Proofs from Simulations and Modular Annotations

Zhenqi Huang Sayan Mitra

{zhuang25, mitras}@illinois.edu
Coordinate Science Laboratory
University of Illinois at Urbana Champaign
Urbana, IL 61801

ABSTRACT

We present a modular technique for simulation-based bounded verification for nonlinear dynamical systems. We introduce the notion of input-to-state discrepancy of each subsystem A_i in a larger nonlinear dynamical system A which bounds the distance between two (possibly diverging) trajectories of A_i in terms of their initial states and inputs. Using the IS discrepancy functions, we construct a low dimensional deterministic dynamical system $M(\delta)$. For any two trajectories of A starting δ distance apart, we show that one of them bloated by a factor determined by the trajectory of M contains the other. Further, by choosing appropriately small δ's the overapproximations computed by the above method can be made arbitrarily precise. Using the above results we develop a sound and relatively complete algorithm for bounded safety verification of nonlinear ODEs. Our preliminary experiments with a prototype implementation of the algorithm show that the approach can be effective for verification of nonlinear models.

Keywords

Compositional Verification, Dynamical Systems, Simulation-based Verification, Input-to-state Stability

1. INTRODUCTION

For nonlinear dynamical systems that do not admit analytic solutions, one has to exclusively rely on numerical simulations. Though simulations give sufficient confidence for design, testing, and performance analysis in many application scenarios, for mathematical guarantees or verification, they are of limited use. Particularly resistant to simulation-based verification are nonlinear models with large sets of initial conditions, inputs, and unknown parameters.

Several recent papers [4, 10, 11, 17] present techniques for proving or disproving properties of such models. The details vary to some extent, but the common strategy relies on the following simulate-and-bloat step: For a particular initial state $\mathbf{x}$ and a time bound T, compute a (possibly inaccurate) simulation of the system $\xi_{\mathbf{x}}$ starting from $\mathbf{x}$ upto time T. Then, the simulated trajectory $\xi_{\mathbf{x}}$ is bloated by some factor, to get a *tube* $\mathbf{B}(\xi_{\mathbf{x}})$ that contains all the trajectories starting from a neighborhood $B(\mathbf{x})$ of initial states around $\mathbf{x}$ upto T. The simulate-and-bloat step is repeated for finitely many initial states and their union is guaranteed to over-approximate the reach set of the system from all the initial states up to time T. The technique works as well for dynamical systems with bounded number of unknown parameters, by encoding all the nondeterministic choices in the initial state and it's embarrassingly parallel as the each simulate-and-bloat can be computed independently.

The bloating factor is crucial for performance of verification with the above strategy. From basic continuity of the trajectories, we know that neighboring initial states have trajectories that remain close over time. With more information about the sensitivity of the trajectories to the initial state we get bounds on the distance between neighboring trajectories [16]. For example, Lipschitz continuity of the dynamic function gives a bound on the distance between the neighboring trajectories that grows exponentially with time. Stronger notions like sensitivity, incremental Lyapunov functions, and contraction metrics for dynamical system are used in [5] to obtain more practically useful bounds.

In [11] we defined *discrepancy functions* that generalizes several of these properties and bounds the boating factor as a function of the size of the initial neighborhoods; we used these discrepancy functions for bounded time verification of nonlinear and switched models. But there are no general techniques for computing discrepancy functions (or for that matter sensitivity, contraction metrics and incremental Lyapunov functions) from the syntactic description of a dynamical system. One typically assumes a template polynomial for the candidate function and then solves an optimization problem to find the coefficients or assumes that this information is provided by the system designer as an annotation to the model. Obviously, the problem of finding these annotations becomes harder for larger models in which many components interact.

In this paper, present a new technique for simulation and approximation-based verification for large dynamical systems which only uses *input-to-state discrepancy* for the smaller constituent subsystems. Consider a large dynamical system A consisting of several interacting subsystems $A_1, \ldots, A_N$, that is, the input signals of a subsystem A_i are driven by the outputs (or states) of some other components A_j. Lets say that each A_i is n-dimensional which makes A nN-dimensional.

Our main idea in this paper is to use a new type of input-to-state discrepancy function (IS discrepancy) for each subsystem A_i to construct a (small) $N+1$-dimensional dynamical system M that bounds the needed bloating factor for A. An IS discrepancy for A_i (together with its witnesses) gives a bound on the distance between two trajectories as a function of (a) their initial states and (b) the inputs they experience.

Input-to-state stability (ISS), its variants and their characterization in terms of necessary and sufficient conditions have been one of the major advances of nonlinear control theory in the last two decades [2,3,25]. Incremental ISS has been used to construct discrete symbolic models that approximately bisimulate continuous systems [15, 23]. Under additional assumptions about the stability of the overall system, it has been shown that a large system can be reduced to a smaller system with similar behaviors [26]. Our work is the first to connect these ideas to simulation-based safety verification of composed systems. Moreover, our technique does not rely on any stability assumptions of the composed system. Though our results do not give new techniques for computing IS discrepancy functions, but they do reassure that if such techniques are developed for smaller or special types of nonlinear models, then larger compositions of such subsystems can be automatically verified.

Contributions. (i) We introduce a method for constructing an approximation of a composed dynamical system using the IS discrepancy functions of the components (Definition 4). Specifically, we use the collection of IS discrepancy functions for the subsystems to define a family of dynamical systems $M(\delta)$, where the parameter δ defines the initial state of M.

(ii) We show that $M(\delta)$ has a unique trajectory μ, and that any trajectory $\xi_{\mathbf{x}}$ of A point-wise bloated by the value of $\mu(t)$ contains the reach set of all the trajectories of A starting from a δ-ball around $\mathbf{x}$ (Theorem 5.4). Thus, by simulating A and (the smaller) M we can compute bounded-time reach set overapproximations of A.

(iii) We also show that by choosing appropriately small δ's the overapproximations computed by the above method can be made arbitrarily precise; modulo the precision of the numerical simulations (Theorem 5.7).

(iv) Using the above results we develop an algorithm for bounded safety verification of nonlinear dynamical systems that iteratively refines initial set partitions (Algorithm 1). We show that the algorithm is sound and is guaranteed to terminate whenever the model is robustly safe or unsafe with respect to a given unsafe set. Our preliminary experimental results with a prototype implementation of the algorithm validates the approach and underscore its promise.

2. PRELIMINARIES

We will use the notations from the hybrid I/O automaton (HIOA) framework for modeling compositions of dynamical systems [19, 21]. For a natural number $n \in \mathbb{N}$, $[n]$ is the set $\{1, 2, \ldots, n\}$. For a sequence A of objects of any type with n elements, we refer to the i^{th} element, $i \leq n$ by A_i. Let V be a finite set of real-valued variables. Variables are names for state and input components. A *valuation* $\mathbf{v}$ *for* V is a function mapping each variable name to its value in $\mathbb{R}$. The set of valuations for V is denoted by $Val(V)$.

For any function $f : A \to B$ and a set $S \subseteq A$, $f \lceil S$ is the restriction of f to S. That is, $(f \lceil S)(s) = f(s)$ for each $s \in S$. So, for a variable $v \in V$ and a valuation $\mathbf{v} \in Val(V)$, $\mathbf{v} \lceil v$ is the function mapping $\{v\}$ to the value $\mathbf{v}(v)$.

Trajectories model the continuous evolution of variable valuations over time. A *trajectory* for V is a differentiable function $\tau : \mathbb{R}_{\geq 0} \to Val(V)$. The set of all possible trajectories for V is denoted by $Traj(V)$. For any function $f : C \to [A \to B]$ and a set $S \subseteq A$, $f \downarrow S$ is the restriction of $f(c)$ to S. That is, $(f \downarrow S)(c) = f(c) \lceil S$ for each $c \in C$. In particular, for a variable $v \in V$ and a trajectory $\tau \in Traj(V)$, $\tau \downarrow v$ is the trajectory of v defined by τ.

Valuations can be viewed as vectors in $\mathbb{R}^{|V|}$ dimensional space with by fixing some arbitrary ordering on variables. For a valuation $\mathbf{v}$, $|\mathbf{v}|$ is ℓ^2-norm of the vector of variable values. $B_\delta(\mathbf{v}) \subseteq Val(V)$ is the closed ball of valuations with radius δ centered at $\mathbf{v}$. The notions of continuity, differentiability, and integration are lifted to functions defined over sets of valuations in the usual way.

A function $f : A \to \mathbb{R}$ is *Lipschitz* if there exists a constant $L \geq 0$—called the *Lipschitz constant*—such that for all $a_1, a_2 \in A$ $|f(a_1) - f(a_2)| \leq L|a_1 - a_2|$. A continuous function $\alpha : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is in the *class of* $\mathcal{K}$ *functions* if $\alpha(0) = 0$ and it is strictly increasing. Class $\mathcal{K}$ functions are closed under composition and inversion. A class $\mathcal{K}$ function α is a *class* $\mathcal{K}_\infty$ function if $\alpha(x) \to \infty$ as $x \to \infty$. A continuous function $\beta : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is called a *class* $\mathcal{KL}$ *function* if for any t, $\beta(x, t)$ is a class $\mathcal{K}$ function in x and for any x, $\beta(x, t) \to 0$ as $t \to \infty$.

3. MODELS AND COMPOSITION

3.1 Dynamical System Modules

A dynamical system is specified by a collection of ordinary differential equations (ODEs), possibly with inputs, and a set of initial states. For reducing notational complexity, we identify output variables with state variables in this paper but our results can be extended to systems where outputs are distinct in a straightforward manner. The following definition introduces this class of dynamical systems.

Definition 1. *A* dynamical system *A is a tuple $\langle X, U, \Theta, f \rangle$ where*

(i) X is a set of variables called the state variables*; valuations of X are called* state*;*

(ii) U is a set of variables called the input variables *that are distinct from the state variables;*

(iii) $\Theta \subseteq Val(X)$ is a compact set of initial states*;*

(iv) $f : Val(X) \times Val(U) \to Val(X)$ is called the dynamic mapping*. In addition, f is Lipschitz continuous with respect to both arguments.*

An *input signal* of A is a trajectory of input variables $\eta \in Traj(U)$. For a given input signal $\eta \in Traj(U)$ and an initial state $\mathbf{x} \in \Theta$, the *solution* (or trajectory) of A is a state trajectory $\xi \in Traj(X)$ satisfying: (a) $\xi(0) = \mathbf{x}$, (b) for any $t \in \mathbb{R}_{\geq 0}$, the time derivative of ξ at t satisfies the differential equation:

$$\dot{\xi}(t) = f(\xi(t), \eta(t)). \tag{1}$$

Under the Lipschitz assumption of the dynamic mapping (iv) and the differentiability of η, the differential equation (1) admits a unique solution. This solution ξ is uniquely defined by the initial state $\mathbf{x} \in Val(X)$ and the input signal $\eta \in$

$Traj(U)$. A dynamical system without inputs ($U = \varnothing$) is said to be *closed*; otherwise, it is *open*. For closed system, for any $\mathbf{x} \in Val(X)$, $Traj(A, \mathbf{x})$ is a singleton.

Notations. The set of all trajectories of A with respect to a set of initial states $\Theta' \subseteq Val(X)$ and a set of input signals $H \subseteq Traj(U)$ is denoted by $Traj(A, \Theta', H)$. We will drop the argument H for closed dynamical systems. The components of dynamical system A and A_i are denoted by $X_A, U_A, \Theta_A, f_{\mathcal{A}}$ and X_i, U_i, Θ_i, f_i, respectively. We will drop the subscripts when they are clear from context.

Next, for a closed dynamical system A we define reachable states and safety. A state $\mathbf{x} \in Val(X)$ is *T-reachable* if there exists a trajectory $\xi \in Traj(A, \Theta, \varnothing)$ and a time $t \leq T$ such that the trajectory $\xi(t) = \mathbf{x}$. The set of T-reachable states is denoted by $\mathsf{Reach}_A(\Theta, T)$ and the set of all reachable states is denoted by $\mathsf{Reach}_A(\Theta)$.

Definition 2. *For $\epsilon \geq 0$ and time $T \geq 0$, and an open unsafe set $\mathbb{U} \subseteq Val(X)$, A is* ϵ-robustly safe up to T with respect to $\mathbb{U}$ *if $B_\epsilon(\mathsf{Reach}_A(\Theta, T)) \cap \mathbb{U} = \varnothing$. If there exists some $\epsilon > 0$ for which this condition holds, then A is* robustly safe up to T with respect to $\mathbb{U}$.

There are a rich body of studies where static analysis is used to compute reachable sets (see for example [12–14]). In this paper, we present an approach uses modular annotations for dynamic analysis.

3.2 Composition of Modules

Large and complex dynamical system models are created by *composing* smaller modules or subsystems. Formally, the composition operation takes a pair of compatible subsystems and defines a new dynamical system by plugging-in or identifying the input variables of one subsystem with state variables of another. Several subsystems can be composed inductively. The resulting system may still have input variables that are not identified with any of the state variables. A pair of dynamical subsystems A_1 and A_2 are *compatible* if they do not share any of the state variables $X_1 \cap X_2 = \varnothing$.

Definition 3. *For a pair of compatible dynamical systems $A_1 = \langle X_1, U_1 \Theta_1, f_1 \rangle$ and $A_2 = X_2, U_2, \Theta_2, f_2 \rangle$, their composition $A = A_1 \| A_2$ is the tuple $\langle X, U, \Theta, f \rangle$, where*

(i) $X = X_1 \cup X_2$,

(ii) $U = U_1 \cup U_2 \setminus (X_1 \cup X_2)$,

(iii) $\Theta = \{\mathbf{x} \in Val(X) \mid (\mathbf{x} \lceil X_i) \in \Theta_i, i \in \{1, 2\}\}$, *and*

(iv) $f : Val(X) \times Val(U) \to Val(X)$ *is defined as: For each* $\mathbf{x} \in Val(X), \mathbf{u} \in Val(U)$, $i \in \{1, 2\}$, $f(\mathbf{x}, \mathbf{u}) \lceil X_i = f_i(\mathbf{x} \lceil X_i, \mathbf{w})$, *where for each $u \in U_i$:*

$$\mathbf{w}(u) = \begin{cases} \mathbf{x}(u) & \text{if } u \in X \backslash X_i, \\ \mathbf{u}(u) & \text{otherwise.} \end{cases}$$

The definition of $\mathbf{w}$ creates a valuation for U_1 by combining valuations of X_2 and U, (creates a valuation for U_2 by combining valuations of X_1 and U). The definition for f ensures that the inputs to A_1 that come from A_2 are mapped correctly and those that are left unmapped remain as inputs variables in A. It can be checked that f is Lipschitz since f_1 and f_2 are. Therefore $\mathcal{A}$ is indeed a dynamical system and has well-defined trajectories for differentiable input signals.

Example 1. *Consider a dynamical synchronization problem where multiple subsystems start from different initial states and communicate to agree on a trajectory [24]. The interaction is shown by the graph in Figure 1. Each A_i, $i \in \{1, 2, 3\}$, is a dynamical system with the following components: (i) $X_i = \{x_{i1}, x_{i2}, x_{i3}, x_{i4}\}$, (ii) Θ_i is a compact subset of $Val(X_i)$, (iii) $U_1 = X_2, U_2 = X_1 \cup X_3$ and $U_3 = X_1$, [1] and (iv) for all $\mathbf{x}_1 \in Val(X_1), \mathbf{u}_1 \in Val(U_1)$, $f_1(\mathbf{x}_1, \mathbf{u}_1) = D\mathbf{x}_1 + \mathbf{u}_1$. Similarly, $f_2(\mathbf{x}_2, \mathbf{u}_2) = D\mathbf{x}_2 + \frac{1}{2}[I, I]\mathbf{u}_2$ and $f_3(\mathbf{x}_3, \mathbf{u}_3) = D\mathbf{x}_3 + \mathbf{u}_3$, where D is a 4×4 matrix, I is the identity matrix.*

According to Definition 3, the overall system $A = A_1 \| A_2 \| A_3$ with (i) $U_A = \varnothing$, and (ii) for any $\mathbf{x} \in Val(X_A)$,

$$f_{\mathcal{A}}(\mathbf{x}) = \begin{bmatrix} D & I & 0 \\ 0.5I & D & 0.5I \\ I & 0 & D \end{bmatrix} \mathbf{x}.$$

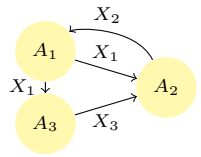

Figure 1: Illustration of Example 1.

For a closed composed system $A = A_1 \| \ldots \| A_N$, a subsystem A_i's input variables are in the set of state variables of A: $U_i \subseteq X_A$. For any state $\mathbf{x}$ of A, let $\xi = Traj(A, \mathbf{x})$ be the trajectory of A. It can be shown that for any subsystem A_i, the restriction of ξ onto A_i's state variables is a trajectory of A_i under the input signal η_i, where η_i is defined as ξ restricted to A_i's input variables. That is $\xi \downarrow X_i = Traj(A_i, \mathbf{x}(X_i), \xi \downarrow U_i)$.

4. INPUT-TO-STATE ANNOTATIONS

For bounded time safety verification of complex dynamical systems, we propose to use annotations for the individual modules. We rely on designers to provide these annotations, perhaps based on their insights about module's designed behavior or through additional computations performed explicitly for finding annotations. In Section 4.2 we relate these annotations to several existing concepts that are used in the control theory literature for stability analysis.

4.1 IS Discrepancy

Roughly, the annotation of a module A bounds the distance between two trajectories of A with different initial states and inputs. We call such an annotation an *input-to-state discrepancy function* or simply an IS discrepancy function.

Definition 4. *For a dynamical system A, a continuous functions $V : Val(X)^2 \to \mathbb{R}_{\geq 0}$ is an* input-to-state discrepancy function *in if*

(i) $\exists$ *class-$\mathcal{K}$ functions $\underline{\alpha}, \overline{\alpha}$ such that for any $\mathbf{x}, \mathbf{x}' \in Val(X)$, $\underline{\alpha}(|\mathbf{x} - \mathbf{x}'|) \leq V(\mathbf{x}, \mathbf{x}') \leq \overline{\alpha}(|\mathbf{x} - \mathbf{x}'|)$, and*

(ii) $\exists \beta : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ *of class-$\mathcal{K}$ in the first argument and $\gamma \in \mathcal{K}$ such that for any $\theta, \theta' \in \Theta$, input trajectories $\eta, \eta' \in Traj(U)$, and $t \in \mathbb{R}_{\geq 0}$,*

$$V(\xi(t), \xi'(t)) \leq \beta(|\theta - \theta'|, t) + \int_0^t \gamma(|\eta(s) - \eta'(s)|) ds, \tag{2}$$

[1] Here we assume that $Val(U_1)$ and $Val(X_2)$ has the same variables ordering, etc.

where $\xi = Traj(A, \theta, \eta)$ *and* $\xi' = Traj(A, \theta', \eta')$.

$(\underline{\alpha}, \overline{\alpha}, \beta, \gamma)$ *are the* witnesses *of the discrepancy function.*

The discrepancy function (and it's witnesses) bounds the maximum distance between two trajectories in terms of the ℓ^2 distance between their input signals and their initial states. In the rest of the paper, we further assume that $\underline{\alpha}^{-1}$ and γ are Lipschitz, and $\beta(\cdot, \cdot)$ has a Lipschitz continuous derivative in the second argument. In general the IS discrepancy annotations have to be provided with the system model. However for some classes of models, annotations may be computed automatically or obtained from other certificates used for stability proofs.

4.2 Finding IS discrepancy

We note 3 different ways of obtaining IS discrepancy functions.

Lipschitz Dynamics. If the dynamic mapping f of system A is Lipschitz, then for any bounded time $T > 0$, we can find a IS discrepancy function of A that holds for all $t \in [0, T]$. This version of IS discrepancy will be enough for bounded safety proofs. The Lipschitz constants can be computed for linear, polynomial and some several other types of functions [27].

Proposition 4.1. *Suppose the dynamic mapping f of system A is Lipschitz in both argument. For any time bound $T > 0$, $V(\mathbf{x}, \mathbf{x}') = |\mathbf{x} - \mathbf{x}'|$ is a discrepancy function with witnesses $(\underline{\alpha}, \overline{\alpha}, \beta, \gamma)$ where $\underline{\alpha}(|\mathbf{x} - \mathbf{x}'|) = \overline{\alpha}(|\mathbf{x} - \mathbf{x}'|) = |\mathbf{x} - \mathbf{x}'|$, $\beta(|\theta - \theta'|, t) = e^{Lt}|\theta - \theta'|$ and $\gamma(|\mathbf{u} - \mathbf{u}'|) = Le^{LT}|\mathbf{u} - \mathbf{u}'|$.*

IS discrepancy functions obtain in this way will have witnesses β and γ exponentially growing in time.

Stable Linear Systems. Suppose A' dynamic mapping $f(\mathbf{x}, \mathbf{u}) = C\mathbf{x} + D\mathbf{u}$, where C is a $n \times n$ matrix and D is a $n \times m$ matrix. If C is asymptotically stable, then its trajectories converge exponentially. And we can get an IS dependency function with exponentially convergent witnesses.

Proposition 4.2. *For linear system A with dynamic mapping $f(\mathbf{x}, \mathbf{u}) = C\mathbf{x} + D\mathbf{u}$ with C stable, there exists $\lambda > 0$, $V(\mathbf{x}, \mathbf{x}') = |\mathbf{x} - \mathbf{x}'|$ is a discrepancy function with witnesses $(\underline{\alpha}, \overline{\alpha}, \beta, \gamma)$ where $\underline{\alpha}(|\mathbf{x} - \mathbf{x}'|) = \overline{\alpha}(|\mathbf{x} - \mathbf{x}'|) = |\mathbf{x} - \mathbf{x}'|$, $\beta(|\theta - \theta'|, t) = e^{-\lambda t}|\theta - \theta'|$ and $\gamma(|\mathbf{u} - \mathbf{u}'|) = |D||\mathbf{u} - \mathbf{u}'|$.*

The positive constant λ can be found algorithmically through solving Lyapunov equation [6].

Incremental Integral ISS. The notion of incremental integral input-to-state stability (incremental integral ISS) of dynamical systems [2] is a generalization of the standard notions of input-to-state stability [1, 3, 25]. A Lyapunove like theorem of proving incremental integral ISS as well as a converse Lyapunov theorem are presented in [2]. Given a proof of an incremental integral ISS property of a model, we get its IS discrepancy function (with witnesses) for free.

Definition 5. *A dynamical system A is called incremental integral input-to-state stable (ISS) if there exists a class-$\mathcal{K}_\infty$ function α, a class-$\mathcal{KL}$ function β and a class-$\mathcal{K}$ function γ such that, for any initial states $\theta, \theta' \in \Theta_A$, for any input signal $\eta, \eta' \in U_A$ and any $t > 0$,*

$$|\alpha(|\xi(t) - \xi'(t)|)| \leq \beta(|\theta - \theta'|, t) + \int_0^t \gamma(|\eta(s) - \eta'(s)|)ds. \quad (3)$$

where $\xi = Traj(A, \theta, \eta)$ *and* $\xi' = Traj(A, \theta', \eta')$.

Proposition 4.3. *Given an incremental integral ISS system A with (α, β, γ) as in Definition 5, then $V(\mathbf{x}, \mathbf{x}') = \alpha(|\mathbf{x} - \mathbf{x}'|)$ is a discrepancy function with witnesses $(\underline{\alpha}, \overline{\alpha}, \beta, \gamma)$ where $\underline{\alpha}(|\mathbf{x} - \mathbf{x}'|) = \overline{\alpha}(|\mathbf{x} - \mathbf{x}'|) = \alpha(|\mathbf{x} - \mathbf{x}'|)$, and β, γ given above.*

5. SMALL APPROXIMANTS FROM IS DISCREPANCY

In this section we define an one-dimensional approximation for dynamical subsystems (Definition 6) that use input-to-state discrepancy functions. For the sake of a cleaner presentation, we develop the results for a dynamical system consisting of two modules with a two-dimensional approximation. The general results follow by straightforward extension and are stated in Section 5.4.

5.1 IS Approximation of $A_1 \| A_2$

Consider the closed dynamical system $A = A_1 \| A_2$, with $X_1 = U_2$ and $X_2 = U_1$ as shown in Figure 2. Let V_i be

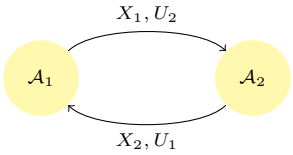

Figure 2: A dynamical system with two modules.

the IS discrepancy function for $A_i, i \in \{1, 2\}$ with witness $(\underline{\alpha}_i, \overline{\alpha}_i, \beta_i, \gamma_i)$. For any pair of initial states θ, θ' in Θ_A, let $\xi = Traj(A, \theta)$ and $\xi' = Traj(A, \theta')$ be the unique trajectories starting from them. We define $\xi_i = \xi \downarrow X_i$ and $\xi_i' = \xi' \downarrow X_i$. From Section 3.2, the restriction of ξ_i and ξ_i' to X_i are trajectories of A_i from $\theta \lceil X_i$ and $\theta' \lceil X_i$. From Definition 4, for every $t \in [0, T]$ the following holds:

$$V_1(\xi_1(t), \xi_1'(t)) \leq \beta_1(|\theta_1 - \theta_1'|, t) + \int_0^t \gamma_1(|\xi_2(s) - \xi_2'(s)|)ds,$$
$$V_2(\xi_2(t), \xi_2'(t)) \leq \beta_2(|\theta_2 - \theta_2'|, t) + \int_0^t \gamma_2(|\xi_1(s) - \xi_1'(s)|)ds. \quad (4)$$

Next, we introduce the key notion of a family of IS approximations for A. Each approximation is parameterized by nonnegative reals δ_1 and δ_2 and is a closed dynamical system M with two main variables m_1 and m_2. As we shall see in Theorem 5.4, at any time t, m_1 gives an upper-bound on the distance between two state trajectories of A_1 that start from neighboring states at most δ_1 apart. Similarly, m_2 gives an upper-bound on neighboring trajectories of A_2.

Of course, the distance between two neighboring state trajectories of A_1 depend (a) their initial states and (b) on the inputs they experience. These inputs in turn, depend on the corresponding state trajectories of A_2. So, the dynamics of m_1 (and m_2) takes into account the impact of both of these factors using the witnesses of the IS discrepancy functions. Since the β witness bounds the impact of initial states on the discrepancy a function of time, the dynamics of m_1 (and m_2) is time varying. For convenience, we have therefore introduced a third clock variable (clk) in M.

Definition 6. *For any pair of nonnegative constants* (δ_1, δ_2)*, the* (δ_1, δ_2)-IS approximation *of* A *is a closed dynamical system* $M = \langle X_M, \Theta_M, U_M, f_M \rangle$ *where*

(i) $X_M = \{m_1, m_2, clk\}$,

(ii) $\Theta_M = \{\theta\}$ *where* θ *defined by* $\theta(m_i) = \beta_i(\delta_i, 0)$*, for* $i \in \{1, 2\}$*, and* $\theta(clk) = 0$,

(iii) $U_M = \varnothing$*, and*

(iv) for any valuation $\mathbf{x} \in Val(X_M)$,

$$f_M(\mathbf{x}) = \begin{bmatrix} \dot{\beta}_1(\delta_1, \mathbf{x}(clk)) + \gamma_1 \circ \underline{\alpha}_2^{-1}(\mathbf{x}(m_2)) \\ \dot{\beta}_2(\delta_2, \mathbf{x}(clk)) + \gamma_2 \circ \underline{\alpha}_1^{-1}(\mathbf{x}(m_1)) \\ 1 \end{bmatrix}. \quad (5)$$

The last component of f_M is the constant 1 and in the initial state $clk = 0$; it follows that along any trajectory μ of M, clk tracks the real time: $\mu(t) \lceil clk = t$. The witness functions $\underline{\alpha}_1^{-1}, \gamma_1$, etc., are Lipschitz and Lipschitz functions are closed under composition, and therefore, f_M is Lipschitz with respect to m_1 and m_2. $\beta_i(\cdot, \cdot)$ has Lipschitz derivatives in the second argument which implies that f_M is also Lipschitz with respect to clk. Thus, M is indeed a closed, deterministic dynamical system with a single initial state and a unique trajectory. Note that both the initial state and the dynamics of M depend on the choice of the parameters δ_1 and δ_2. In Theorem 5.4 we relate m_1 and m_2 with the divergence between trajectories of A_1 and A_2. Specifically, if μ is the trajectory of a (δ_1, δ_2)-IS approximation then $\mu_i = \mu \downarrow m_i(t)$ gives an upperbound on the distance between the trajectories of A_i starting from initial states that are at most δ_i apart.

5.2 Overapproximation with IS Discrepancy

Before diving into technical details, we introduce a couple of notations. For any pair of non-negative reals $\delta = (\delta_1, \delta_2)$ and any state $\mathbf{x} \in Val(X_A)$, we define

$$B_\delta(\mathbf{x}) = B_{\delta_1} \lceil \mathbf{x}(X_1) \times B_{\delta_2}(\mathbf{x} \lceil X_2)$$

as the product of the δ_i-balls around $\mathbf{x} \lceil X_i$. Given a pair of discrepancy functions $V = (V_1, V_2)$ for A_1 and A_2, a state $\mathbf{m} \in Val(X_M)$ of M naturally defines a sublevel set in $Val(X_A) \times Val(X_A)$. In what follows, we denote by $L_V(\mathbf{m}) \subseteq Val(X_A) \times Val(X_A)$ the set

$$\{(\mathbf{x}, \mathbf{x}') \mid \forall i \in \{1, 2\},\ V_i(\mathbf{x} \lceil X_i), \mathbf{x}' \lceil X_i) \leq \mathbf{m} \lceil m_i\}.$$

This set is the intersection of the $(\mathbf{m} \lceil m_i)$-*sublevel sets* of V_i. For a state $\mathbf{x} \in Val(X_A)$ of A and a state $\mathbf{m} \in Val(X_M)$ we define

$$B^V_{\mathbf{m}}(\mathbf{x}) = \{\mathbf{x}' \in Val(X_A) \mid (\mathbf{x}, \mathbf{x}') \in L_V(\mathbf{m})\}$$

as the subset of states of A for which $(\mathbf{x}, \mathbf{x}')$ in the sublevel set defined by $\mathbf{m}$.

We ultimately show that the trajectory of M always upper bounds the right-hand side of Equation (4), that is,

$$\begin{aligned} \mu_1(t) &\geq \beta_1(|\theta_1 - \theta_1'|, t) + \int_0^t \gamma_1(|\xi_2(s) - \xi_2'(s)|)ds, \\ \mu_2(t) &\geq \beta_2(|\theta_2 - \theta_2'|, t) + \int_0^t \gamma_2(|\xi_1(s) - \xi_1'(s)|)ds. \end{aligned} \quad (6)$$

From the construction of M, we observe that at time $t = 0$, the above inequalities hold. Moreover, the first derivatives of the left-hand sides upper bound those of the right-hand sides at time $t = 0$. However, this property at $t = 0$ cannot immediately be generalized to all $t > 0$. In our proof, we first construct a strict upper bound of the right-hand sides of (6) that holds for all t, and then show that this bound converges to $\mu(\cdot)$.

First, for any positive $\epsilon > 0$, we construct a pair of ϵ-factor trajectories $(\mu_{1\epsilon}, \mu_{2\epsilon})$ with derivatives ϵ-close to the first two components of f_M and show that these trajectories strictly upper-bound the discrepancy functions of V_1 and V_2.

For any $\delta_1, \delta_2 \geq 0$ and any $\epsilon > 0$, a pair of trajectories $\mu_{1\epsilon}, \mu_{2\epsilon} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ are defined as solutions to the differential equations:

$$\dot{\mu}_{1\epsilon} = \dot{\beta}_1(\delta_1, t) + \gamma_1 \circ \underline{\alpha}_2^{-1}(\mu_{2\epsilon}) + \epsilon, \text{ and} \quad (7)$$

$$\dot{\mu}_{2\epsilon} = \dot{\beta}_2(\delta_2, t) + \gamma_2 \circ \underline{\alpha}_1^{-1}(\mu_{1\epsilon}) + \epsilon, \quad (8)$$

with $\mu_{1\epsilon}(0) = \beta_1(\delta_1, 0) + \epsilon$ and $\mu_{2\epsilon}(0) = \beta_2(\delta_2, 0) + \epsilon$. The right-hand side of Equation (7) is Lipschitz, and therefore, $\mu_{1\epsilon}$ and $\mu_{2\epsilon}$ are well-defined. For any two initial states of A θ, θ', we define two differentiable functions $g_1, g_2 : \mathbb{R}_{\geq 0} \to \mathbb{R}$:

$$\begin{aligned} g_1(t) &= \mu_{1\epsilon}(t) - \beta_1(\delta_1, t) - \textstyle\int_0^t \gamma_1(|\xi_2(s) - \xi_2'(s)|)ds, \\ g_2(t) &= \mu_{2\epsilon}(t) - \beta_2(\delta_2, t) - \textstyle\int_0^t \gamma_2(|\xi_1(s) - \xi_1'(s)|)ds. \end{aligned} \quad (9)$$

Recall that $\xi = Traj(A, \theta)$ and $\xi' = Traj(A, \theta')$ are the trajectories of A starting from θ and θ'.

Proposition 5.1. *Consider any non-negative pair* $\delta = (\delta_1, \delta_2)$ *and initial states* $\theta, \theta' \in \Theta_A$ *such that* $\theta' \in B_\delta(\theta)$*. Let* $\xi = Traj(A, \theta)$ *and* $\xi' = Traj(A, \theta')$*. Then, for any* $\epsilon > 0, t \geq 0$*, if* $g_1(t), g_2(t) > 0$*, then*

$$V_1(\xi_1(t), \xi_1'(t)) < \mu_{1\epsilon}(t), \text{ and } V_2(\xi_2(t), \xi_2'(t)) < \mu_{2\epsilon}(t).$$

Proof. Here we prove the bound for V_1; the bound for V_2 follows by symmetry. For any $t \geq 0$, since $g_1(t) > 0$,

$$\mu_{1\epsilon}(t) > \beta_1(\delta_1, t) + \int_0^t \gamma_1(|\xi_2(s) - \xi_2'(s)|)ds. \quad (10)$$

From $\theta' \in B_\delta(\theta)$, we have $|\theta_1 - \theta_1'| \leq \delta_1$. Since $\beta_1(\cdot, t)$ is a class-$\mathcal{K}$ function, it follows that

$$\beta_1(\delta_1, t) \geq \beta_1(|\theta_1 - \theta_1'|, t).$$

Thus, Equation (10) becomes

$$\mu_{1\epsilon}(t) > \beta_1(|\theta_1 - \theta_1'|, t) + \int_0^t \gamma_1(|\xi_2(s) - \xi_2'(s)|)ds.$$

By applying Equation (4), it follows that

$$\begin{aligned} \mu_{1\epsilon}(t) &> \beta_1(|\theta_1 - \theta_1'|, t) + \textstyle\int_0^t \gamma_1(|\xi_2(s) - \xi_2'(s)|)ds \\ &\geq V_1(\xi_1(t), \xi_1'(t)). \end{aligned}$$

□

The next lemma, establishes that we can drop the assumption about the positivity of g_1 and g_2 and still arrive at the conclusion of Proposition 5.1.

Lemma 5.2. *Consider any non-negative pair* $\delta = (\delta_1, \delta_2)$*, and initial states* $\theta, \theta' \in \Theta_A$ *such that* $\theta' \in B_\delta(\theta)$*. Let* $\xi =$

$Traj(A,\theta)$ and $\xi' = Traj(A,\theta')$. Thus, for any $\epsilon > 0, t \geq 0$,

$$V_1(\xi_1(t),\xi_1'(t)) < \mu_{1\epsilon}(t) \text{ and } V_2(\xi_2(t),\xi_2'(t)) < \mu_{2\epsilon}(t).$$

Proof. By Proposition 5.1, it suffices to prove that for all $t \geq 0$, $g_1(t), g_2(t) > 0$. At $t = 0$,

$$g_1(0) = \beta_1(\delta_1, 0) + \epsilon - \beta_1(\delta_1, 0) = \epsilon > 0.$$

Similarly, $g_2(0) > 0$. Suppose for the sake of contradiction that $t_a > 0$ is the first time when $g_1(t), g_2(t) > 0$ is violated. From the continuity of g_1, g_2, we have that the both following conditions hold:

(i) $g_1(t), g_2(t) > 0$ for all $t \in [0, t_a)$, and

(ii) $g_1(t_a) = 0$ or $g_2(t_a) = 0$.

Without loss of generality, we assume $g_1(t_a) = 0$. From mean value theorem, there exists some time $t_b \in (0, t_a)$ such that

$$\dot{g}_1(t_b) = \frac{g_1(0) - g_1(t_a)}{0 - t_a} \leq -\frac{\epsilon}{t_a} < 0. \tag{11}$$

We can bound the derivative $\dot{g}_1(t_b)$ as:

$$\dot{g}_1(t_b) = \dot{\mu}_{1\epsilon}(t_b) - \frac{d}{dt}\left(\beta_1(\delta_1, t_b) + \int_0^{t_b} \gamma_1(|\xi_2(s) - \xi_2'(s)|)ds\right).$$

Plugging the right-hand side of Equation (7) into the above equation, it follows:

$$\begin{aligned} \dot{g}_1(t_b) &= \dot{\beta}_1(\delta_1, t_b) + \gamma_1 \circ \underline{\alpha}_2^{-1}(\mu_{2\epsilon}(t_b)) + \epsilon \\ &\quad - \dot{\beta}_1(\delta_1, t_b) - \gamma_1(|\xi_2(t_b) - \xi_2'(t_b)|) \\ &= \epsilon + \left(\gamma_1 \circ \underline{\alpha}_2^{-1}(\mu_{2\epsilon}(t_b)) - \gamma_1(|x_2(t_b) - x_2'(t_b)|)\right). \end{aligned} \tag{12}$$

From condition (i), we know $g_2(t_b) > 0$. It follows from Proposition 5.1 that

$$\mu_{2\epsilon}(t_b) > V_2(\xi_2(t_b), \xi_2'(t_b)). \tag{13}$$

From Definition 4, we have $V_2(\xi_2(t_b), \xi_2'(t_b)) \geq \underline{\alpha}_2(|\xi_2(t_b) - \xi_2'(t_b)|)$. Equation (13) yields $\mu_{2\epsilon}(t_b) > \underline{\alpha}_2(|\xi_2(t_b) - \xi_2'(t_b)|)$. Because $\gamma \circ \underline{\alpha}_2^{-1}$ is a class-$\mathcal{K}$ function, it follows that

$$\gamma_1 \circ \underline{\alpha}_2^{-1}(\mu_{2\epsilon}(t_b)) \geq \gamma_1(|\xi_2(t_b) - \xi_2'(t_b)|).$$

Combining the above equation with Equation (12), we have that $\dot{g}_1(t_b) \geq \epsilon > 0$, which contradicts to Equation (11). □

Lemma 5.2 shows that for any $\epsilon > 0$, the ϵ-factor trajectories $\mu_{1\epsilon}$ and $\mu_{2\epsilon}$ give strict upper bounds on the distance between corresponding trajectories of A_1 and A_2. In the following lemma, we show that as $\epsilon \to 0$, $\mu_{i\epsilon}$ converges to the trajectory $\mu \downarrow m_i$; recall that μ is the trajectory of the IS approximation M. It follows that the trajectory μ indeed bounds the divergence of any trajectories of A.

Lemma 5.3. *Consider any non-negative pair $\delta = (\delta_1, \delta_2)$ and initial states $\theta, \theta' \in \Theta_A$ such that $\theta' \in B_\delta(\theta)$. Let $\xi = Traj((A,\theta))$, $\xi' = Traj((A,\theta'))$, and μ be the trajectory of A's (δ_1, δ_2)-IS approximation M. Then for all $t \geq 0$,*

$$(\xi(t), \xi'(t)) \in L_V(\mu(t)).$$

Proof. For brevity we write $\mu \downarrow m_i$ as μ_i and $\mu \downarrow clk$ as clk. Recall, we have $clk(t) = t$. Rewiriting the condition that the solution μ of M satisfies the differential equation defined by f_M, we have

$$\begin{aligned} \dot{\mu}_1(t) &= \dot{\beta}_1(\delta_1, t) + \gamma_1 \circ \underline{\alpha}_2^{-1}(\mu_2(s))ds, \\ \dot{\mu}_2(t) &= \dot{\beta}_2(\delta_2, t) + \gamma_2 \circ \underline{\alpha}_1^{-1}(\mu_1(s))ds, \\ \dot{clk}(t) &= 1. \end{aligned} \tag{14}$$

By integrating both sides with initial condition $\mu_1(0) = \beta_1(\delta_1, 0)$ and $\mu_2(0) = \beta_2(\delta_2, 0)$, we have,

$$\begin{aligned} \mu_1(t) &= \beta_1(\delta_1, t) + \textstyle\int_0^t \gamma_1 \circ \underline{\alpha}_2^{-1}(\mu_2(s))ds, \\ \mu_2(t) &= \beta_2(\delta_2, t) + \textstyle\int_0^t \gamma_2 \circ \underline{\alpha}_1^{-1}(\mu_1(s))ds, \\ clk(t) &= t. \end{aligned} \tag{15}$$

Similarly, by integrating Equation (7), we have

$$\begin{aligned} \mu_{1\epsilon}(t) &= \beta_1(\delta_1, t) + \textstyle\int_0^t \gamma_1 \circ \underline{\alpha}_2^{-1}(\mu_{2\epsilon}(s))ds + \epsilon(1+t) \\ \mu_{2\epsilon}(t) &= \beta_2(\delta_1, t) + \textstyle\int_0^t \gamma_2 \circ \underline{\alpha}_1^{-1}(\mu_{1\epsilon}(s))ds + \epsilon(1+t). \end{aligned} \tag{16}$$

Define $h(t) \triangleq |\mu_1(t) - \mu_{1\epsilon}(t)| + |\mu_2(t) - \mu_{2\epsilon}(t)|$. Plugging in Equation (15) and (16) into the definition of $h(t)$, we have:

$$\begin{aligned} h(t) \leq\ & 2\epsilon(t+1) + \int_0^t |\gamma_1 \circ \underline{\alpha}_2^{-1}(\mu_{1\epsilon}(s)) - \gamma_1 \circ \underline{\alpha}_2^{-1}(\mu_1(s))|ds \\ & + \int_0^t |\gamma_2 \circ \underline{\alpha}_1^{-1}(\mu_{2\epsilon}(t)) - \gamma_2 \circ \underline{\alpha}_1^{-1}(\mu_2(t))|ds. \end{aligned}$$

From the Lipschitz property of $\gamma_1 \circ \underline{\alpha}_2^{-1}$ and $\gamma_2 \circ \underline{\alpha}_1^{-1}$, we can find a constant $L > 0$ such that $|\gamma_1 \circ \underline{\alpha}_2^{-1}(\mu_{1\epsilon}(s)) - \gamma_1 \circ \underline{\alpha}_2^{-1}(\mu_1(s))| \leq L|\mu_1(t) - \mu_{1\epsilon}(t)|$ and $|\gamma_2 \circ \underline{\alpha}_1^{-1}(\mu_{2\epsilon}(s)) - \gamma_2 \circ \underline{\alpha}_1^{-1}(\mu_2(s))| \leq L|\mu_2(t) - \mu_{2\epsilon}(t)|$. It follows that

$$h(t) \leq 2\epsilon(t+1) + \int_0^t Lh(s)ds.$$

By Gronwall-Bellman inequality [20], it follows that

$$h(t) \leq 2\epsilon(t+1) + 2\epsilon L \int_0^t (s+1)e^{L(t-s)}ds. \tag{17}$$

It follows that for any $t \in \mathbb{R}_{\geq 0}$, the integral $\int_0^t (s+1)e^{L(t-s)}ds$ is bounded. Thus $h(t) \to 0$ as $\epsilon \to 0$, which implies both $|\mu_1(t) - \mu_{1\epsilon}(t)|$ and $|\mu_2(t) - \mu_{2\epsilon}(t)|$ converge to 0. Using Lemma 5.2, and taking the limit of $\epsilon \to 0$, it follows that

$$V_1(\xi_1(t), \xi_1'(t)) \leq \mu_1(t) \text{ and } V_2(\xi_2(t), \xi_2'(t)) \leq \mu_2(t).$$

That is, for any $t \geq 0$, $(\xi(t), \xi'(t)) \in L_V(\mu(t))$. □

Theorem 5.4 states that the reach set of any (large) dynamical system $A = A_1 \| A_2$ from a set of states can be overapproximated by bloating an individual execution ξ of A by a factor that is entirely determined by (a) IS discrepancy functions V_1 and V_2 of its (smaller) subsystems, and (b) the trajectory μ of a (small, 2-dimensional) dynamical system M that is its IS approximation.

Theorem 5.4. *Consider a closed dynamical system $A = A_1 \| A_2$ with IS discrepancy functions $V = (V_1, V_2)$. Let $\xi = Traj(A, \theta)$ for some initial state $\theta \in \Theta_A$. For any nonnegative pair $\delta = (\delta_1, \delta_2)$ suppose μ is the trajectory of the (δ_1, δ_2)-IS approximation M. Then, for any $T \geq 0$*

$$\mathsf{Reach}_A(B_\delta(\theta), T) \subseteq \bigcup_{t \in [0,T]} B^V_{\mu(t)}(\xi(t)).$$

Proof. For any $\mathbf{x} \in \mathsf{Reach}_{\mathcal{A}}(B_\delta(\theta), T)$, there exists an initial state $\theta' \in B_\delta(\theta)$, a trajectory $\xi' = Traj(A, \theta')$ and a time $t \in [0, T]$ such that $\xi'(t) = \mathbf{x}$. It follows Lemma 5.3 that $(\xi(t), \xi'(t)) \in L_V(\mu(t))$, and therefore, $\mathbf{x} \in B^V_{\mu(t)}(\xi(t))$. □

Theorem 5.4 establishes an overapproximation of set of reachable states from a δ-ball $B_\delta(\theta)$. To compute the set of reachable state from a compact initial set Θ_A, we can first compute a δ-cover of Θ_A, and then compute the union of reach set of the covers.

Remark 1. Theorem 5.4 does not require A to be stable or any global property to hold for the IS discrepancy functions.

Remark 2. To use Theorem 5.4 we need to (a) find IS discrepancy functions for the subsystems, and (b) compute individual executions ξ of A and μ of M. Fortunately, for large classes of nonlinear dynamical systems there exist scalable numerical techniques for (b). This is one of the motivations of this work. For linear and some special classes of nonlinear systems (a) can be solved automatically (see Section 4.2).

5.3 Precision of IS Approximation

The precision of this overapproximation is determined by $|\mu(t)|$. In the following, we show that the precision can be made arbitrarily high with sufficiently small but positive δ_1, δ_2.

Lemma 5.5. *Consider any $T > 0$, $t \in [0, T]$, and a sequence of pairs of positive reals $\delta^k = (\delta_1^k, \delta_2^k)$ converging to $(0, 0)$. For the trajectory (μ^k) of the corresponding (δ_1^k, δ_2^k)-IS approximation M^k, $|(\mu^k \downarrow m_i(t)| \to 0$ for $i \in \{1, 2\}$.*

Proof. Fix a $T > 0$ and $\delta^k = (\delta_1^k, \delta_2^k)$. This defines the (δ_1^k, δ_2^k)-IS approximation M^k and its trajectory μ^k. We will prove that for all $t \in [0, T]$,

$$|(\mu^k \downarrow m_1)(t)| + |(\mu^k \downarrow m_2)(t)| \to 0,$$

as $\delta^k \to 0$. Here on we drop the superscript k and use the notations setup earlier: $\mu_i = \mu \downarrow m_i$, etc.

From the first row in Equation (15), we have that

$$|\mu_1(t)| \leq \beta_1(\delta_1, t) + \int_0^t |\gamma_1 \circ \underline{\alpha}_2^{-1}(\mu_2(s))| ds \tag{18}$$

From the Lipschitz property of $\gamma_1 \circ \underline{\alpha}_2^{-1}$, there exists some $L_1 > 0$, such that $|\gamma_1 \circ \underline{\alpha}_2^{-1}(\mu_2(s)) - \gamma_1 \circ \underline{\alpha}_2^{-1}(0)| \leq L|\mu_2(s) - 0|$. Since $\gamma_1 \circ \underline{\alpha}_2^{-1}$ is of class-$\mathcal{K}$, it follows that

$$|\gamma_1 \circ \underline{\alpha}_2^{-1}(\mu_2(s))| \leq L|\mu_2(s)|.$$

From Equation (15), we observe that $i \in \{1, 2\}$ $\mu_i(t)$ are nonnegative scalers. We drop the absolute value symbols $|\cdot|$. Then Equation (18) reduces to

$$|\mu_1(t)| \leq \beta_1(\delta_1, t) + \int_0^t L|\mu_2(s)| ds. \tag{19}$$

Since $\beta_1(\delta_1, t)$ is bounded in compact intervals, define

$$B_1^T(\delta_1) = \sup_{t \in [0,T]} \beta_1(\delta_1, t), \tag{20}$$

as the upper bound of the function $\beta_1(\cdot, t)$ in interval $t \in [0, T]$. It follows from Equation (19) that

$$|\mu_1(t)| \leq B_1^T(\delta_1) + \int_0^t L|\mu_2(s)| ds. \tag{21}$$

Starting from the second row of Equation (15), by following similar steps from Equation (18)-(21), we have:

$$|\mu_2(t)| \leq B_2^T(\delta_2) + \int_0^t L|\mu_1(s)| ds. \tag{22}$$

Summing up Equation (21) and (22), by applying Gronwall-Bellman inequality, we have

$$|\mu_1(t)| + |\mu_2(t)| \leq (B_1^T(\delta_1) + B_2^T(\delta_2)) e^{Lt}.$$

For $i \in \{1, 2\}$, since $\beta_i(\cdot, \cdot)$ is a class-$\mathcal{K}$ function in the first argument, it follows from Equation (20) that $B_i(\delta_i^k) \to 0$ as $\delta_i^k \to 0$. It follows that, $|\mu_1^k(t)| + |\mu_2^k(t)| \to 0$ as $\delta^k \to 0$. □

Proposition 5.6 follows from the fact that for $i \in \{1, 2\}$, for any $\mathbf{x}, \mathbf{x}' \in X_i$, $\underline{\alpha}_i(\mathbf{x} - \mathbf{x}') \leq V_i(\mathbf{x}, \mathbf{x}')$ (Definition 4).

Proposition 5.6. *For dynamical system A with discrepancy function V_1, V_2, fix any $\mathbf{x} \in X_A$. For any $\epsilon > 0$, there exist $r > 0$, such that $B_r^V(\mathbf{x}) \subseteq B_\epsilon(\mathbf{x})$.*

With Lemma 5.5 and Proposition 5.6, the following theorem is straightforward.

Theorem 5.7. *Consider a closed dynamical system $A = A_1 || A_2$ with IS discrepancy $V = \{V_1, V_2\}$. Let $\xi = Traj(A, \theta)$ for some initial state $\theta \in \Theta_A$. For any $\epsilon > 0$, there exists positive pair $\delta_1, \delta_2 > 0$ such that , for A's (δ_1, δ_2)-IS approximation M, for any $T \geq 0$*

$$\bigcup_{t \in [0,T]} B^V_{\mu(t)}(\xi(t)) \subseteq B_\epsilon(\mathsf{Reach}_{\mathcal{A}}(B_\delta(\theta), T)),$$

where μ is the unique trajectory of M.

Remark 3. If the overapproximation obtained from Theorem 5.4 is not precise enough to prove safety, then, we can refine the parameters δ_1 and δ_2. Then we can compute $B^V_{\mu(t)}(\xi(t))$ for each of the smaller partitions with higher precision. This is the approach used for developing Algorithm 1.

5.4 Approximations for $A_1 \| A_2 \| \ldots A_N$

The approximation and its analysis presented in the previous section can be extended to a closed systems with N components: $A = A_1 \| A_2 \ldots \| A_N$. For any trajectories $\xi, \xi' \in Traj(A, \Theta)$, like the notations we used in Section 5.1, for eachl $i \in [N]$, we denfine $\xi_i = \xi \downarrow X_i$ and $\xi_i' = \xi \downarrow X_i$.

The natural generalization of Definition 4 to a set of discrepancy functions according to the composition topology for A is given below:

Definition 7. *A set of input-to-state discrepancy functions of $\mathcal{A}$ is a set of continuous functions $V = \{V_i\}_{i \in [N]}$ with class-$\mathcal{K}$ witnesses $\{(\underline{\alpha}_i, \overline{\alpha}_i, \beta_i)\}_{i \in [N]}$ and $\{\gamma_{ji}\}_{(j,i): X_j \cap U_i \neq \varnothing}$, where for any $\theta, \theta' \in \Theta_A$, , for each $t \geq 0$ each $i \in [N]$*

$$\begin{aligned} V_i(\xi_i(t), \xi_i'(t)) \leq & \beta_i(|\xi_i(0) - \xi_i'(0)|, t) \\ & + \int_0^t \sum_{j: X_j \cap U_i \neq \varnothing} \gamma_{ji}(|\xi_j(s) - \xi_j'(s)|) ds, \end{aligned}$$

where $\xi = Traj(A, \theta)$ and $\xi' = Traj(A, \theta')$.

The set $\{A_j | X_j \cap U_i \neq \varnothing\}$ is the set of modules that provide inputs to module A_i. Similar to Definition 4, Definition 7 requires that each module A_i, is associated with functions V_i and witnesses $(\underline{\alpha}_i, \overline{\alpha}_i, \beta_i)$. Furthermore, each pair (A_j, A_i), where part of A_i's input comes from A_j's state, is

associated with a witness function γ_{ji}. Generalizing Definition 6, the IS approximation of A is a $(N+1)$-dimensional closed deterministic dynamical system M.

Definition 8. *For any $\delta = (\delta_1, \ldots, \delta_N) \in {\mathbb{R}_{\geq 0}}^N$, the δ-IS approximation of A is a closed dynamical system $M = \langle X_M, \Theta_M, U_M, f_M \rangle$, where*

(i) $X_M = \{m_1, m_2, \ldots, m_N, clk\}$,

(ii) $\Theta_M = \{\theta\}$, *where θ is defined by* $\theta(m_i) = \beta_i(\delta_i, 0)$, *for* $i \in [N]$, *and* $\theta(clk) = 0$,

(iii) $\mathcal{U}_{\mathcal{B}} = \varnothing$,

(iv) For any valuation $\mathbf{x} \in Val(X_M)$ *and each* $i \in [N]$:

$$f_M \downarrow m_i(\mathbf{x}) = \dot{\beta}_i(\delta_i, \mathbf{x}(clk)) + \sum_{j: X_j \cap U_i \neq \varnothing} \gamma_{ji} \circ \underline{\alpha}_j^{-1}(\mathbf{x}(m_j)),$$

$$f_M \downarrow clk(\mathbf{x}) = 1.$$

For any state $\mathbf{m} \in Val(X_M)$, the intersection of all sublevel sets of $\{V_i\}_{i \in [N]}$ is denoted as $L_V(\mathbf{m})$ as a generalization of the $A_1 || A_2$ case.

Remark 4. The IS approximation M is $N+1$-dimensional. Construction of M only uses (a) information of individual modules (IS discrepancy functions etc.) and (b) the topology of the composition. No additional information about the behavior of the composed system A is needed.

It follows that for a closed composed system $A = A_1 \| \ldots A_N$ and its IS approximation M, the conclusions of Theorem 5.4 and 5.7 hold with the obvious changes.

6. FROM SIMULATIONS TO PROOFS

In Section 5, from a closed dynamical system A composed of N subsystems and a set of IS discrepancy functions for the subsystems, we constructed an $(N+1)$-dimensional IS approximation M. With Theorem 5.4, by computing trajectories $\xi = Traj(A, \theta)$ of A and a trajectories μ of M, we can compute overapproximations $\mathsf{Reach}_A(B_\delta(\theta), T)$. Computing precise overapproximations of $\mathsf{Reach}_A(\Theta_A, T)$ then reduce to computing finitely many trajectories of A and Ms which can be accomplished using numerical ODE solvers. In this section, we present a safety verification algorithm using this idea.

6.1 Simulations of Dynamical Systems

Given a closed dynamical system A, an initial state θ, let $\xi = \{A, \theta\}$. For a step size $\tau > 0$, validated ODE solvers (such as [7,8,22]) compute a sequence of boxes $R_1, R_2, \ldots, R_l \subseteq Val(X_A)$, such that for each $k \in [l]$, $t \in [(k-1)\tau, k\tau]$, $\xi(t) \in R_k$. For a desired error bound $\epsilon > 0$, by reducing the step size τ, the diameter of R_k can be made smaller then ϵ. We capture such simulation trace in the definition below.

Definition 9. *Given a dynamical system A, an initial state θ, a time bound T, an error bound $\epsilon > 0$, and time step $\tau > 0$, for $\xi = Traj(A, \theta)$, a $(\theta, T, \epsilon, \tau)$-simulation trace is a finite sequence $\phi = (R_0, t_0), (R_1, t_1), \ldots, (R_l, t_l)$ where*

(i) $t_0 = 0$, $t_l = T$, *and* $\forall\ k \in [l]$, $t_i - t_{i-1} \leq \tau$,

(ii) $\forall k \in [l]$ *and* $\forall t \in [t_{k-1}, t_k]$, $\xi(t) \in R_k$, *and*

(iii) $\forall k \in [l]$, $dia(R_k) \leq \epsilon$.

In Algorithm 1 presented in Section 6.2, the subroutine $Simulate(A, \theta, T, \epsilon, \tau)$ (line 6,7) computes a $(\theta, T, \epsilon, \tau)$-simulation as defines in Definition 9. For the completeness of the algorithm, we require that for any precision parameters $\epsilon, \tau > 0$, a simulation trace fulfill such precision can be computed.

6.2 Verification Algorithm

Algorithm 1: Verifying interconnecting systems

```
   input: A, 𝕌, ε0, δ0, T, {V_i, α̲_i, ᾱ_i, β_i, γ_ij}
1  δ ← δ0; ε ← ε0; ℛ ← ∅;
2  𝒞 ← Partition(Θ_𝒜, δ, ε);
3  while 𝒞 ≠ ∅ do
4      for (θ, δ, ε) ∈ 𝒳 do
5          M ← ISApprox(δ, {V_i, α̲_i, ᾱ_i, β_i, γ_ij});
6          ψ ← Simulate(A, θ, T, ε, τ);
7          φ ← Simulate(M, θ_M, T, ε, τ);
8          ρ ← SupByTime(φ);
9          S ← B^V_ρ(ψ);
10         if S ∩ 𝕌 = ∅ then
11             𝒞 ← 𝒞\{(θ, δ, ε)}; ℛ ← ℛ ∪ S ;
12         else if ∃k, B^V_{r_k}(R_k) ⊆ 𝕌 then
13             return (UNSAFE, ℛ)
14         else
15             𝒞 ← 𝒞\{(θ, δ, ε)};
16             𝒞 ← 𝒞 ∪ Partition(Θ ∩ B_δ(θ), (δ_1/2, ..., δ_N/2), ε/2);
17         end
18     end
19 end
20 return (SAFE, ℛ);
```

We introduce Algorithm 1 to verify a closed composed system $A = A_1 \| \ldots \| A_N$. Let each subsystem A_i be equipped with discrepancy functions V_i with witnesses $(\underline{\alpha}_i, \overline{\alpha}_i, \beta_i, \{\gamma_{ji}\})$. The set $\mathcal{C}$ computed in line 2 is a finite set of triples $\{(\theta_c, \delta, \epsilon)\}_{c \in |\mathcal{C}|}$, such that $\{\theta_c\}_{c \in |\mathcal{C}|}$ is a δ-cover of the initial set Θ_A. Each θ_c is associated with precession parameter $\epsilon > 0$ and positive real-valued vector δ. For each triple $(\theta, \delta, \epsilon)$ in the cover set $\mathcal{C}$, an δ-IS approximation M (line 5) is constructed following Definition 8.

The $Simulate()$ (line 6, 7) function is used in two ways:

(i) in computing a simulation trace $\psi = \langle R_0, t_0 \rangle, \ldots, \langle R_p, t_p \rangle$ containing the trajectory $\xi = Traj(A, \theta)$ of the (large) dynamical system A, and

(ii) in computing a simulation trace $\phi = \langle Q_0, t_0 \rangle, \ldots, \langle Q_p, t_p \rangle$ of the trajectory $\mu = Traj(M, \theta_M)$, of the (smaller) IS approximation M.

Here we assume the time stamps of the sequence ψ matches up with that of ϕ. This can be achieved by using a fixed step solver or through resimulating using smaller step sizes. The sequence ρ computed in line 8 is a sequence of the pair $\langle r_0, t_0 \rangle, \ldots, \langle r_p, t_p \rangle$, where for each $k \in [p]$, r_k is a nonnegative real defined as $r_k = \sup_{\mathbf{m} \in Q_k} |\mathbf{m}|$. In line 9, the sequence of sets $\{R_k\}$ is bloated by the sequence of factors $\{r_k\}$ element-wise to construct a tube S. We claim that the tube S contains the set of reachable state of $\mathcal{A}$ from the set of initial state $B_\delta(\theta)$. Then the algorithm checks whether this tube is safe or not, or further refinement is needed.

6.3 Analysis of the Algorithm

We establish the soundness and relative completeness of the algorithm in Theorems 6.3 and 6.4.

Proposition 6.1. *For any* $(\theta, \delta, \epsilon) \in \mathcal{C}$, $\xi \in Traj(A, B_\delta(\theta))$ *and* $t \in [t_{k-1}, t_k]$: $\xi(t) \in B^V_{r_k}(R_k)$.

This follows directly from Theorem 5.4. It also straightforward to check the following invariant of Algorithm 1.

Proposition 6.2. *For compact initial set* Θ_A, *during a run of Algorithm 1,* $\mathcal{C}$ *is finite. And,* $\bigcup_{(\theta,\delta,\epsilon)\in\mathcal{C}} B_\delta(\theta) \supseteq \Theta_A$.

Theorem 6.3. *Algorithm 1 is sound. That is, if it returns* SAFE *then* A *is safe up to* T, *and if it returns* UNSAFE *then* A *is unsafe.*

Proof. Suppose the algorithm returns SAFE. For any cover $(\theta, \delta, \epsilon) \in \mathcal{C}$, S computed in line 9 is the union of a sequence of regions $\{B^V_{r_k}(R_k)\}$. It follows from Proposition 6.1 that $\mathsf{Reach}_A(B_\delta(\theta), T) \subseteq S$. Thus if $S \cap \mathbb{U} = \varnothing$, then $\mathsf{Reach}_A(B_\delta(\theta)) \cap \mathbb{U} = \varnothing$. The algorithm returns SAFE, if all such covers are checked safe. From Proposition 6.2, we conclude $\mathsf{Reach}_A(\Theta_A, T) \cap \mathbb{U} = \varnothing$.

Otherwise if the algorithm returns UNSAFE, there exists at least one set $B^V_{r_k}(R_k)$ contained in the unsafe set $\mathbb{U}$. It follows from Proposition 6.1 that for some trajectory $\xi \in Traj(A, B_\delta(\theta))$ and some $t \in [t_{k-1}, t_k]$, $\xi(t) \in \mathbb{U}$. □

Theorem 6.4. *Algorithm 1 is relatively complete. That is, if* A *is robustly safe then Algorithm 1 terminates and returns* SAFE *and if* A *is unsafe then it terminates and returns* UNSAFE.

Proof. Suppose that for some $\epsilon' > 0$, A is ϵ'-robustly safe up to time T. It follows from Definition 2 that

$$B_{\epsilon'}(\mathsf{Reach}_A(\Theta_A, T)) \cap \mathbb{U} = \varnothing.$$

It follows that line 11 is never executed. For any $\theta \in \Theta$, we will show that for small enough refinement parameters $\delta, \epsilon > 0$, for any k, $dia(B^V_{r_k}(R_k)) < \epsilon'$. From Proposition 5.6, we can show that exists $e > 0$ such that for $r_k < e$,

$$B^V_{r_k}(R_k) \subseteq B_{\epsilon'/3}(R_k). \tag{23}$$

From Lemma 5.5, there exists a *delta* > 0, for all $t \in [0, T]$, $\forall i \in [N]$, $|\mu(t)| \leq e/2$. For a simulation trace $\phi = \langle M_0, t_0\rangle, \ldots, \langle M_q, t_q\rangle$ (line 7), for $\epsilon \leq e/2$, it follows from Definition 9 that for all $k \in [q]$, the diameter $dia(M_k) \leq e/2$. Thus for any $k \in [q]$, $r_k = \sup_{\mathbf{m}\in M_k} |\mathbf{m}| \leq \epsilon + \sup_{t\in[t'_{l-1}, t'_l]} |\mu(t)| \leq e/2 + e/2 = e$. It follows from Equation (23) that by choosing $\delta \leq d$ and $\epsilon \leq e/2$, we have $B^V_{r_k}(R_k) \subseteq B_{\epsilon'/3}(R_k)$. Notice that the diameter of R_k is bounded by the refinement parameter ϵ. By choosing $\epsilon = \min\{\epsilon'/3, e\}$, it follows that

$$dia(B_{\epsilon'/3}(R_k)) \leq \epsilon'/3 + dia(R_k) \leq \epsilon'/3 + \epsilon'/3 < \epsilon'.$$

Thus, after a number of $\max\{\log(\frac{\epsilon_0}{\min\{\epsilon'/3, e\}}), \log\frac{\delta_0}{d}\}$ refinements, the parameters δ, ϵ are small enough to guarantee that $S \cap \mathbb{U} = \varnothing$. Thus the algorithm returns SAFE.

On the other hand, suppose A is unsafe with respect to an open unsafe set $\mathbb{U}$. There exists an initial state θ, a time $t \geq 0$ and a $\epsilon' > 0$ such that $B_{\epsilon'}\xi(\theta, t) \subseteq \mathbb{U}$. For the same number of refinement as the robustly safe case, it can be shown that there exists an $B^V_{r_k}(R_k) \subseteq B_{\epsilon'}\xi(\theta, t)$. It follows that the algorithm returns UNSAFE. □

7. EXPERIMENTAL VALIDATION

We have created a prototype implementation of Algorithm 1 in Matlab using the built-in ODE solvers. Currently, we assume that the error bounds of the computation in line 6-7 are indeed met by the Matlab's ODE solver. To make this step rigorous, in the future, we will use a validated ODE solver like [7, 8, 22].

We verify the safety of several linear and nonlinear models. Each module in the linear synchronization examples (Example 1, see [24] for detail) is a 4-dimensional linear dynamical system and the overall system is composed of several modules in different topologies.

The nonlinear water tank network example is a modified version of the one presented in [9]. In this example, each module captures the fluid levels in a group of tanks, which depends on the flows from other groups of tanks.

The closed loop robotic arm system consists of two modules: a 4-dimensional model of the robotic arm (see [3]), and a 2-dimensional adaptive controller.

We perform several experiments for time bound $T = 20s$ on a Intel i5-3470 CPU. The columns in Table 1 present (i) the system being verified, (ii) the number of total state variables, (iii) the number of modules, (iv) the number of covers for the initial set, (v) the total number of simulation boxes generated, and (vi) the running time of the algorithm. Our experimental results show that the running time roughly scales linearly with the total number of simulation boxes generated for both the original system A and its IS approximation M. The number of simulation boxes generated is proportional to the product of the total number of covers and the time bound. Fixed a compact initial set, the number of covers generated depends on the level of precision needed to prove (or disprove) safety, which depends on the distance between the unsafe set to the reachable states. We also observe that the dimension and non-linearity of the system does not explicitly influence the running time.

System	# V	# N	# C	# sim	RT (s)
Lin. Sync I	12	3	128	42112	115.7
Lin. Sync II	16	4	128	45440	129.2
Lin. Sync III	24	6	128	45649	135.1
Nonli. WT I	10	2	128	45184	127.4
Nonli. WT II	15	3	128	47232	134.9
Nonli. WT III	30	6	128	47232	140.0
Nonli. Rob. I	6	2	64	22592	49.3
Nonli. Rob. II	6	2	216	76248	166.8

Table 1: Experimental results. The columns represent: (1) the system being verified, (2) # state variables, (3) # modules, (4) # covers of initial set, (5) # total simulation boxes, (6) run time.

8. CONCLUSIONS

The technique we present for proving bounded time safety properties of (possibly unstable) nonlinear dynamical systems uses numerical simulations and IS discrepancy functions for the subsystems. IS discrepancy of a subsystem A_i, bounds the distance between two (possibly diverging) trajec-

tories of A_i in terms of their initial states and input signals. It is closely related to the notion of input-to-state stability that is well studied in control theory, but importantly, does not require the subsystems or the overall system to be stable. Consequently, our construction of the low dimensional dynamical system $M(\delta)$ that gives a bound on the divergence of trajectories of A, does not rely on any global properties like small-gain of the interconnection nor stability of A, but instead only uses the individual discrepancy functions and the numerical simulations of A and $M(\delta)$. Further, we also show that by choosing appropriately small δ's the overapproximations can be made arbitrarily precise; and therefore our verification algorithm is sound and relatively complete.

To make this technique practical, we have to develop systematic methods for finding these discrepancy functions for nonlinear models. While there are existing approaches based on static analysis, one alternative direction would be to used simulations themselves to bootstrap the search for discrepancy function [11, 18]. A orthogonal direction is to extend the results to switched or hybrid systems.

9. REFERENCES

[1] D. Angeli. A lyapunov approach to incremental stability properties. *Automatic Control, IEEE Transactions on*, 47(3):410–421, 2002.

[2] D. Angeli. Further results on incremental input-to-state stability. *Automatic Control, IEEE Transactions on*, 54(6):1386–1391, 2009.

[3] D. Angeli, E. D. Sontag, and Y. Wang. A characterization of integral input-to-state stability. *Automatic Control, IEEE Transactions on*, 45(6):1082–1097, 2000.

[4] Y. Annpureddy, C. Liu, G. Fainekos, and S. Sankaranarayanan. *S-taliro: A tool for temporal logic falsification for hybrid systems*. Springer, 2011.

[5] 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*, 44(8):2163–2170, 2008.

[6] P. Benner, J.-R. Li, and T. Penzl. Numerical solution of large-scale lyapunov equations, riccati equations, and linear-quadratic optimal control problems. *Numerical Linear Algebra with Applications*, 15(9):755–777, 2008.

[7] O. Bouissou and M. Martel. Grklib: a guaranteed runge kutta library. In *Scientific Computing, Computer Arithmetic and Validated Numerics, 2006. SCAN 2006. 12th GAMM-IMACS International Symposium on*, pages 8–8. IEEE, 2006.

[8] CAPD. Computer assisted proofs in dynamics, 2002.

[9] X. Chen, E. Abrahám, and S. Sankaranarayanan. Taylor model flowpipe construction for non-linear hybrid systems. In *Real-Time Systems Symposium (RTSS), 2012 IEEE 33rd*, pages 183–192. IEEE, 2012.

[10] A. Donzé. Breach, a toolbox for verification and parameter synthesis of hybrid systems. In *Computer Aided Verification*, pages 167–170. Springer, 2010.

[11] P. Duggirala, S. Mitra, and M. Viswanathan. Verification of annotated models from executions. In *International Conference on Embedded Software*, 2013.

[12] M. Fränzle and C. Herde. Hysat: An efficient proof engine for bounded model checking of hybrid systems. *Formal Methods in System Design*, 30(3):179–198, 2007.

[13] G. Frehse. Phaver: Algorithmic verification of hybrid systems past hytech. In M. Morari and L. Thiele, editors, *HSCC*, volume 3414 of *Lecture Notes in Computer Science*, pages 258–273. Springer, 2005.

[14] G. Frehse, C. L. Guernic, A. Donzé, S. Cotton, R. Ray, O. Lebeltel, R. Ripado, A. Girard, T. Dang, and O. Maler. Spaceex: Scalable verification of hybrid systems. In G. Gopalakrishnan and S. Qadeer, editors, *CAV*, volume 6806 of *Lecture Notes in Computer Science*, pages 379–395. Springer, 2011.

[15] A. Girard, G. Pola, and P. Tabuada. Approximately bisimilar symbolic models for incrementally stable switched systems. *Automatic Control, IEEE Transactions on*, 55(1):116–126, 2010.

[16] Z. Han and P. J. Mosterman. Towards sensitivity analysis of hybrid systems using simulink. In *Proceedings of the 16th international conference on Hybrid systems: computation and control*, pages 95–100. ACM, 2013.

[17] Z. Huang. On simulation based verification of nonlinear nondeterministic hybrid systems. 2013.

[18] Z. Huang and S. Mitra. Computing bounded reach sets from sampled simulation traces. In *The 15th International Conference on Hybrid Systems: Computation and Control (HSCC 2012), Beijing, China.*, 2012.

[19] D. K. Kaynar, N. Lynch, R. Segala, and F. Vaandrager. *The Theory of Timed I/O Automata*. Synthesis Lectures on Computer Science. Morgan Claypool, November 2005. Also available as Technical Report MIT-LCS-TR-917.

[20] H. K. Khalil. *Nonlinear Systems*. Prentice Hall, third edition, 1992.

[21] S. Mitra. *A Verification Framework for Hybrid Systems*. PhD thesis, Massachusetts Institute of Technology, Cambridge, MA 02139, September 2007.

[22] N. S. Nedialkov, K. R. Jackson, and G. F. Corliss. Validated solutions of initial value problems for ordinary differential equations. *Applied Mathematics and Computation*, 105(1):21–68, 1999.

[23] G. Pola, A. Girard, and P. Tabuada. Approximately bisimilar symbolic models for nonlinear control systems. *Automatica*, 44(10):2508–2516, 2008.

[24] L. Scardovi and R. Sepulchre. Synchronization in networks of identical linear systems. *Automatica*, 45(11):2557–2562, 2009.

[25] E. D. Sontag. Comments on integral variants of iss. *Systems & Control Letters*, 34(1-2):93 – 100, 1998.

[26] P. Tabuada, A. D. Ames, A. Julius, and G. J. Pappas. Approximate reduction of dynamic systems. *Systems & Control Letters*, 57(7):538–545, 2008.

[27] G. Wood and B. Zhang. Estimation of the lipschitz constant of a function. *Journal of Global Optimization*, 8(1):91–103, 1996.