}, t' = 1] \dots \\ \vdash \text{UGpAttr}(\alpha_{\text{guard}}) \end{array}$$

The derivation continues using the loopT rule with pre-attractivity loop invariant  $Inv_a \equiv \bigvee_{p \in \mathcal{P}} (u = p \wedge V_p < W \wedge (V_p \geq U \rightarrow V_p < W + kt))$ . This yields four premises labeled ①–④ which are shown and proved further below.

$$\text{loopT} \frac{\text{①} \quad \text{②} \quad \text{③} \quad \text{④}}{\bigwedge_{p \in \mathcal{P}} V_p < W, \text{⑥}, k < 0, \text{⑦}, W + kT \leq U, t = 0 \vdash [\alpha_{\text{guard}}, t' = 1] \dots}$$

Premise ① proves the invariant  $Inv_a$  after unfolding the initialization program  $\alpha_i$  using  $[\cup]$ ,  $[\cdot]$ .

$$\frac{\mathbb{R} \quad \frac{*}{\bigwedge_{p \in \mathcal{P}} V_p < W, t = 0, u = p \vdash Inv_a}}{[\cup], [\cdot] \quad \bigwedge_{p \in \mathcal{P}} V_p < W, t = 0 \vdash [\alpha_i] Inv_a}$$

Premise ④ is proved by  $\mathbb{R}$  after unfolding the disjuncts of the loop invariant with  $\vee L$  (the arithmetical argument is identical to earlier proofs). The selected disjunct (indexed by  $p$ ) is abbreviated  $R \equiv u = p \wedge V_p < W \wedge (V_p \geq U \rightarrow V_p < W + kt)$ .

$$\frac{\mathbb{R} \quad \textcircled{b}, k < 0, W + kT \leq U, R \vdash t \geq T \rightarrow \|x\| < \varepsilon}{\text{VL} \quad \textcircled{b}, k < 0, W + kT \leq U, \text{Inv}_a \vdash t \geq T \rightarrow \|x\| < \varepsilon} *$$

The derivation from premise ② unfolds  $\alpha_u$  using dL's hybrid program axioms similar to the stability proof, and an arithmetic simplification step yields the premises of  $\text{MLF}_G$  for guarded mode switches from  $p$  to  $q$ ,  $p, q \in \mathcal{P}$ .

$$\frac{\mathbb{R} \quad \frac{\mathbb{R} \quad G_{p,q} \vdash V_q \leq V_p}{\mathbb{R} \quad R, G_{p,q} \vdash V_q < W \wedge (V_q \geq U \rightarrow V_q < W + kt)} \quad \text{[:=]} \quad \frac{R, G_{p,q} \vdash [u := q] \text{Inv}_a}{\text{cut} \quad \frac{\text{Inv}_a, u = p \vdash [\bigcup_{q \in \mathcal{P}} (?G_{p,q}; u := q)] \text{Inv}_a}{[\cdot, ?] \quad \frac{\text{Inv}_a \vdash [?u = p; \bigcup_{q \in \mathcal{P}} (?G_{p,q}; u := q)] \text{Inv}_a}{[\cdot] \quad \text{Inv}_a \vdash [\alpha_u] \text{Inv}_a}} *$$

The derivation from premise ③ unfolds the plant model and then proceeds identically to the corresponding derivation for rule CLF.

$$\frac{\mathbb{M}[\cdot] \quad \frac{\mathbb{C}, R \vdash [x' = f_p(x), t' = 1 \& Q_p] R}{\mathbb{C}, R \vdash [x' = f_p(x), t' = 1 \& Q_p] \text{Inv}_a} \quad \text{cut} \quad \frac{\mathbb{C}, \text{Inv}_a, u = p \vdash [x' = f_p(x), t' = 1 \& Q_p] \text{Inv}_a}{[\cdot, ?] \quad \frac{\mathbb{C}, \text{Inv}_a \vdash [?u = p; x' = f_p(x, y), t' = 1 \& Q_p] \text{Inv}_a}{[\cdot] \quad \mathbb{C}, \text{Inv}_a \vdash [\alpha_p, t' = 1] \text{Inv}_a}} *$$

**PROOF OF COROLLARY 6.** The derivation of rule  $\text{MLF}_\tau$  departs more significantly from the derivations of rules CLF, MLF,  $\text{MLF}_G$ . For this proof,  $\mathbb{R}_{\text{exp}}$  is used to indicate arithmetic steps that use properties of the real exponential function. Tools are available for answering such questions [14] although they are not known to be decidable; additional explanation is given below for steps that only require elementary properties of the exponential function. The proof also shows how to derive arithmetic conditions (arising from the time-dependent switching controller) in a correct by construction manner. Recall from that the modes  $p \in \mathcal{P}$  are partitioned into two subsets consisting of the stable  $\mathcal{S} = \{p \in \mathcal{P}, \lambda_p > 0\}$  and unstable  $\mathcal{U} = \{p \in \mathcal{P}, \lambda_p \leq 0\}$  modes. The derivation starts with an  $\wedge R$  step for the stability and pre-attractivity conjuncts which are proved separately below.

$$\frac{\vdash \text{UStab}(\alpha_{\text{time}}) \quad \vdash \text{UGpAttr}(\alpha_{\text{time}})}{\wedge R \quad \vdash \text{UGpAS}(\alpha_{\text{time}})}$$

**Stability.** The stability derivation begins with cut and Skolemization steps. The first cut is  $\exists W > 0$  ① with the abbreviation ①  $\equiv \bigwedge_{p \in \mathcal{P}} \forall x (\|x\| = \varepsilon \rightarrow V_p \geq W)$ , where the upper bound  $W > 0$  is chosen to be the maximum of the respective bounds for each  $V_p$  on the compact set characterized by  $\|x\| = \varepsilon$ . After Skolemizing  $W$ , the second arithmetic cut is the formula  $\exists \delta (0 < \delta \leq \varepsilon \wedge \textcircled{b})$ , where the conjuncts for  $p \in \mathcal{U}$  use  $e^{\lambda_p \Theta_p} > 0$ .

$$\textcircled{b} \equiv \bigwedge_{p \in \mathcal{S}} \forall x (\|x\| < \delta \rightarrow V_p < W) \wedge \bigwedge_{p \in \mathcal{U}} \forall x (\|x\| < \delta \rightarrow V_p < W e^{\lambda_p \Theta_p})$$

Such a  $\delta$  exists by continuity for each  $V_p, p \in \mathcal{P}$ ,  $V_p(0) = 0$  from the premise of rule  $\text{MLF}_\tau$ . After both cuts, the antecedent  $\delta$  is used to witness the succedent by  $\exists R$ .

$$\frac{\exists R \quad \frac{\textcircled{a}, \delta \leq \varepsilon, \textcircled{b} \vdash \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{time}}] \|x\| < \varepsilon)}{\text{cut, } \mathbb{R}_{\text{exp}}, \exists L \quad \frac{\varepsilon > 0, W > 0, \textcircled{a} \vdash \exists \delta > 0 \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{time}}] \|x\| < \varepsilon)}{\text{cut, } \mathbb{R}, \exists L \quad \frac{\varepsilon > 0 \vdash \exists \delta > 0 \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{time}}] \|x\| < \varepsilon)}{\vdash \text{UStab}(\alpha_{\text{time}})}} *$$

The derivation continues after both cuts similarly to MLF by unfolding and proving the LHS of the implications in antecedent ①. The resulting assumption on the initial state is abbreviated  $B \equiv \bigwedge_{p \in \mathcal{S}} V_p < W \wedge \bigwedge_{p \in \mathcal{U}} V_p < W e^{\lambda_p \Theta_p}$ . Then, the loopT rule is used with the following stability loop invariant  $\text{Inv}_s$ , which yields premises ①–④ shown and proved further below:

$$\text{Inv}_s \equiv \tau \geq 0 \wedge \|x\| < \varepsilon \wedge \left( \bigvee_{p \in \mathcal{S}} (u = p \wedge V_p < W e^{-\lambda_p \tau}) \vee \bigvee_{p \in \mathcal{U}} (u = p \wedge V_p < W e^{-\lambda_p (\tau - \Theta_p)} \wedge \tau \leq \Theta_p) \right)$$

$$\frac{\text{loopT} \quad \frac{\textcircled{1}, \delta \leq \varepsilon, \|x\| < \delta, B \vdash [\alpha_{\text{time}}] \|x\| < \varepsilon}{\text{VL}, \rightarrow L \quad \frac{\textcircled{a}, \delta \leq \varepsilon, \textcircled{b}, \|x\| < \delta \rightarrow [\alpha_{\text{time}}] \|x\| < \varepsilon}{\text{VR}, \rightarrow R \quad \textcircled{a}, \delta \leq \varepsilon, \textcircled{b} \vdash \forall x (\|x\| < \delta \rightarrow [\alpha_{\text{time}}] \|x\| < \varepsilon)}} \textcircled{1} \quad \textcircled{2} \quad \textcircled{3} \quad \textcircled{4}$$

Premise ① shows that the system state satisfies the invariant  $\text{Inv}_s$  after initialization with program  $\alpha_i \equiv \tau := 0; \bigcup_{p \in \mathcal{P}} u := p$ . This is proved from  $B$  after unfolding  $\alpha_i$  using  $[\cdot]$ ,  $[\cdot :=]$  and substituting  $\tau = 0$  in the loop invariant (using  $e^0 = 1$ ).

$$\frac{\mathbb{R}_{\text{exp}} \quad \delta \leq \varepsilon, \|x\| < \delta, B, \tau = 0, u = p \vdash \text{Inv}_s}{[\cdot], [\cdot :=]} \quad \delta \leq \varepsilon, \|x\| < \delta, B \vdash [\alpha_i] \text{Inv}_s$$

Premise ④ proves trivially since the postcondition  $\|x\| < \varepsilon$  is part of the loop invariant.

$$\frac{*}{\mathbb{R} \text{Inv}_s \vdash \|x\| < \varepsilon}$$

The derivation from premise ② unfolds the switching controller  $\alpha_u$  in  $\alpha_{\text{time}}$  with dL's hybrid program axioms, recall:

$$\alpha_u \equiv \bigcup_{p \in \mathcal{P}} \left( ?u = p; \bigcup_{q \in \mathcal{P}} (? \theta_{p,q} \leq \tau; \tau := 0; u := q) \right)$$

This unfolding yields four possible shapes of premises (abbreviated as ... and shown immediately below) for a switch from the current mode  $p$  to mode  $q$ . In each case, the antecedent assumption corresponds to the disjunct of  $\text{Inv}_s$  for mode  $p$ , while the succedent assumption corresponds to the disjunct for mode  $q$  with timer  $\tau$  reset to 0 by the switching controller. The four cases correspond to whether  $p \in \mathcal{S}$  or  $p \in \mathcal{U}$  and similarly for  $q$ , as labeled below.

$$\frac{\dots}{[\cdot], [\cdot], [\cdot], [\cdot :=]} \quad \frac{\text{Inv}_s, u = p \vdash [\bigcup_{q \in \mathcal{P}} (? \theta_{p,q} \leq \tau; \tau := 0; u := q)] \text{Inv}_s}{[\cdot], [\cdot]} \quad \frac{\text{Inv}_s \vdash [?u = p; \bigcup_{q \in \mathcal{P}} (? \theta_{p,q} \leq \tau; \tau := 0; u := q)] \text{Inv}_s}{[\cdot]} \quad \text{Inv}_s \vdash [\alpha_u] \text{Inv}_s$$

$$\begin{aligned} \theta_{p,q} \leq \tau, V_p &< W e^{-\lambda_p \tau} \vdash V_q < W & (p \in \mathcal{S}, q \in \mathcal{S}) \\ \theta_{p,q} \leq \tau, V_p &< W e^{-\lambda_p \tau} \vdash V_q < W e^{\lambda_q \Theta_q} & (p \in \mathcal{S}, q \in \mathcal{U}) \\ \theta_{p,q} \leq \tau, V_p &< W e^{-\lambda_p (\tau - \Theta_p)}, \tau \leq \Theta_p \vdash V_q < W & (p \in \mathcal{U}, q \in \mathcal{S}) \\ \theta_{p,q} \leq \tau, V_p &< W e^{-\lambda_p (\tau - \Theta_p)}, \tau \leq \Theta_p \vdash V_q < W e^{\lambda_q \Theta_q} & (p \in \mathcal{U}, q \in \mathcal{U}) \end{aligned}$$



The derivation continues by picking  $T \geq 0$  such that  $R \equiv W \leq Ue^{\sigma T} \wedge \bigwedge_{p \in \mathcal{U}} W \leq Ue^{\sigma T} e^{-\sigma \Theta_p}$ , such a  $T$  exists since  $\sigma > 0$ . The quantifiers in the succedent are unfolded and the LHS of the implications in ② are proved. The resulting antecedent (from ②) is abbreviated  $B \equiv \bigwedge_{p \in \mathcal{S}} V_p < W \wedge \bigwedge_{p \in \mathcal{U}} V_p < We^{\lambda_p \Theta_p}$ . The loopT rule is used with the following pre-attractivity loop invariant  $Inv_s$ , which yields premises ①–④ shown and proved further below:

$$Inv_a \equiv \tau \geq 0 \wedge t \geq \tau \wedge$$

$$\left( \bigvee_{p \in \mathcal{S}} (u = p \wedge V_p < W e^{-\sigma(t-\tau)} e^{-\lambda_p \tau}) \vee \bigvee_{p \in \mathcal{U}} (u = p \wedge V_p < W e^{-\sigma(t-\tau)} e^{-\lambda_p(\tau - \Theta_p)} \wedge \tau \leq \Theta_p) \right)$$

	①	②	③	④
loopT	$\textcircled{b}, T \geq 0, R, B, t = 0 \vdash [\alpha_{\text{guard}}, t' = 1] \dots$			
$\text{VL}, \rightarrow^{\text{L}}$	$\textcircled{a}, \textcircled{b}, T \geq 0, R, \ x\  < \delta, t = 0 \vdash [\alpha_{\text{guard}}, t' = 1] \dots$			
$[\cdot], :=$	$\textcircled{a}, \textcircled{b}, T \geq 0, R, \ x\  < \delta \vdash [t := 0; \alpha_{\text{guard}}, t' = 1] \dots$			
$\text{VR}, \rightarrow^{\text{R}}$	$\textcircled{a}, \textcircled{b}, T \geq 0, R \vdash \forall x (\ x\  < \delta \rightarrow \dots)$			
$\exists \mathbb{R}$	$\varepsilon > 0, W > 0, \textcircled{a}, U > 0, \textcircled{b} \vdash \exists T \geq 0 \forall x (\ x\  < \delta \rightarrow \dots)$			

Premise ① is proved by unfolding the initialization program  $\alpha_i$ . This is proved from  $B$  after unfolding  $\alpha_i$  using axioms  $[\cup]$ ,  $[\text{:=}]$  and substituting  $\tau = 0$  and  $t = 0$  in the loop invariant (using  $e^0 = 1$ ).

Premise ④ is proved by unfolding the loop invariant with  $\forall L$ . This yields two possible premise shapes, corresponding to  $p \in \mathcal{S}$  or  $p \in \mathcal{U}$ . In both cases, assuming the negation of the succedent proves the corresponding implication LHS in the antecedent assumption ⑥, which gives  $V < U$  as an assumption. The remaining arithmetic argument underlying these premises proceeds by contradicting this assumption (below).

$$\text{vL, } \mathbb{R} \overline{\textcircled{b}}, R, \text{Inv}_a \vdash t \geq T \rightarrow \|x\| < \varepsilon$$

For  $p \in \mathcal{S}$ , the following sequence of inequalities is used (note that  $\sigma < \lambda_p$  is implied by the later premises):

$$\begin{aligned} V_p &< W e^{-\sigma(t-\tau)} e^{-\lambda_p \tau} \text{ (from invariant)} \\ &= W e^{-\sigma t} e^{-\tau(\lambda_p - \sigma)} \\ &\leq W e^{-\sigma T} e^{-\tau(\lambda_p - \sigma)} \text{ (from } t \geq T, \sigma > 0) \\ &\leq U e^{-\tau(\lambda_p - \sigma)} \text{ (from } R) \\ &\leq U \text{ (from } \sigma < \lambda_p, \tau \geq 0, \text{ contradiction)} \end{aligned}$$
$$\begin{aligned} V_p &< W e^{-\sigma(t-\tau)} e^{-\lambda_p(\tau-\Theta_p)} \text{ (from invariant)} \\ &\leq W e^{-\sigma(t-\tau)} \text{ (from } \tau \leq \Theta_p, \lambda_p \leq 0) \\ &= W e^{-\sigma t} e^{\sigma \tau} \\ &\leq W e^{-\sigma t} e^{\sigma \Theta_p} \text{ (from } \sigma > 0, \tau \leq \Theta_p) \\ &\leq W e^{-\sigma T} e^{\sigma \Theta_p} \text{ (from } t \geq T, \sigma > 0) \\ &\leq U \text{ (from } R, \text{ contradiction)} \end{aligned}$$

$$\frac{*}{\vdash \mathcal{L}_{f_p}(V_p) \leq -\lambda_p V_p} \\ \frac{V_p < W e^{-\lambda_p(\tau - \Theta_p)} \vdash [x' = f_p(x), \tau' = 1 \wedge \tau \leq \Theta_p] V_p < W e^{-\lambda_p(\tau - \Theta_p)}}{}$$

$$\textcircled{a} \equiv \bigwedge_{p \in \mathcal{S}} \forall x (\|x\| < \delta \rightarrow V_p < W) \wedge \\ \wedge \bigwedge_{p \in \mathcal{U}} \forall x (\|x\| < \delta \rightarrow V_p < W e^{\lambda_p \Theta_p})$$
$$\frac{\frac{\text{cut}, \mathbb{R}, \exists \mathbb{L} \quad \varepsilon > 0, W > 0, \textcircled{a}, U > 0, \textcircled{b} \vdash \exists T \geq 0 \forall x (\|x\| < \delta \rightarrow \dots)}{\text{cut}, \mathbb{R}, \exists \mathbb{L} \quad \varepsilon > 0, W > 0, \textcircled{a} \vdash \exists T \geq 0 \forall x (\|x\| < \delta \rightarrow \dots)}}{\text{cut}, \mathbb{R}, \exists \mathbb{L} \quad \varepsilon > 0 \vdash \exists T \geq 0 \forall x (\|x\| < \delta \rightarrow \dots)}}{\text{VR}, \rightarrow \mathbb{R} \quad \vdash \text{UGpAttr}(\alpha_{t_{\text{ime}}})}$$

The derivation from premise ② unfolds the switching controller  $\alpha_u$  in  $\alpha_{\text{time}}$  with dL's hybrid program axioms. Similar to the derivation for the stability conjunct, this unfolding yields four possible shapes of premises (abbreviated as ... and shown immediately below) for maintaining the invariant  $Inv_a$  after a switch from the current mode  $p$  to the next mode  $q$ .

$$\begin{array}{c}
 \dots \\
 \frac{[u], [i], [?], [:=]}{Inv_a, u = p \vdash [\bigcup_{q \in \mathcal{P}} (? \theta_{p,q} \leq \tau; \tau := 0; u := q)] Inv_a} \\
 \frac{[i], [?]}{Inv_a \vdash [? u = p; \bigcup_{q \in \mathcal{P}} (? \theta_{p,q} \leq \tau; \tau := 0; u := q)] Inv_a} \\
 \frac{[u]}{Inv_a \vdash [\alpha_u] Inv_a} \\
 \\
 t \geq \tau, \theta_{p,q} \leq \tau, V_p < W e^{-\sigma(t-\tau)} e^{-\lambda_p \tau} V_q < W e^{-\sigma t} \quad (p \in \mathcal{S}, q \in \mathcal{S}) \\
 t \geq \tau, \theta_{p,q} \leq \tau, V_p < W e^{-\sigma(t-\tau)} e^{-\lambda_p \tau} V_q < W e^{-\sigma t} e^{\lambda_q \Theta_q} \quad (p \in \mathcal{S}, q \in \mathcal{U}) \\
 t \geq \tau, \theta_{p,q} \leq \tau, V_p < W e^{-\sigma(t-\tau)} e^{-\lambda_p(\tau-\Theta_p)}, \tau \leq \Theta_p \vdash V_q < W e^{-\sigma t} \quad (p \in \mathcal{U}, q \in \mathcal{S}) \\
 t \geq \tau, \theta_{p,q} \leq \tau, V_p < W e^{-\sigma(t-\tau)} e^{-\lambda_p(\tau-\Theta_p)}, \tau \leq \Theta_p \vdash V_q < W e^{-\sigma t} e^{\lambda_q \Theta_q} \quad (p \in \mathcal{U}, q \in \mathcal{U})
 \end{array}$$

The derivation from premise ③ unfolds the plant model  $\alpha_p$ . This results in two possible shapes of premises, depending if  $p \in \mathcal{S}$  or  $p \in \mathcal{U}$ , which are abbreviated ⑤ and ⑥ respectively. In either case, the key step shows that the appropriate upper bound on  $V_p$  is preserved.

$$\begin{array}{c}
 \text{⑤} \quad \text{⑥} \\
 \frac{[i], [?]}{Inv_a, u = p \vdash [x' = f_p(x), \tau' = 1, t' = 1 \ \& \ \tau \leq \Theta_p] Inv_a} \\
 \frac{[i], [?]}{Inv_a \vdash [? u = p; x' = f_p(x), \tau' = 1, t' = 1 \ \& \ \tau \leq \Theta_p] Inv_a} \\
 \frac{[u]}{Inv_a \vdash [\alpha_p] Inv_a}
 \end{array}$$

For premise ⑤, the proof uses  $\text{dbx}_{\neq}$  with cofactor  $-\lambda_p$ , with abbreviation  $P_s = W e^{-\sigma(t-\tau)} e^{-\lambda_p \tau}$ , noting that the Lie derivative of  $P_s$  is  $-\lambda_p P_s$ . This yields the third premise of rule  $\text{MLF}_{\tau}$ .

$$\begin{array}{c}
 * \\
 \frac{}{\vdash \mathcal{L}_{f_p}(V_p) \leq -\lambda_p V_p} \\
 \text{dbx}_{\neq} \frac{}{V_p < P_s \vdash [x' = f_p(x), \tau' = 1, t' = 1 \ \& \ \tau \leq \Theta_p] V_p < P_s}
 \end{array}$$

The proof for premise ⑥ is similar using  $\text{dbx}_{\neq}$  with cofactor  $-\lambda_p$ , with abbreviation  $P_u = W e^{-\sigma(t-\tau)} e^{-\lambda_p(\tau-\Theta_p)}$ , noting that the Lie derivative of  $P_u$  is  $-\lambda_p P_u$ . This yields the third premise of rule  $\text{MLF}_{\tau}$ .

$$\begin{array}{c}
 * \\
 \frac{}{\vdash \mathcal{L}_{f_p}(V_p) \leq -\lambda_p V_p} \\
 \text{dbx}_{\neq} \frac{}{V_p < P_u \vdash [x' = f_p(x), \tau' = 1, t' = 1 \ \& \ \tau \leq \Theta_p] V_p < P_u} \quad \square
 \end{array}$$

## B COUNTEREXAMPLE

The cruise controller automaton from Section 5.2 is taken from the suite of examples for the Stabhyli tool [26, 27]. Using the default instructions on a Linux machine, Stabhyli generates a success message with the following output (newlines added for readability):

```

...
SOSSolution( Problem is solved. (accepted); ...
...
### Lyapunov template for mode normal_PI: \

```

```

+V_23*relV^2+V_22*intV^2+V_21*intV*relV \
+V_20*relV+V_19*intV
### Lyapunov function for mode normal_PI: \
+572572089848357/144115188075855872*intV*relV \
+256336575597239/281474976710656*relV^2 \
+6008302119812893/4611686018427387904*intV^2 \
+5787253314511645/618970019642690137449562112*relV \
+566167770976729/39614081257132168796771975168*intV
...

```

The hybrid system is stable

The generated Lyapunov function candidate  $V$  does not exactly satisfy all of the required arithmetical conditions for the normal PI mode [26]. For example, one requirement is that it should be non-negative in the mode invariant  $-15 \leq \text{relV} \leq 15 \wedge -500 \leq \text{intV} \leq 500$ . It can be checked that  $\text{intV} = -\frac{1}{17179869184}$ ,  $\text{relV} = 0$  is a counterexample, with  $V = -3.90488 \times 10^{-24}$ .

A heuristic approach to resolve this numerical issue is to truncate terms in the candidate  $V$  with extremely small coefficients and then check the resulting truncated candidate. This heuristic is applied for the case study in Section 5.2, where the KeYmaera X proof succeeded using the truncated candidate together with the rest of the Lyapunov function candidates generated by Stabhyli (for other automaton modes).