Verification of Annotated Models from Executions

Parasara Sridhar Duggirala
Department of Computer Science
University of Illinois at Urbana Champaign
duggira3@illinois.edu

Sayan Mitra
Coordinated Science Laboratory
University of Illinois at Urbana Champaign
mitras@illinois.edu

Mahesh Viswanathan
Department of Computer Science
University of Illinois at Urbana Champaign
vmahesh@illinois.edu

ABSTRACT

Simulations can help enhance confidence in system designs but they provide almost no formal guarantees. In this paper, we present a simulation-based verification framework for embedded systems described by non-linear, switched systems. In our framework, users are required to annotate the dynamics in each control mode of switched system by something we call a discrepancy function that formally measures the nature of trajectory convergence/divergence of the system. Discrepancy functions generalize other measures of trajectory convergence and divergence like Contraction Metrics and Incremental Lyapunov functions. Exploiting such annotations, we present a sound and relatively complete verification procedure for robustly safe/unsafe systems. We have built a tool based on the framework that is integrated into the popular Simulink/Stateflow modeling environment. Experiments with our prototype tool shows that the approach (a) outperforms other verification tools on standard linear and non-linear benchmarks, (b) scales reasonably to larger dimensional systems and to longer time horizons, and (c) applies to models with diverging trajectories and unknown parameters.

1. INTRODUCTION

Simulations play an important role in helping designers gain confidence in the correctness of their systems, especially in the context of embedded systems, where verification of designs remains computationally challenging. However, while simulations have proved to be valuable and scalable, they provide almost no formal guarantees about the correctness of designs. Recently, there have been some proposals [11, 16, 8, 6, 21, 13] to obtain formal correctness guarantees from multiple simulation runs of system. In the context of embedded systems, most of them consider continuous dynamical models described by linear differential equations; see Section 2 for a detailed discussion of these papers. In this paper, we consider embedded systems described by a richer class of *switched, non-linear* dynamical system models. These are models with multiple control modes where different (possibly nonlinear) physical laws govern the evolution of system state, and a switching/control sequence determines which control mode is visited at different times. Embedded systems with time triggered behavioral changes can be naturally modeled in this framework. We present a framework that formally verifies the safety of such systems based on simulating system designs or executing system implementations.

Our approach, relies on the inherent continuity in the behaviors of such a system — if two executions start close by, then the distance between them at time t ($< T$) can be bounded. However, obtaining such a relationship is computationally intractable for general systems. We, therefore, require users to provide *annotations* on the dynamics that allows us to compute such a relationship. Our use of annotations is inspired by the central role that concepts like loop invariants have played in the verification of software.

We introduce a class of annotations that we call *discrepancy functions*. We show that discrepancy function is a generalization of other well known measures of trajectory convergence and divergence such as *Contraction metric* [18] and *Incremental stability* [2] in the control theory literature. Symbolic models for control systems were computed using a similar property called *Incremental forward completeness* in [25]. Thus, the annotations we require, might be naturally produced by a control theorist during the design process. Moreover, there are proposals to construct such measures automatically in the control theory literature, using sum-of-squares and convex optimization tools [3]. In this paper, we also outline some automated techniques to generate discrepancy function annotations for systems; our method is not guaranteed to succeed, but we used them to analyze some of the examples we consider in our experiments.

We then present an algorithm to verify bounded time safety of nonlinear switched system from simulations using such annotations. Simulation traces or executions of embedded systems observe and record the system state only at discrete points in time. Thus, the gaps in the sampled trace have to be filled in order to reason about the actual trace. Second, the recorded states in the execution/simulation might not be the actual states of the system due to errors introduced from sensor quantizations and from numerical integrators used to generate the simulation trace. Our algorithm accounts for these sources of error, and exploits the annotations to overcome these challenges. We show that our verification algo-

rithm is sound and relatively complete. That is, the answers of safety/unsafety of the system given by our algorithm are correct, and if the system is either robustly safe or unsafe, our algorithm is guaranteed to terminate; we say a system is robustly safe, if all states in some envelope around the system behaviors are safe. In the situation where the system is safe but not robustly safe, our algorithm might not terminate.

We have built a prototype tool called **C**heck **E**xecute **C**ompare **E**ngine (C2E2) that implements our approach. Our tool uses the Simulink Stateflow modeling framework, which is widely popular among designers of embedded systems. The annotations for the examples we considered were either obtained from the literature, or using our automated approach. Our experimental analysis shows that the approach successfully analyzes commonly arising non-linear systems, and on standard benchmarks outperforms recent tools for non-linear systems like $Flow^*$ [5] and *Ariadne* [4]. Our experiments also demonstrate that the method scales to reasonably large dimensional systems and to longer time horizons. One advantage of such a simulation based approach is that it also allows us to verify executable systems where the system models have unknown parameters. A traditional model checker would fail to analyze such systems because of the incompleteness of the system model.

2. RELATED WORK

Safety verification of dynamical and hybrid systems using simulations has been studied in a handful of papers. In [11], the authors construct a Metric Transition System using the simulations and then verify the transition system. The approach is sound and is relatively complete only for linear models. An incremental Lyapunov function-based approach is used in [12] for constructing approximate bisimulations. In contrast, our approach does not construct intermediate transition relations but directly checks bounded safety.

In [15], the authors give a bisimulation function for stable systems, which is related to incremental Lyapunov functions (see Section 4). Our discrepancy functions can be seen as an extension of bisimulation functions for systems with possibly divergent trajectories. Sensitivity analysis is the central theme in the paper [8] and the authors provide an algorithm for systematic analysis using simulations and sensitivity of dynamical system. Similar to earlier approaches, this technique is sound for linear systems but does not provide any formal guarantees for nonlinear systems. Contraction metrics introduced in [18] can informally, be considered as a Lyapunov function for sensitivity. Discrepancy functions introduced in the current paper extend the notion of Contraction metric for performing sound and relatively complete analysis of nonlinear systems. In a similar spirit to this paper, analysis using control theoretic annotations to Simulink models and code has been also been explored recently in [14].

Other approaches which uses simulations for verifying properties of embedded systems are given in [16, 6, 21, 13]. Symbolic representation of sets of initial states that behave similarly is constructed using simulations from Simulink Stateflow models in [16]. Approaches [6, 21] use statistical techniques and heuristics to give probabilistic guarantees about the system. Distributed hybrid systems with inaccurately synchronized clocks were analyzed using simulations in [9]. The approach computes overapproximations of reachable set of states and guarantees soundness and relative completeness, however does not take advantage of annotations. δ-complete decision procedure for real arithmetic was used for verifying safety of nonlinear hybrid systems in [10]. In [10], given $\delta > 0$ and a formula, the decision procedure returns either *unsat* if the formula is unsatisfiable or *δ-sat* if a δ perturbation of the formula is satisfiable. Thus, if the decision procedure returns δ-sat, one cannot infer the system to be either safe or unsafe. In contrast, if the technique in the current paper returns *safe* then the system is indeed safe and if it returns *unsafe* then the system is indeed unsafe.

3. PRELIMINARIES

For a vector $x \in \mathbb{R}^n$, $||x||$ denotes the ℓ^2 norm For $x_1, x_2 \in \mathbb{R}^n$, $||x_1 - x_2||$ is the Euclidean distance between the points. $B_\delta(x_1) \subseteq \mathbb{R}^n$ denotes the closed ball of radius δ centered at x_1. For a set $S \subseteq \mathbb{R}^n$, $B_\delta(S) = \cup_{x \in S} B_\delta(x)$. A set S_1 is a *δ-overapproximation* of S_2, if $S_2 \subseteq S_1 \subseteq B_\delta(S_2)$. For a bounded set S, a *δ-cover* of S is a finite collection of points $\mathcal{X} = \{x_i\}_{i=1}^m$ such that $S \subseteq \bigcup_{i=1}^m B_\delta(x_i)$. Its diameter $diameter(S) \triangleq \sup_{x_1, x_2 \in S} ||x_1 - x_2||$.

For an $n \times n$ matrix $A \in \mathbb{R}^{n \times n}$, the *norm* is defined as $||A|| = \max_{x:||x||=1} ||x^T A x||$. A is *positive semi-definite*, written as $A \succeq 0$, if $\forall x \in \mathbb{R}^n$, $x^T A x \geq 0$. It is *positive definite*, $A \succ 0$, if the previous inequality is strict. It is *negative (semi) definite* if $-A$ is positive (semi) definite.

A continuous function $f : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}$ is *smooth* if all its higher derivatives and partial derivatives exist and are also continuous. It has a Lipschitz constant $K \geq 0$ if for every $x_1, x_2 \in \mathbb{R}^n$, $||f(x_1) - f(x_2)|| \leq K||x_1 - x_2||$. A non-negative function $g : \mathbb{R}^n \to \mathbb{R}$ is a *class $\mathcal{K}$ function* if $g(x) \geq 0$ for $x \neq 0, g(0) = 0$ and $g(x) \to 0$ as $x \to 0$. A class $\mathcal{K}$ function g is called $\mathcal{K}_\infty$ if $g(x) \to \infty$ as $x \to \infty$. For example, the function $f(y_1, y_2) = y_1^2$ belongs to class $\mathcal{K}$ but not to $\mathcal{K}_\infty$. A function $g : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}$ is called a $\mathcal{KL}$ function, if and only if (1) for each $t \in \mathbb{R}$, $g_t(x) \triangleq g(x,t)$ is a $\mathcal{K}$ function and (2) for each $x \in \mathbb{R}^n$, $g_x(t) \triangleq g(x,t) \to 0$ as $t \to \infty$ (see Appendix of [17] for these standard definitions).

A *matrix function* $\mathbf{M} : \mathbb{R}^n \times \mathbb{R}_{\geq 0} \to \mathbb{R}^{m \times m}$ maps a state $x \in \mathbb{R}^n$ and a time t to a matrix $\mathbf{M}(x,t)$. $\mathbf{M}$ is called an *uniform metric* if $\forall x \in \mathbb{R}^n, \forall t > 0$, $\mathbf{M}(x,t)$ is symmetric, positive definite and $\forall y \in \mathbb{R}^m, \exists\, v_2, v_1 \in \mathbb{R}$ such that $0 < v_2 < v_1$, $v_2 \cdot y^T y \leq y^T \mathbf{M}(x,t) y \leq v_1 \cdot y^T y$. For Contraction Metric later introduced in the paper, we consider uniform metrics which satisfy the above properties over a subset of $\mathbb{R}^n \times \mathbb{R}$.

3.1 Dynamical and Switched System Models

An n-dimensional *nonlinear dynamical system* is specified by a differential equation:

$$\dot{x} = f(x,t), \tag{1}$$

where the variable x takes values in $\mathbb{R}^n$, t is a non-negative real variable which models time, and $f : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^n$ is a continuous function. In this context points in $\mathbb{R}^n$ are called *states*. A solution for Equation (1) is a function $\xi : \mathbb{R}^n \times \mathbb{R}_{\geq 0} \to \mathbb{R}^n$, such that for a given initial state $x_0 \in \mathbb{R}^n$, the state of the system at time t is $\xi(x_0, t)$. A solution is also called a *trajectory*. For the vector-valued function $f(x,t) =$

$[f_1(x,t)\cdots f_n(x,t)]^T$, the Jacobian matrix is denoted by $\frac{\partial f}{\partial x}$ and it generalizes differentiation of scalar functions.

A *switched system* is specified by a set of differential equations and a set of *switching signals*. Each switching signal defines the time intervals over which particular differential equation governs the evolution of the system. Let $\mathcal{F} = \{f_i\}_{i\in\mathcal{I}}$ be a collection of continuous functions indexed by a finite set $\mathcal{I}$, which specify the right hand side of the differential equations. A *switching point* p consists of (a) an element of $\mathcal{I}$, denoted by $p.\mathsf{mode}$, and (b) a nonnegative real number denoted by $p.\mathsf{time}$ which defines the time up to which the system evolves with dynamics $\dot{x} = f_{p.\mathsf{mode}}(x,t)$. A sequence of switching points $\sigma = p_0, p_1, \ldots, p_k$ with $p_0.\mathsf{time} = 0$ and strictly increasing switching times[1] naturally defines a switching signal $\sigma : [0, p_k.\mathsf{time}) \to \mathcal{I}$ as $\sigma(t) = p_i.\mathsf{mode}$ if and only if t is in the half-open interval $[p_{i-1}.\mathsf{time}, p_i.\mathsf{time})$. The execution of a switching system given a switching signal $\sigma = p_1, \ldots, p_k$ is defined as $\xi_\sigma : \mathbb{R}^n \times \mathbb{R}_{\geq 0} \to \mathbb{R}^n$ where $\xi_\sigma(x_0, 0) = x_0$ and $\forall t \in (p_{j-1}.\mathsf{time}, p_j.\mathsf{time})$, the execution satisfies the constraint $\dot{\xi_\sigma}(x_0,t) = f_{p_j.\mathsf{mode}}(\xi_\sigma(x_0,t), t - p_{j-1}.\mathsf{time})$ and $\xi_\sigma(x_0, p_j.\mathsf{time}) = lim_{t\to p_j.\mathsf{time}^-}\xi_\sigma(x_0,t)$. The *reachable set* for a state x_0 for a switching signal σ at a given time t_0 is given by $\{\xi_\sigma(x_0,t_0)\}$. This notion extends naturally for a set of states and interval durations.

We specify a set of switching signals by what we call a *switching interval sequence* which is a finite sequence of the form $\rho = q_1, \ldots, q_k$ where each q_i is of the form $(q_i.\mathsf{mode}, q_i.\mathsf{range})$ with $q_i.\mathsf{mode} \in \mathcal{I}$ and $q_i.\mathsf{range}$ is a closed interval over $\mathbb{R}_{\geq 0}$. The i^{th} element in the sequence is also denoted as $\rho[i]$. The upper and lower bounds of the interval $q_i.\mathsf{range}$ are denoted as $q_i.\mathsf{ub}$ and $q_i.\mathsf{lb}$ respectively. A switching interval sequence defines a set of switching signals $sig(\rho) = \{\sigma |\ \sigma = p_0, \ldots, p_k,$ $p_0.\mathsf{time} = 0, \forall i \in 1:k, p_i.\mathsf{time} - p_{i-1}.\mathsf{time} \in q_i.\mathsf{range}\}$. The set of executions corresponding to ρ is defined as, $\xi_\rho(x_0,t) = \{\xi_\sigma(x_0,t) \mid \sigma \in sig(\rho)\}$. As an extension of switching signal, the *reachable set* for x_0 for ρ at time t_0 is $\bigcup_{\sigma\in sig(\rho)}\{\xi_\sigma(x_0,t_0)\}$. Similar to switching signals, this notion extends naturally for a set of states and interval durations.

DEFINITION 1. *The system $\mathcal{F}$, with a switching interval sequence ρ is ϵ-*robustly safe upto *T_{bound}, for a given initial state x_0, an unsafe set $U \subseteq \mathbb{R}^n$, an $\epsilon \geq 0$ and a time bound T_{bound} if for every $t \in [0, T_{bound}]$, $B_\epsilon(\xi_\rho(x_0,t)) \cap U = \emptyset$. It is* robustly safe *if it is ϵ-robustly safe for some $\epsilon > 0$. The definition is extended in the natural way to a set of initial states Θ.*

4. TRAJECTORY DISCREPANCY FUNCTION

The bounded safety verification algorithm proposed in Section 6 exploits annotations that have to be provided with the system model. We propose a type of annotation which generalizes several different types of proof certificates that are used in the control theory literature for analyzing trajectories of dynamical systems. We call this general class of annotations discrepancy functions. Informally, a trajectory discrepancy function gives an upper bound on the distance between two trajectories as a function of the distance between their initial states and the time elapsed. In the following subsections, we present three different ways to obtain discrepancy functions with the help of a running example.

[1]In this paper we require strictly increasing switching times, but in the general theory of switched systems the switching times may be nondecreasing [17].

DEFINITION 2. *A smooth function $V : \mathbb{R}^{2n} \to \mathbb{R}_{\geq 0}$ is called a* discrepancy function *for the system (1) if and only if there are functions $\alpha_1, \alpha_2 \in \mathcal{K}_\infty$ and a uniformly continuous function $\beta : \mathbb{R}^{2n} \times \mathbb{R} \to \mathbb{R}_{\geq 0}$ with $\beta(x_1,x_2,t) \to 0$ as $||x_1 - x_2|| \to 0$ such that for any pair of states $x_1, x_2 \in \mathbb{R}^n$:*

$$x_1 \neq x_2 \iff V(x_1,x_2) > 0, \tag{2}$$

$$\alpha_1(||x_1 - x_2||) \leq V(x_1,x_2) \leq \alpha_2(||x_1 - x_2||) \textit{and} \tag{3}$$

$$\forall\, t > 0.\ V(\xi(x_1,t),\xi(x_2,t)) \leq \beta(x_1,x_2,t), \tag{4}$$

A tuple $(\alpha_1, \alpha_2, \beta)$ satisfying the above conditions is called a witness *to the discrepancy function.*

The complete annotation for the system (1) is a discrepancy function and its witness. The first condition requires that the function $V(x_1,x_2)$ vanishes to zero if and only if the first two arguments are identical. The second condition states that the value of $V(x_1,x_2)$ can be upper and lower-bounded by functions of the ℓ^2 distance between x_1 and x_2. These functions are used in algorithm in Figure 1 for computing the tubes that are used in safety verification. The final, and the more interesting, condition requires that the function V applied to solutions of (1) at a time t from a pair of initial states is upper bounded and converges to 0 as the ℓ^2 norm of $x_1 - x_2$ converges to 0. *Local* discrepancy functions can be obtained by restricting Definition 2 for a subset of $\mathbb{R}^n$.

Remark : *[Comparison of Discrepancy Function and Sensitivity Analysis]* Sensitivity s_x for system (1) is given by the differential equation $\dot{s_x} = \frac{\partial f}{\partial x}s_x$ and the value of sensitivity at time t for an initial state x_0, denoted as $s_{x_0}(t)$ is obtained by solving this differential equation along the solution of (1). It has been observed in [8] that $||s_{x_1}(t)|| \cdot \epsilon$ is an estimate of $||\xi(x_1,t) - \xi(x_2,t)||$ where $||x_1 - x_2|| = \epsilon$. For nonlinear systems, this estimate is neither an overapproximation, nor an underapproximation. Compared to sensitivity analysis, our approach requires that $\beta(x_2,x_1,t)$ gives an overapproximation of $V(\xi(x_2,t),\xi(x_1,t))$.

In the remainder of this section, we observe that proof certificates routinely used in stability analysis of dynamical systems are in fact discrepancy functions [2].

4.1 Lipschitz dynamics

Consider system (1) with L as Lipschitz constant for $f(x,t)$. We observe that for such system, the function $||x_1 - x_2||$ is a discrepancy function. Lipschitz constants can be computed algorithmically for linear, polynomial, and certain classes of trigonometric functions. For more general classes, empirical techniques can estimate it over closed subsets [24].

PROPOSITION 1. *For system (1) with Lipschitz constant $L \in \mathbb{R}_{\geq 0}$ for the function $f(x,t)$, $V(x_1,x_2) \triangleq ||x_1 - x_2||$ is a discrepancy function with witness $(\alpha_1,\alpha_2,\beta)$ where $\alpha_1(||x_1 - x_2||) = \alpha_2(||x_1 - x_2||) = ||x_1 - x_2||$ and $\beta(x_1,x_2,t) = e^{Lt}||x_1 - x_2||$.*

[2]Proofs of these proposition can be found in the full version at https://publish.illinois.edu/c2e2-tool/

Example 1 A second order differential equation modeling the dynamics of current in an RLC circuit is given by: $\frac{d^2i}{dt^2} + \frac{R}{L}\frac{di}{dt} + \frac{i}{LC} = 0$. For particular choice of the R, L, and C parameters the system can be written as:

$$\begin{pmatrix}\dot{u}\\ \dot{v}\end{pmatrix} = \begin{pmatrix}0 & 1\\ -\frac{1}{LC} & -\frac{R}{L}\end{pmatrix}\begin{pmatrix}u\\ v\end{pmatrix} = \begin{pmatrix}0 & 1\\ -2 & -2\end{pmatrix}\begin{pmatrix}u\\ v\end{pmatrix}. \quad (5)$$

The system with state space $\bar{u} = (u, v)$ is a damped oscillatory system that eventually stabilizes to the origin. Considering an operating region in the state space of the system, say $R = [-10, 10] \times [-10, 10]$, the Lipschitz constant over this interval can be computed by maximizing $\frac{||A_1[u_1,v_1]^T - A_1[u_2,v_2]^T||}{||[u_1-u_2\ v_1-v_2]^T||}$ by over (u_1, v_1) and (u_2, v_2) in R, where A_1 is the matrix in Equation (5). Thus, in this case the Lipschitz constant is equal to the matrix norm $||A_1||$. For this example, we found the Lipschitz constant to be $L = 2.9208$ using MATLAB. It follows that, the discrepancy function is given as $V(u_1, v_1, u_2, v_2) = |||[u_1 - u_2\ v_1 - v_2]^T||$ and $\beta(u_1, v_1, u_2, v_2, t) = e^{2.9208t}|||[u_1 - u_2\ v_1 - v_2]^T||$. □

4.2 Contraction metrics

DEFINITION 3 (DEFINITION 2 FROM [18]). *A uniform metric* $\mathbf{M} : \mathbb{R}^n \times \mathbb{R}_{\geq 0} \to \mathbb{R}^{n\times n}$ *is called a* Contraction metric *for system (1) if* $\exists \beta_M \in \mathbb{R}_{\geq 0}$ *such that*

$$\frac{\partial f}{\partial x}^T \mathbf{M}(x,t) + \mathbf{M}(x,t)\frac{\partial f}{\partial x} + \dot{\mathbf{M}}(x,t) + \beta_M \mathbf{M}(x,t) \preceq 0. \quad (6)$$

THEOREM 2 (THEOREM 2 FROM [18]). *For system (1) with a contraction metric* $\mathbf{M}$*, the trajectories converge exponentially with time, i.e.* $\exists\, k \geq 1, \gamma > 0$ *such that,* $\forall x_1, x_2 \in \mathbb{R}^n$, $\delta x^T \cdot \delta x \leq k\delta x_0^T \cdot \delta x_0 e^{-\gamma t}$*, where* $\delta x_0 = x_1 - x_2$ *and* $\delta x = \xi(x_1, t) - \xi(x_2, t)$.

PROPOSITION 3. *For system (1) with a contraction metric* $\mathbf{M}$*,* $V(x_1, x_2) \triangleq (x_1 - x_2)^T(x_1 - x_2)$ *is a discrepancy function with witness* $(\alpha_1, \alpha_2, \beta)$ *where* $\alpha_1 = \alpha_2 = (||x_1 - x_2||)^2$ *and* $\beta(x_1, x_2, t) = k(||x_1 - x_2||)^2 e^{-\gamma t}$ *where* k, γ *are from Theorem 2.*

Example 2 Continuing with the system in Example 1, we compute the Jacobian $\frac{\partial f}{\partial \bar{u}} = \begin{pmatrix}0 & 1\\ -2 & -2\end{pmatrix}$ and observe that the matrix function $\mathbf{M}(\bar{u}, t) \triangleq \begin{pmatrix}2.5 & 0.5\\ 0.5 & 0.75\end{pmatrix}$ is a uniform metric. Evaluating the left hand side of equation (6) with $\beta_M = 0.5$, we obtain $\frac{\partial f}{\partial \bar{x}}^T \mathbf{M}(\bar{u}, t) + \mathbf{M}(\bar{u}, t)\frac{\partial f}{\partial \bar{u}} + \dot{\mathbf{M}}(\bar{u}, t) + \beta_M \mathbf{M}(\bar{u}, t) = \begin{pmatrix}-0.75 & 0.25\\ 0.25 & -1.625\end{pmatrix} \prec 0$. Hence, $\mathbf{M}(\bar{u}, t)$ is a Contraction metric for Example 1. From Theorem 2, we have that $\exists k \geq 1, \gamma > 0$, such that $\delta\bar{u}^T \cdot \delta\bar{u} \leq k\delta\bar{u}_0^T \cdot \delta\bar{u}_0 e^{-\gamma t}$. From Proposition 3, the function $V(u_1, v_1, u_2, v_2) = [u_1 - u_2\ v_1 - v_2]^T[u_1 - u_2\ v_1 - v_2]$ is a discrepancy function with witness $\alpha_1 = \alpha_2 = ((u_1 - u_2)^2 + (v_1 - v_2)^2)$ and $\beta(u_1, v_1, u_2, v_2, t) = k((u_1 - u_2)^2 + (v_1 - v_2)^2)e^{-\gamma t}$. □

4.3 Incremental Stability

Incremental stability is a notion used in control theory [2] which formalizes the property that the Euclidean distance between two trajectories is bounded by a $\mathcal{KL}$ function of the distance between their initial states and time. This is stronger than what is required in a discrepancy function which may not converge to zero as time goes to infinity. Relaxing the requirement of convergence of trajectories, and enforcing that the distance between trajectories is a bounded function of distance between initial states and time would lead to the notion of Incremental forward completeness defined in [25].

DEFINITION 4. *The system (1) is* Incrementally stable *if there is a* $\mathcal{KL}$ *function* β *such that for any two initial states* x_1 *and* x_2 *in* $\mathbb{R}^n$, $||\xi(x_1, t) - \xi(x_2, t)|| \leq \beta(||x_1 - x_2||, t)$.

THEOREM 4 (THEOREM 1 FROM [2]). *If system (1) is incrementally stable then there exists a smooth function* $V : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ *and* $\exists \alpha_1, \alpha_2 \in \mathcal{K}_\infty$ *and* $\alpha \in \mathcal{K}$*, such that for every pair of states* $x_1, x_2 \in \mathbb{R}^n$

$$\alpha_1(||x_1 - x_2||) \leq V(x_1, x_2) \leq \alpha_2(||x_1 - x_2||), \text{and} \quad (7)$$

$$V(\xi(x_1, t), \xi(x_2, t)) - V(x_1, x_2) \leq \int_0^t -\alpha(|||\xi(x_1, \tau) - \xi(x_2, \tau)|||)d\tau. \quad (8)$$

The function V *is called an* Incremental Lyapunov function.

PROPOSITION 5. *For system (1) with Incremental Lyapunov function* V*, then the function* V *is a discrepancy function with witness* $(\alpha_1, \alpha_2, \beta)$ *where* α_1 *and* α_2 *are from Equation 7 and* $\beta(x_1, x_2, t) = V(x_1, x_2) + \int_0^t -\alpha(||\xi(x_1, \tau) - \xi(x_2, \tau)||)d\tau$ *where* α *is from Equation 8.*

DEFINITION 5 (FROM [25]). *System (1) is* Incrementally forward complete *if it is Lipschitz continuous, and there exists continuous function* $\beta : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ *such that for every* $s \in \mathbb{R}_{\geq 0}, \beta(\cdot, s)$ *is a* $\mathcal{K}_\infty$ *function and for any two initial states* x_1 *and* x_2 *in* $\mathbb{R}^n$, $||\xi(x_1, t) - \xi(x_2, t)|| \leq \beta(||x_1 - x_2||, t)$*. We refer* β *as a witness for incremental forward completeness.*

PROPOSITION 6. *If system (1) is Incrementally forward complete with witness function* β_1*, then the function* $V(x_1, x_2) = ||x_1 - x_2||$ *is a discrepancy function with witness* $(\alpha_1, \alpha_2, \beta)$ *as* $\alpha_1 = \alpha_2 = ||x_1 - x_2||$ *and* $\beta(x_1, x_2, t) = \beta_1(||x_1 - x_2||, t)$.

Example 3 Continuing with the system in Example 1, here we start with a candidate quadratic Incremental Lyapunov function $V(u_1, v_1, u_2, v_2) \triangleq [u_1 - u_2\ v_1 - v_2]^T P[u_1 - u_2\ v_1 - v_2]$, with $\alpha_1 \triangleq 0.375(u_1 - u_2)^2 + 0.375(v_1 - v_2)^2 + 0.5(u_1 - u_2)(v_1 - v_2)$, $\alpha_2 \triangleq 1.25(u_1 - u_2)^2 + 1.25(v_1 - v_2)^2 + 0.5(u_1 - u_2)(v_1 - v_2)$ and $\alpha \triangleq (u_1 - u_2)^2 + (v_1 - v_2)^2$, with $P = \begin{pmatrix}1.25 & 0.25\\ 0.25 & 0.375\end{pmatrix}$. First we check that V is indeed an Incremental Lyapunov function by computing $\dot{V}(u_1, v_1, u_2, v_2)$ which turns out to be $[u_1 - u_2\ v_1 - v_2]^T[A^T P + PA][u_1 - u_2\ v_1 - v_2] =$

$-\alpha(u_1, v_1, u_2, v_2)$. Since $\alpha > 0$ whenever $(u_1, v_1) \neq (u_2, v_2)$, $(u_1, v_1) \neq (0, 0)$ and $(u_2, v_2) \neq (0, 0)$. Integrating both sides, we get $V(\xi(u_1, v_1, t), \xi(u_2, v_2, t)) - V(u_1, v_1, u_2, v_2) \leq \int_0^t -\alpha(||\xi(u_1, v_1, \tau), \xi(u_2, v_2, \tau)||)\, d\tau$. Hence V is a discrepancy function with witness $(\alpha_1, \alpha_2, \beta)$ where $\beta(u_1, v_1, u_2, v_2, t) = V(u_1, v_1, u_2, v_2) + \int_0^t -\alpha(\xi(u_1, v_1, \tau), \xi(u_2, v_2, \tau))d\tau$. □

Example 4 Consider a two dimensional linear system: $\dot{u} = -u$; $\dot{v} = \frac{-v_0}{100}$, with initial state (u_0, v_0). A trajectory of the system is given by $\xi((u_0, v_0), t) = (u_0 e^{-t}, v_0 \frac{(1-t)}{100})$. The system converges to origin. In this example, the distance between two trajectories from different initial states decreases linearly and not exponentially. It can be verified that the function $V(u_1, v_1, u_2, v_2) = (u_1 - u_2)^2 + (v_1 - v_2)^2$ is an Incremental Lyapunov function. The Jacobian $\frac{\partial f}{\partial \bar{u}}$ is $\begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix}$ and hence a uniform metric $\mathbf{M}(\bar{u}, t)$ that satisfies Definition 3 does not exist. □

As seen in Example 4, Incremental Lyapunov function exists for systems which Contraction metric does not exist. However, existence of Contraction metric ensures exponential convergence of trajectories which is a much stronger guarantee than what is ensured by Incremental stability. If Contraction metric is a constant function, then one can derive equivalence between Contraction metric and Incremental stability. The common trait in these two concepts is that these are useful only for proving convergence of trajectories. This is not necessary for a discrepancy function and Incremental forward completeness. For more details regarding these concepts, an interested reader is referred to [18, 2, 25].

Our last example of this section illustrates that for unstable systems over a bounded time horizon, we can still obtain discrepancy functions, even though trajectories from neighboring states actually diverge with time.

Example 5 Consider the system $\dot{u} = 1$; $\dot{v} = \frac{v_0}{100}$, where (u_0, v_0) is the initial state of the trajectory. The closed form solution of the above system is given as $u(t) = u_0 + t, v(t) = v_0(1 + \frac{t}{100})$. For two trajectories starting from (u_1, v_1) and (u_2, v_2), the distance between the trajectories after time t is given as $\sqrt{(u_1 - u_2)^2 + (1 + \frac{t}{100})^2 (v_1 - v_2)^2}$. Observe that the function $V(u_1, v_1, u_2, v_2) = \sqrt{(u_1 - u_2)^2 + (v_1 - v_2)^2}$ with $\alpha_1 = \alpha_2 = \sqrt{(u_1 - u_2)^2 + (v_1 - v_2)^2}$ and $\beta(u_1, v_1, u_2, v_2, t) = \sqrt{(u_1 - u_2)^2 + (1 + \frac{t}{100})^2 (v_1 - v_2)^2}$ satisfies all the conditions in Definition 2 and hence is a discrepancy function . □

5. COMPUTING ANNOTATIONS

Our verification algorithm relies on annotations, namely the discrepancy functions of the dynamical system and its witness. We expect the users to derive these annotations through some means—possibly using existing control theoretic techniques. In Section 4 we showed how knowledge about a system in terms of Lipschitz constants, Contraction metrics, and Incremental Lyapunov functions can be exploited for obtaining annotations. In this section, we briefly discuss the related but orthogonal issue of obtaining discrepancy functions for both linear and nonlinear dynamical systems. The strategy discussed here restricts the search to *exponential discrepancy functions* which grow or shrink exponentially with time. Similar conditions for Incrementally forward complete systems can be found in [25].

DEFINITION 6. *For system (1) a discrepancy function of the system $V : \mathbb{R}^{2n} \to \mathbb{R}_{\geq 0}$ is said to be an* exponential discrepancy function *if $\exists \gamma \in \mathbb{R}$ such that:*

$$\frac{\partial V(x_1, x_2)}{\partial x_1} f(x_1, t) + \frac{\partial V(x_1, x_2)}{\partial x_2} f(x_2, t) \leq \gamma V(x_1, x_2). \quad (9)$$

Since $V(\xi(x_1, t), \xi(x_2, t)) \leq e^{\gamma t} V(x_1, x_2)$, it follows that V satisfies Equation (4) with $\beta(x_1, x_2, t) = e^{\gamma t} V(x_1, x_2)$. Thus an exponential discrepancy function V is indeed a special type of discrepancy function.

PROPOSITION 7. *Consider a linear system $\dot{x} = Ax$. Suppose two $n \times n$ matrices P and Q satisfy the (Lyapunov-like) equation $A^T P + PA = Q$ and P is positive definite and Q is either positive definite or negative semi-definite. Then, $V(x_1, x_2) \triangleq (x_1 - x_2)^T P (x_1 - x_2)$ is an exponential discrepancy function.*

The hypothesis of Proposition 7 is satisfied by linear systems that are Lyapunov stable, globally asymptotically stable (refer to [17] for formal definitions) and for systems whose trajectories diverge. For such systems, exponential discrepancy functions can be computed completely automatically.

The underlying principle for finding exponential discrepancy functions for nonlinear systems is similar. The key step is to identify classes of systems for which Equations (2), (3), and (9) can be encoded and effectively solved as convex optimization problems. We demonstrate the procedure for finding quadratic discrepancy functions encoded as linear matrix inequalities (LMIs) which are solved using existing software tools such as the sum-of-squares toolbox [22]. Similar procedures may be instantiated for finding polynomials discrepancy functions of higher degree.

Consider that a candidate quadratic form $V(x_1, x_2) \triangleq (x_1 - x_2)^T P (x_1 - x_2)$, where P is a $n \times n$ matrix. Plugging this in Equation (9) we get: $(f(x_1, t) - f(x_2, t))^T P (x_1 - x_2) + (x_1 - x_2)^T P (f(x_1, t) - f(x_2, t)) < \gamma V(x_1, x_2)$. We denote the left hand side of this expression by $R(x_1, x_2, t)$ and proceed as follows: (1) Express the constraints $V(x_1, x_2) > 0$ and $R(x_1, x_2, t) \leq 0$ as LMIs and check feasibility. (2) If feasible, search for appropriate $\gamma \leq 0$ such that $R(x_1, x_2, t) \leq \gamma V(x_1, x_2)$, encoded as an LMI. (3) If the check in step (1) is *infeasible* , then express the constraints $V(x_1, x_2) > 0$ and $R(x_1, x_2, t) > 0$ as LMIs and check feasibility. (4) If feasible, search for appropriate $\gamma \geq 0$ such that $R(x_1, x_2, t) \leq \gamma V(x_1, x_2)$ encoded as an LMI. (5) If step (3) returns *infeasible* then the search for a quadratic discrepancy function fails.

6. VERIFICATION FROM ANNOTATIONS AND SIMULATIONS

In this section, we present an algorithm which uses simulations and annotations for checking safety of switched systems. First, we define the notion of simulations we use, then

we present a subroutine for verification of dynamical systems (Section 6.2), and finally in Section 6.3 we present an algorithm for verifying switched models.

6.1 Simulation Traces for Dynamical Systems

Given the model of a dynamical system, an initial state x_0 and a period of integration $h > 0$ (also called the sampling period), a standard ODE solver approximates the values of $\xi(x_0, 0), \xi(x_0, h), \xi(x_0, 2h), \ldots$ by numerically integrating the right hand side of the differential equation. In our algorithms and implementations, we rely on a validated ODE solver (for example VNODE-LP [20]), which computes a sequence of regions $R_1, R_2, \ldots$ such that for each $t \in [j \cdot h, (j+1) \cdot h], \xi(x_0, t) \in R_j$. If the diameter of R_i is greater than the desired simulation error bound ϵ, then we reduce the value of h adaptively until the diameter becomes less than ϵ. Features of such simulation traces are stated in the definition below.

DEFINITION 7. *For system (1), given an initial state x_0, a time bound T, error bound $\epsilon > 0$, and time step $\tau > 0$, a (x_0, T, ϵ, τ) -simulation trace is a finite sequence $\psi = (R_0, t_0), (R_1, t_1), \ldots, (R_k, t_k)$ where $R_0 = \{x_0\}, \forall i > 0, R_i \subseteq \mathbb{R}^n, t_i \in \mathbb{R}_{\geq 0}$ and*

(1) $\forall\, i \in \{0, 1, \ldots k\}, t_{i+1} - t_i \leq \tau, t_0 = 0$, and $t_k = T$,

(2) $\forall\, i > 0, \forall t \in [t_{i-1}, t_i], \xi(x_0, t) \in R_i$, and

(3) $\forall\, i > 0, diameter(R_i) \leq \epsilon$.

It follows that the union of the regions in a (x_0, T, ϵ, τ)-trace contains the set of all states reached by the system from x_0 in T time. We will identify this union with the name of the simulation trace ψ.

6.2 Simulation to Verification: Dynamical Systems

In this section, we will present an algorithm for checking safety of a dynamical system using annotations. For the remainder of this subsection, we consider purely dynamical systems such as system (1), an annotation V for it, and a witness $(\alpha_1, \alpha_2, \beta)$ for the annotation. For any state $x \in \mathbb{R}^n$, we define $B^V_\delta(x) \triangleq \{y \mid V(x, y) \leq \delta\}$. For a subset $W \subseteq \mathbb{R}^n$ $B^V_\delta(W) \triangleq \cup_{x \in W} B^V_\delta(x)$. $B^{\alpha_1}_\delta(x)$ and $B^{\alpha_2}_\delta(x)$ are defined analogously. It follows from Definition 2 that for any $x \in \mathbb{R}^n$,

$$B^{\alpha_2}_\delta(x) \subseteq B^V_\delta(x) \subseteq B^{\alpha_1}_\delta(x). \tag{10}$$

The algorithm is given in Figure 1. It takes the following inputs: (a) initial partitioning parameter δ_0, (b) the dynamical system model specified by the function f, (c) Θ, which is an ω-approximation of the *bounded* set of initial states, (d) U is an *open* set of unsafe states, (e) an annotation V for f and its witness, and (f) T_b is the time bound for verification. We claim that the algorithm returns "SAFE" if all the executions starting from Θ are safe up to T_b, "UNSAFE" if $\exists x_0 \in \Theta$ such that all executions starting from $B_{(\omega+\delta)}(x_0)$ are unsafe and, it returns "ω-TOO LARGE" otherwise.

In line 4, δ-Partition(S) returns a δ-cover of S. As $S = \Theta$ is bounded, δ-Partition(S) returns a finite cover. A simulation trace ψ is obtained in line 8, which is a finite sequence

1: **Input:** δ_0, $\langle f, \Theta, U\rangle$, ω, $V(x_1, x_2)$, $(\alpha_1, \alpha_2, \beta)$, T_b
2: $S \leftarrow \Theta$; $\delta \leftarrow \delta_0$; $\mathcal{R} \leftarrow \emptyset$
3: **while** $S \neq \emptyset$ **do**
4: $\quad\mathcal{X} \leftarrow \delta$-Partition$(S)$
5: $\quad$**for** $x_0 \in \mathcal{X}$ **do**
6: $\quad\quad\epsilon \leftarrow \sup\{\beta(y, x_0, t) \mid y \in B_\delta(x_0),\ 0 \leq t \leq T_b\}$
7: $\quad\quad\epsilon' \leftarrow \sup\{\beta(y, x_0, t) | y \in B_{(\omega+\delta)}(x_0),\ 0 \leq t \leq T_b\}$
8: $\quad\quad\psi \leftarrow$ simulate$(x_0, T_b, \epsilon, \tau)$
9: $\quad\quad\mathcal{T} \leftarrow B^V_\epsilon(\psi)$
10: $\quad\quad$**if** $\mathcal{T} \cap U = \emptyset$ **then**
11: $\quad\quad\quad S \leftarrow S \setminus B_\delta(x_0)$; $\mathcal{R} \leftarrow \mathcal{R} \cup \mathcal{T}$
12: $\quad\quad$**else if** $\exists i.\ B^V_{\epsilon'}(R_i) \subseteq U$ **then**
13: $\quad\quad\quad$**return** (UNSAFE, $\mathcal{R}$, $max\{2\epsilon + \epsilon'\}$)
14: $\quad\quad$**else if** $\exists i.\ R_i \subseteq U$ **and** $B^V_{\epsilon'}(R_i) \not\subseteq U$ **then**
15: $\quad\quad\quad$**return** (ω-TOO LARGE, $\mathcal{R}$, $max\{2\epsilon + \epsilon'\}$)
16: $\quad\quad$**end if**
17: $\quad$**end for**
18: $\quad\delta \leftarrow \delta/2$; $\tau \leftarrow \tau/2$
19: **end while**
20: **return** (SAFE, $\mathcal{R}$, $max\{2\epsilon + \epsilon'\}$)

Figure 1: Algorithm 1: Safety verification of dynamical systems.

$(R_0, t_0), (R_1, t_1), \ldots, (R_k, t_k)$ described in Section 6.1. The tube $\mathcal{T}$ constructed in line 9 is guaranteed to contain all the states reachable within time T_b from states in $B_\delta(x_0)$ based on the properties of β and the accuracy of the simulation. The algorithm returns a tuple, where the first element is either SAFE or UNSAFE or ω-TOO LARGE. The second element is the collection of all the tubes computed in line 9 that are safe, denoted as $\mathcal{R}$. The third element $max\{2\epsilon + \epsilon'\}$ is the maximum value of $2\epsilon + \epsilon'$ encountered in line 6 and line 7. This value gives the upper bound on the approximation of the reachable set computed by the union of tubes in line 9. We now establish the soundness and relative completeness of the algorithm using a some intermediate propositions.

PROPOSITION 8. *If $x \in B_\delta(x_0)$ then $\forall t \in [0, T_b], \xi(x, t) \in B^V_\epsilon(\xi(x_0, t))$, where $\epsilon = sup\{\beta(x, x_0, t) | 0 \leq t \leq T_b, x \in B_\delta(x_0)\}$.*

PROPOSITION 9. *For $x \in B_\delta(x_0)$, for any $t \in [0, T_b], \xi(x, t) \in B^V_\epsilon(\psi)$, where ψ is the union of regions obtained from a $(x_0, T_b, \epsilon, \tau)$-simulation trace.*

THEOREM 10. *Algorithm 1 is sound. That is, if it returns "SAFE" then all the executions from Θ are safe, and when it returns "UNSAFE" there exists at least one execution from the initial set, that is unsafe.*

PROOF. Observe that from Proposition 9, the set of all states reachable within time T_b from some state in $B_\delta(x_0)$ is contained in the tube $\mathcal{T}$ computed in line 9. Thus, if $\mathcal{T} \cap U = \emptyset$, then all executions from the set $B_\delta(x_0)$ are safe, and so are eliminated from consideration in future iterations (line 11). Hence, if the algorithms exits the while loop because $S = \emptyset$, we can conclude that the system is safe.

On the other hand, if there is some R_i in the simulation trace ψ such that $B^V_{\epsilon'}(R_i) \subseteq U$, then it means that $\exists x_0 \in \Theta$ such

that all executions starting from $B_{(\omega+\delta)}(x_0)$ are unsafe. Since Θ is an ω-approximation of the initial states, and x_0 is an element in δ-partitioning of Θ, it follows that there exists at least one state from the set of initial states in $B_{(\omega+\delta)}(x_0)$. Hence, there exists at least one execution from the initial set that is unsafe. Thus, the decision in line 13 is correct. □

PROPOSITION 11. *The collection of safe tubes $\mathcal{R}$ returned by Algorithm 1 in line 20 is utmost $max\{2\epsilon + \epsilon'\}$-approximation of the set of reachable states from the initial set of states.*

THEOREM 12. *For $\omega = 0$, Algorithm 1 is a complete procedure for robust safety verification of dynamical systems. That is, if all the executions from Θ are robustly safe, then the it will terminate and return "SAFE". If any of the executions from Θ is unsafe, then it will terminate and return "UNSAFE".*

PROOF. Suppose that all the executions from Θ are ϵ_0 robustly safe. From the proof of Theorem 10, we can conclude two things. First, line 13 is never executed, since the system is safe. Second, when a set of initial states in eliminated from consideration (line 11), those states are safe. Now, since $V \leq \alpha_2, \alpha_2 \in \mathcal{K}_\infty$, $\exists\delta'$ such that whenever $||x - y|| < \delta', V(x, y) < \epsilon_0/4$. Also, since β is uniformly continuous in x when $t \in [0, T_b]$, we have that $\exists\delta_1$, such that $\forall y \in B_{\delta_1}(x), t \in [0, T_b]$, we have $\beta(x, y, t) < \delta'$. Thus $\exists\delta_1$ such that the value of ϵ in line 6 is $< \epsilon_0/4$.

We also have that $\alpha_1 \leq V, \alpha_1 \in \mathcal{K}_\infty$, thus $\exists\delta''$ such that $\alpha_1(\delta'') < \epsilon_0/2$. Thus $B^V_{\delta''}(x) \subset B_{\epsilon_0/2}(x)$. Let δ_2 be the value of δ in the algorithm such that the value of ϵ in line 6 is $< \delta''$. If the δ in the algorithm reaches a value $< \min\{\delta_1, \delta_2\}$, The tubes computed in line 9 are

$$\begin{aligned}\mathcal{T} &= B^V_{\delta''}(\psi) \\ &\subseteq B^{\alpha_1}_{\delta''}(\psi) \\ &\subset B_{\epsilon_0/2}(B_{\epsilon_0/4}(\xi(x_0, t))) \\ &\subset B_{3\epsilon_0/4}(\xi(x_0, t))\end{aligned}$$

Since the system is robustly safe, all the tubes would be safe and hence the algorithm will terminate and prove that system is safe.

Suppose $\langle f, \Theta, U\rangle$ is unsafe. Since U is open, there is a initial state y_0, time $t \leq T_b$, and $\epsilon_0 > 0$, such that $B_{\epsilon_0}(\xi(y_0, t)) \subseteq U$. Now, since $\xi(\cdot)$ is continuous, there are τ_0 and δ_0 such that for any $x_0 \in B_{\delta_0}(y_0)$, there is an i such that $||\xi(x_0, i\tau_0) - \xi(y_0, t)|| < \epsilon_0/4$. Further, $\beta(x_0, y_0, t) \to 0$ as $||x_0 - y_0|| \to 0$, hence $\exists\delta_1$, such that for every $x_0 \in B_{\delta_1}(y_0), \beta(x_1, x_2, t) < \epsilon_0/4$. Finally, since we can simulate with arbitrary precision, and δ and τ are decreasing, we will eventually generate a simulation trace, for which line 13 will be reached. □

We remark that in the case when the dynamical system has some execution from Θ that is safe but not robustly safe, Algorithm 1 may not terminate. Observe that the proof of soundness and relative completeness also holds for a sequence ω_i converging to 0. Further, relative completeness of the above algorithm is achieved if δ and τ can be made arbitrarily small. However, even if we have finite precision arithmetic, relative completeness is achieved if the system is robustly safe with ϵ_0 greater than the the granularity of the precision.

1: **Input:** δ_0, $\langle\mathcal{F}, \Theta, U\rangle$, ρ, $\{V_i\}$, $\{(\alpha_{1,i}, \alpha_{2,i}, \beta_i)\}$
2: $\delta \leftarrow \delta_0$; $\tau \leftarrow 0$;
3: $S \leftarrow \Theta$; $\omega \leftarrow 0$; $\mathcal{R} \leftarrow \emptyset$
4: **for all** $i = 1 : k$, where $\rho = q_1, q_2, \ldots, q_k$ **do**
5: $(result, \mathcal{R}, \omega) \leftarrow Alg1(\delta, \langle f_{\rho[i].\mathsf{mode}}, S, U\rangle, \omega, \rho[i].\mathsf{ub})$
6: **if** $result =$ SAFE **then**
7: $S \leftarrow Project(\mathcal{R}, [\rho[i].\mathsf{ub}, \rho[i].\mathsf{lb}])$
8: **else if** $result =$ UNSAFE **then**
9: **return** UNSAFE
10: **else if** $result = \omega$-TOO LARGE **then**
11: $\delta \leftarrow \delta/2$; GOTO Line 3
12: **end if**
13: **end for**
14: **return** SAFE

Figure 2: Algorithm 2: Safety verification of switching system for switching interval sequence ρ

6.3 Simulation to Verification: Switched Systems

In this section, we will present an algorithm for verifying switched systems with respect to a set of switching signals that uses Algorithm 1. The algorithm takes an input (a) Initial partitioning parameter δ_0 (b) $\mathcal{F} = \{f_i\}_{i\in\mathcal{I}}$, a collection of dynamical subsystems, (c) Θ, a *bounded* set of initial states, (d) U is an *open* set of unsafe states, (e) $\rho = q_1, q_2, \ldots, q_k$, a collection of switching signals, and (f) Annotations $V_i(\cdot)$ and witnesses $(\alpha_{1,i}, \alpha_{2,i}, \beta_i)$ for each of the subsystems in $\mathcal{I}$. The time bound for verification is the maximum duration of the switching signal $\sigma \in sig(\rho)$.

For each $\ell \in \{1, \ldots, k\}$, Algorithm 2 makes subroutine calls to Algorithm 1 (subroutine $Alg1$ in line 5) which attempts to verify that the dynamical system $\dot{x} = f_{q_\ell.\mathsf{mode}}(x, t)$ is safe for the duration $q_\ell.\mathsf{ub}$. In the process, Algorithm 1 also computes an ω-overapproximation of the reachable states during $q_\ell.\mathsf{range}$ and this is used as ω-approximate initial set for the dynamics $f_{q_{\ell+1}.\mathsf{mode}}$. If Algorithm 2 fails to prove safety or unsafety of the system, it implies that the overapproximation of the reach set for one of the dynamical systems is too coarse. Thus, the value of δ is decreased so as to get a better cover for the initial set Θ and hence a better approximation of the reachable set of states. The algorithm is given in Figure 2. The soundness of Algorithm 2 follows from soundness of Algorithm 1 and Theorem 11.

THEOREM 13. *The algorithm in Figure 2 is sound, i.e., when it returns "SAFE" the system is safe, and when it returns "UNSAFE" the system is unsafe.*

PROOF. The proof is based on Theorem 10 and Theorem 11. From Theorem 11, we know that the order of approximation computed by Algorithm 1 in the duration $\rho[i].\mathsf{range}$ is sound. Observe that algorithm 2 returns "SAFE" only when all the subroutine calls return "SAFE" and thus it follows from Theorem 10 that the system is safe in each of the dynamical systems. Notice that algorithm 2 returns "UNSAFE" only when at least one of the subroutine call returns "UNSAFE" and thus, because of Theorem 11 and Theorem 10, it follows that the system is indeed unsafe. □

THEOREM 14. *If the system $\langle \mathcal{F}, \Theta, U \rangle$ with the set of switching signals $sig(\rho)$ is robustly safe then the Algorithm 2 terminates and returns "SAFE". On the other hand, if the system is unsafe, then algorithm will terminate and return "UNSAFE"*

PROOF. If the system is safe, then it follows from Theorem 10 that line 9 is never executed. Thus, the subroutine call to verification of dynamical system would either return "SAFE", in which case, the algorithm continues, or it would return "ω-TOO LARGE" in which case, we decrease value of δ. Thus, the value of $2\epsilon + \epsilon'$ computed by Algorithm 1 converges to zero which ensures that for each mode $\omega \to 0$. Since the system is robustly safe, each of the dynamical systems is also robustly safe, and thus $\exists \omega > 0$ such that the each of the dynamical systems would return "SAFE" and hence the algorithm in Figure 2 would return "SAFE".

If the system is unsafe, then it follows from Theorem 10 that line 6 is never executed. Thus, the subroutine call would either return "UNSAFE" in which case, the system is unsafe or it would return "ω-TOO LARGE" in which case we decrease value of δ. This ensures that $\omega \to 0$. Observe that Algorithm 1 would return unsafe only when the condition in line 12 is satisfied. Now since $\delta \to 0$, it implies that $\epsilon \to 0$ and $\epsilon' \to 0$ and thus $B^V_{\epsilon'}(R_i) \subseteq U$ is satisfied for some R_i. Hence the algorithm will return "UNSAFE". □

We remark that in the case where the system is safe, but not robustly safe, then the above algorithm need not terminate. Further, if the algorithm infers that the system is unsafe, then we can generate a set of traces that correspond to the unsafe behavior. We will conclude this section by pointing out that we are making some computational assumptions about the sets Θ, U, and of the functions V that ensure that all the steps in the algorithms 1 and 2 are computable. We do not explicitly state these assumptions to ensure that our discussion in this paper highlights the key ideas without getting bogged down by technicalities. On a similar note, one can also use α_1 and α_2 in line 9, instead of V without losing the soundness and completeness guarantees; however, since these are bonded overapproximations, using them might affect the number of iterations needed to prove safety.

Example 6 Continuing on Example 1, we now compare the performance of the three discrepancy functions defined in Section 4 for the verification procedure described in Figure 1. We begin with the initial conditions as $\Theta = 3 \leq x \leq 5 \wedge y = 0$. The unsafe state if given as $1 < t < 1.2 \wedge x > 3$ and initial value of δ as 0.1. The number of executions required for proving safety is 70, 10 and 10 if we use discrepancy function as Lipschitz constant, contraction metric and incremental Lyapunov function respectively. This is expected because Lipschitz constant estimates the distance between the executions to grow exponentially which is a coarse approximation. This indicates that verification time depends on the accuracy of the annotation provided by the user. □

7. EXPERIMENTAL EVALUATION

For demonstrating the effectiveness of our technique which uses annotations and simulations for verification, we have built a tool called **C**heck **E**xecute **C**ompare **E**ngine (C2E2). Our tool uses the Simulink Stateflow modeling framework, which is popular among designers of embedded systems. The system verified by C2E2 is described as a Simulink/Stateflow model, which is (automatically) translated into a hybrid automaton according to the semantics described in [19], and VNODE-LP was used to generate simulators for each of the modes of the hybrid automaton. VNODE-LP integration engine uses finite precision interval arithmetic and Taylor models for generating simulations described in Section 6.1. The tool is developed in C++ and uses GNU Linear Programing Kit (GLPK) to check the distance of simulation traces from the unsafe set. Observe that the algorithm presented in Section 6 requires arbitrary precision arithmetic for relative completeness, however in practice, we use finite precision arithmetic which requires the robustness to be greater than the granularity of precision. In practice we terminate if the partitioning reaches 10^{-7} and terminate by saying that the system is not robust with respect to sensitive perturbations.

Our evaluation has four parts: First, we verify a benchmark suite consisting of natural linear and nonlinear dynamical system models. Second, we verify several adaptive control examples where the executable system has a reference model with unknown parameters. Third, we evaluate scalability by increasing the time horizon for verification and the number of dimensions of two parameterized models. Finally, we study the effect of the initial partitioning.

7.1 Benchmarks and comparison with other tools

We compare the performance of C2E2 against $Flow^*$ [5] and Ariadne [4] using a benchmark suite consisting of linear and nonlinear models. Ariadne uses faithful geometric representation of sets for computing reachable set and $Flow^*$ uses Taylor Models. Results of comparing the performance with Breach are discussed later in this section. In Table 7, we report the time taken by $Flow^*$ and C2E2 for computing reach set and checking safety with respect to the unsafe set, and the time taken by Ariadne for computing the reachable states. One limitation of $Flow^*$ is that we can only specify unsafe sets as rectangles and not as arbitrary polyhedral constraints. Considering that runtime for $Flow^*$ depends on remainder errors and order of Taylor model, we use adaptive orders and set the remainder error to a value such that increasing it by a factor of 2 would change the verification result from "SAFE" to "UNKNOWN". The parameters for Ariadne is set to the same values as that for $Flow^*$. Table 7 show that C2E2 outperforms the other tools in all examples, and in most cases it is faster by at least an order of magnitude.

Breach [7] is another tool against which we evaluated C2E2 . Breach is a toolbox developed in MATLAB with a GUI, making a fair comparison difficult. We ran Breach on Vanderpol coupled oscillator, Sinusoidal tracking, and tank examples, and measured the "wall clock" running time. In all cases C2E2 was faster; we don't report these numbers because of inaccuracies inherent in such numbers. Breach, like $Flow^*$, does not allow polyhedral unsafe sets. Also Breach is neither sound nor complete for nonlinear models, but inaccuracies in the verification results for the examples were not observed.

For the adaptive control system, the n-tank system and the

Benchmark	Vars.	TH	Refs.	Sims.	C2E2 (sec)	*Flow** (sec)	Ariadne (sec)
Moore-Greitzer Jet Engine [3]	2	10	12	36	1.56	10.54	56.57
Brussellator	2	10	33	115	5.262	16.77	72.75
VanDerPol	2	10	5	17	0.75	8.93	98.36
Coupled VanDerPol [3]	4	10	10	62	1.43	90.96	270.61
Sinusoidal Tracking [23]	6	10	12	84	3.68	48.63	763.32
Linear Adaptive	3	10	8	16	0.47	NA	NA
Nonlinear Adaptive	2	10	16	32	1.23	NA	NA
NonLin. Adpt. + Disturbance	3	10	22	48	1.52	NA	NA

Table 1: Experimental Results for benchmark examples. Vars: Number of Variables, TH: Time Horizon for Verification, Refs: Number of Refinements, Sims: Total number of simulation traces required for proving safety.

nonlinear navigation system the annotations were derived manually, and for all the other examples the annotations were obtained from the papers [3, 23] in which the systems appeared.

7.2 Systems models with unknown parameters

One prominent advantage of our approach is that it supports verification of executable systems where the reference model has unknown parameters. An illustrative example is the linear plant: $\dot{x} = 1; \dot{y} = \theta + u$, where θ is an unknown parameter and u is the control input. Following a standard adaptive control technique for driving y to zero, a new variable $\hat{\theta}$—an estimator for θ—is introduced giving the new dynamics for y: $\dot{x} = 1$; $\dot{y} = -\sigma y + \theta - \hat{\theta}$; $\dot{\hat{\theta}} = \gamma y$; Constants $\sigma, \gamma > 0$ are chosen by the designer. For the new system, $V((x_1, y_1, \hat{\theta}_1), (x_2, y_2, \hat{\theta}_2)) \triangleq \frac{1}{2}(x_1 - x_2)^2 + \frac{\gamma}{2}(y_1 - y_2)^2 + \frac{1}{2}(\hat{\theta}_1 - \hat{\theta}_2)^2$ is an incremental Lyapunov function $\dot{V} = -\gamma\sigma(y_1 - y_2)^2 < 0$ is used as an annotation.

Consider the nonlinear system: $\dot{x} = \theta x + u$ with control input u. Similar to the earlier example, we introduce $\hat{\theta}$ and define $u = -\hat{\theta}x - x$ such that the closed system becomes: $\dot{x} = (\theta - \hat{\theta})x - x; \dot{\hat{\theta}} = x^2$ The Lyapunov function $\frac{1}{2}x^2 + \frac{1}{2}(\theta - \hat{\theta})^2$ establishes stability of the system. For annotation, we come up with a quartic (fourth degree) discrepancy function . A modified version of this example introduces unknown disturbance inputs. Traditional model checkers that model unknown parameters as unknown constant variable require partial information (such as range of values) for handling these systems which is not required by our technique.

7.3 Scalability with time and dimensions

To check the scalability of the approach with time horizon, we verified the VanDerPol and the Nonlinear Adaptive control benchmarks for time horizons 10, 20 and 40. The verification times of the former were 0.741, 1.662 and 4.373 seconds and for the latter were 1.245, 2.604 and 6.075 seconds respectively. This suggests that the verification time scales roughly linearly with the time horizon for these stable systems.

Table 3(a) shows the scaling of the verification times with the number of dimensions. We consider the a switched variant of nonlinear version of the n interconnected tank system of [1] and a switched nonlinear model with $n/4$ vehicles and each vehicle having 4 continuous variables. For n-tank the initial value of δ is large and this triggers several refinements and for n-vehicles the initial value of δ is small and this decrease (or eliminates) the need for refinements. There are two key observations. First, as the number of refinements increase, the size of the cover increases proportional to the number of dimensions. This is evident in the case of n-tanks, where for the $n = 12$, 1 refinement step required checking of 16 executions, whereas in the case of $n = 24$, 4 refinement steps required 100 executions. Second, as the number of dimensions increase, a smaller value of initial partitioning parameter δ increases the size of the cover exponentially. This is evident in the case of n-vehicles, where adding each new vehicle increased the number of simulations by a factor of 2.

7.4 Dependence on Initial set partition

Table 3(b) shows the verification times for different δ-coverings of the initial set. If the value of δ is too small, then C2E2 generates a large initial partitioning and hence increases the number of simulations. On the other hand, if the initial δ is too large, then C2E2 needs to perform many refinements, and hence, takes more time. The value of optimum value of δ clearly depends on that robustness of the system and the relative distance of simulations from unsafe set. Observe that in Table 3(b), the partitioning with $\delta = 0.2$ takes less time for verification than $\delta = 0.5$ and $\delta = 0.1$. Searching for the optimal value of δ is an interesting direction of future work.

8. CONCLUSIONS AND FUTURE WORK

In this paper we present a class of annotations for dynamical systems which are a generalization of other existing well studied notions of trajectory convergence and divergence studied in Control theory such as Lipschitz constant, Contraction metrics and Incremental stability. Further, we showed that such annotations can also be obtained for systems that exhibit divergent behavior. Verification algorithm for switching systems that exploit simulations and such annotations was presented and was shown to be sound and relatively complete. This is the first simulation-based verification algorithm for nonlinear switched systems that is sound and complete. We have developed a tool C2E2 that implements this algorithm and is integrated to the Simulink/Stateflow modeling framework. Preliminary experimental results demonstrate the promise of this verification approach.

Benchmark	Refs.	Sims.	Time
12-Tanks	1	16	2.744
18-Tanks	4	76	15.238
24-Tanks	4	100	22.126
30-Tanks	4	124	28.824
12-Vehicles	0	32	5.477
16-Vehicles	0	64	12.238
20-Vehicles	0	128	25.144
24-Vehicles	0	256	54.236

(a) Scalability of verification of for n-Tank and n-vehicle systems.

Benchmark	δ	Refs.	Sims.	Time
Nonlin. Adpt.	0.5	16	32	1.01
Nonlin. Adpt.	0.2	9	20	0.91
Nonlin. Adpt.	0.05	5	13	0.58
Nonlin. Adpt.	0.01	0	26	1.32
VanDerPol	0.5	30	96	3.84
VanDerPol	0.2	5	17	0.75
VanDerPol	0.05	8	32	1.44
VanDerPol	0.01	0	120	5.87

(b) Dependence of running time on initial state covers.

Figure 3: Scalability and Initial state covers. Refs: Number of refinements, Sims: Number of simulation traces, Time: Running time of C2E2 in seconds.

As part of future work, one can look at automatic generation of annotations from sample executions, Taylor expansion or Lagrangian remainders. Computing approximate bisimulations for dynamical systems using annotations is also worthwhile investigating.

Acknowledgements: We like to thank Daniel Liberzon for pointers to Incremental Stability and Contraction Metric. The authors were supported by the National Science Foundation research grant CSR 1016791.

9. REFERENCES

[1] M. Althoff, O. Stursberg, and M. Buss. Reachability analysis of nonlinear systems with uncertain parameters using conservative linearization. In *C.D.C.*, 2008.

[2] D. Angeli. A lyapunov approach to incremental stability properties. *IEEE Trans. Automat. Contr.*, 2000.

[3] E. M. Aylward, P. A. Parrilo, and J.-J. E. Slotine. Stability and robustness analysis of nonlinear systems via contraction metrics and sos programming. *Automatica*, 2008.

[4] A. Balluchi, A. Casagrande, P. Collins, A. Ferrari, T. Villa, and A. Sangiovanni-Vincentelli. Ariadne: a framework for reachability analysis of hybrid automata. In *M.T.N.S.*, 2006.

[5] X. Chen, E. Abraham, and S. Sankaranarayanan. Taylor model flowpipe construction for non-linear hybrid systems. In *R.T.S.S.*, 2012.

[6] E. Clarke and P. Zuliani. Statistical model checking for cyber-physical systems. In *A.T.V.A.* 2011.

[7] A. Donzé. Breach, a toolbox for verification and parameter synthesis of hybrid systems. In *C.A.V.* 2010.

[8] A. Donzé and O. Maler. Systematic simulation using sensitivity analysis. *H.S.C.C*, 2007.

[9] P. S. Duggirala, T. Johnson, A. Zimmerman, and S. Mitra. Static and dynamic analysis of timed distributed traces. In *R.T.S.S.*, 2012.

[10] S. Gao, J. Avigad, and E. M. Clarke. Delta-complete decision procedures for satisfiability over the reals. In *I.J.C.A.R.*, 2012.

[11] A. Girard. Verification using simulation. In *H.S.C.C.*, 2006.

[12] A. Girard, G. Pola, and P. Tabuada. Approximately bisimilar symbolic models for incrementally stable switched systems. *IEEE Trans. Automat. Contr.*, 2010.

[13] Z. Huang and S. Mitra. Computing bounded reach sets from sampled simulation traces. In *H.S.C.C.*, 2012.

[14] R. Jobredeaux, T. Wang, and E. Feron. Autocoding control software with proofs i: Annotation translation. In *D.A.S.C.*, 2011.

[15] A. A. Julius, G. E. Fainekos, M. Anand, I. Lee, and G. J. Pappas. Robust test generation and coverage for hybrid systems. In *H.S.C.C.*, 2007.

[16] A. Kanade, R. Alur, F. Ivancic, S. Ramesh, S. Sankaranarayanan, and K. Shashidhar. Generating and analyzing symbolic traces of simulink/stateflow models. In *C. A. V.* 2009.

[17] D. Liberzon. *Switching in Systems and Control*. 2003.

[18] W. Lohmiller and J. J. E. Slotine. On contraction analysis for non-linear systems. *Automatica*, 1998.

[19] K. Manamcheri, S. Mitra, S. Bak, and M. Caccamo. A step towards verification and synthesis from simulink/stateflow models. In *H.S.C.C*, 2011.

[20] N. Nedialkov. Vnode-lp: Validated solutions for initial value problem for odes. Technical report, 2006.

[21] T. Nghiem, S. Sankaranarayanan, G. Fainekos, F. Ivancic, A. Gupta, and G. Pappas. Monte-carlo techniques for falsification of temporal properties of non-linear hybrid systems. In *H.S.C.C*, 2010.

[22] S. Prajna, A. Papachristodoulou, P. Seiler, and P. Parrilo. Sostools: Sum of squares optimization toolbox for matlab. 2004.

[23] B. Sharma and I. Kar. Design of asymptotically convergent frequency estimator using contraction theory. *IEEE Trans. Automat. Contr.*, 2008.

[24] G. Wood and B. Zhang. Estimation of the lipschitz constant of a function. *Journal of Global Optimization*, 1996.

[25] M. Zamani, G. Pola, M. Mazo, and P. Tabuada. Symbolic models for nonlinear control systems without stability assumptions. *IEEE Trans. Automat. Contr.*, 2012.