ARTICLE IN PRESS

Nonlinear Analysis: Hybrid Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Nonlinear Analysis: Hybrid Systems

journal homepage: www.elsevier.com/locate/nahs

Bounded invariant verification for time-delayed nonlinear networked dynamical systems

Zhenqi Huang *, Chuchu Fan, Sayan Mitra

Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, United States

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Compositional verification
Delayed dynamical systems
Simulation-based verification
Input-to-state stability

ABSTRACT

We present a technique for bounded invariant verification of nonlinear networked dynamical systems with delayed interconnections. The underlying problem in precise bounded-time verification lies with computing bounds on the sensitivity of trajectories (or solutions) to changes in initial states and inputs of the system. For large networks, computing this sensitivity with precision guarantees is challenging. We introduce the notion of input-to-state (IS) discrepancy of each module or subsystem in a larger nonlinear networked dynamical system. The IS discrepancy bounds the distance between two solutions or trajectories of a module in terms of their initial states and their inputs. Given the IS discrepancy functions of the modules, we show that it is possible to effectively construct a reduced (low dimensional) time-delayed dynamical system, such that the trajectory of this reduced model precisely bounds the distance between the trajectories of the complete network with changed initial states. Using the above results we develop a sound and relatively complete algorithm for bounded invariant verification of networked dynamical systems consisting of nonlinear modules interacting through possibly delayed signals. Finally, we introduce a local version of IS discrepancy and show that it is possible to compute them using only the Lipschitz constant and the Jacobian of the dynamic function of the modules.

Published by Elsevier Ltd.

1. Introduction

Numerical simulations are extensively used for analyzing nonlinear dynamical systems, yet for models with uncertainty in initial states, parameters and inputs, finite number of simulations alone cannot give proofs for invariant properties. Several recent papers [1–5] present simulation-based techniques for proving or disproving properties of such models. The details vary to some extent, but the common theme is to combine finite number of numerical simulations with symbolic static analysis to compute over-approximations of the infinitely many behaviors of the system that may arise from these uncertainties. In other words, the knowledge obtained from the static analysis is used to cover infinitely many behaviors of the system from finite simulation data.

For a dynamical system $\dot{\mathbf{x}} = f(\mathbf{x})$ and a particular initial state $\mathbf{x}$, let $\xi_{\mathbf{x}}$ be the numerically computed trajectory from $\mathbf{x}$ for a certain time bound T. From the continuous dependence of $\xi_{\mathbf{x}}$ on $\mathbf{x}$, we know that all the trajectories from a neighborhood of $\mathbf{x}$ will be close to $\xi_{\mathbf{x}}$. With more information about the sensitivity of the trajectories to the initial state we get better quantitative bounds on the distance between neighboring trajectories. This enables us to compute a tube around $\xi_{\mathbf{x}}$, that

* Corresponding author. Tel.: +1 2175502866.
E-mail addresses: zhuang25@illinois.edu (Z. Huang), cfan10@illinois.edu (C. Fan), mitras@illinois.edu (S. Mitra).

http://dx.doi.org/10.1016/j.nahs.2016.05.005
1751-570X/Published by Elsevier Ltd.

contains all possible trajectories from the neighborhood of $\mathbf{x}$. The precision or the conservativeness of this bound impacts the quality of the over-approximation, and therefore, the performance of verification with the above strategy.

For example, the Lipschitz constant of the dynamic function f gives a bound on the distance between the neighboring trajectories that grows exponentially with time. Although checking Lipschitz continuity is generally undecidable, for certain classes of functions Lipschitz constants can be inferred from elementary functions [6]. Stronger notions like sensitivity [1,7], incremental Lyapunov functions [8], and contraction metrics for dynamical system are used in [9] to obtain more practically useful bounds.

Generalizing several of these properties, in [3] the authors introduced the notion of *discrepancy function* as a continuous function (of the distance between initial states and time) characterizing the convergence or divergence rates of trajectories. It was shown that if a nonlinear, switched, or hybrid system model is annotated with appropriate discrepancy function(s) then the above approach gives a sound and relatively complete algorithm for verifying bounded time invariants.

Until recently, there were 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. Finding these annotations becomes increasingly difficult for larger models in which many components interact [10].

In this paper, we address this problem by proposing a compositional approach for automatically computing discrepancy functions for dynamical systems that are created by composing many modules that interact over a (possibly delayed) network. Consider a networked dynamical system $\mathcal{A}$ consisting of several interacting subsystems or modules $\mathcal{A}_1, \ldots, \mathcal{A}_N$. That is, the input signals of a subsystem $\mathcal{A}_i$ are driven by the outputs (or states) of some set of other components. Let us say that each $\mathcal{A}_i$ is n-dimensional which makes $\mathcal{A}$ nN-dimensional. Our solution has several parts. First, building up on our previous work [4,5] we introduce a new type of input-to-state discrepancy function (IS discrepancy) for each subsystem $\mathcal{A}_i$. An IS discrepancy for $\mathcal{A}_i$ (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. Using IS discrepancy of the modules we syntactically construct a reduced N-dimensional dynamical system M. If the interconnections in the original network $\mathcal{A}$ have delays then so do the interconnections in the reduced network. We show that the trajectories of M give a discrepancy function for $\mathcal{A}$. We adopt the technique of [11] to this compositional setting for computing a local version of IS discrepancy that uses only the Lipschitz constants and the Jacobian matrices of the modules. This approach of [11] bounds the distance between two trajectories as an exponential function of the eigenvalues of the Jacobian matrix.

Input-to-state stability (ISS), its variants and characterization in terms of necessary and sufficient conditions have been one of the major advances of nonlinear control theory in the last two decades [12–14]. Incremental ISS has been used to construct discrete symbolic models that approximately bisimulate continuous systems [15,16]. Under additional assumptions about the stability of the overall system, such as a small-gain condition, it has been shown that a large system can be reduced to a smaller system with similar behaviors [17,18]. 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.

There has been recent work on verification of delayed differential equations (see, for example, [19] and the references therein). The algorithm in [19] iteratively computes validated simulations of delayed differential equations as sequences of Taylor over-approximations of time intervals, and verifies safety property using SMT solvers. Part of its technique can be used in our approach as a mean for computing validated numerical simulations for delayed differential equations. Our approach, in addition, involves systematically generating numerical simulations to refine reach sets and dynamically reasoning about sensitivity of interconnecting networks.

Summary of contributions: (i) We introduce a method for constructing an approximation of a networked dynamical system with time delay ($\mathcal{A}$) 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. This approach for delayed networks extends our result for delay-free networks [4]. The extension involves generalizing the model of networked dynamical systems to cover interconnections with delays, which leads to delayed differential equations, and the construction of the corresponding delayed reduced system.

(ii) We show that $M(\delta)$ has a unique trajectory μ, and that any trajectory $\xi_{\mathbf{x}}$ of $\mathcal{A}$ point-wise bloated by the value of $\mu(t)$ contains the reach set of all the trajectories of $\mathcal{A}$ starting from a δ-ball around $\mathbf{x}$ (Theorem 7). Thus, by simulating $\mathcal{A}$ and (the smaller) $M(\delta)$ we can compute bounded-time reach set over-approximations of $\mathcal{A}$.

(iii) We also show that by choosing appropriately small δ's the over-approximations computed by the above method can be made arbitrarily precise; modulo the precision of the numerical simulations (Theorem 10).

(iv) We give an algorithm for computing a local version of IS discrepancy function along a trajectory $\xi_{\mathbf{x}}$ of $\mathcal{A}$ using only the Lipschitz constant and Jacobian matrix of the dynamic mapping of each module.

(v) 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 experiments with a prototype implementation of the algorithm show that the approach achieves best performance when verifying networks of stable modules with light inter-modular couplings.