Safe Over- and Under-Approximation of Reachable Sets for Delay Differential Equations

Bai Xue[1], Peter N. Mosaad[1], Martin Fränzle[1], Mingshuai Chen[2,3], Yangjia Li[2], and Naijun Zhan[2,3]

[1] Dpt. of Computing Science, C. v. Ossietzky Universität Oldenburg, Germany
{bai.xue|peter.nazier.mosaad|fraenzle}@informatik.uni-oldenburg.de,
[2] State Key Lab. of Computer Science, Institute of Software, CAS, China
[3] University of Chinese Academy of Science, China
{chenms|yangjia|znj}@ios.ac.cn

Abstract. Delays in feedback control loop, as induced by networked distributed control schemes, may have detrimental effects on control performance. This induces an interest in safety verification of delay differential equations (DDEs) used as a model of embedded control. This article explores reachable-set computation for a class of DDEs featuring a local homeomorphism property. This topological property facilitates construction of over- and under-approximations of their full reachable sets by performing reachability analysis on the boundaries of their initial sets, thereby permitting an efficient lifting of reach-set computation methods for ODEs to DDEs. Membership in this class of DDEs is determined by conducting sensitivity analysis of the solution mapping with respect to the initial states to impose a bound constraint on the time-lag term. We then generalize boundary-based reachability analysis to such DDEs. Our reachability algorithm is iterative along the time axis and the computations in each iteration are performed in two steps. The first step computes an enclosure of the set of states reachable from the boundary of the step's initial state set. The second step derives an over- and under-approximations of the full reachable set by including (excluding, resp.) the obtained boundary enclosure from certain convex combinations of points in that boundary enclosure. Experiments on two illustrative examples demonstrate the efficacy of our algorithm.

1 Introduction

The rapidly increasing deployment of cyber-physical systems into diverse safety-critical application domains ranging from, among others transportation systems over chemical processes to health-care renders safety analysis and verification for these systems societally important. Formally, the safety verification problem can often be reduced to a problem of deciding whether the system of interest may in its evolution touch a specified set of unsafe states [22, 24, 29]. Reachability analysis, which involves computing appropriate approximations of the reachable state sets, plays a fundamental role in addressing such safety verification challenges. It usually employs either over-approximations (i.e., super-sets of the actual reach set) to determine whether a system starting from legal initial states satisfies some specified safety properties, or under-approximations (i.e.,

sub-sets [12]) to detect falsification of safety properties by finding counterexamples[4]. The use of such approximations instead of exact reach sets is justified by the fact that the exact sets are generally not computable.

Ordinary differential equations (ODEs) are traditionally used for describing system dynamics within continuous or hybrid-state feedback control loops. Consequently, significant research has been invested in reachability analysis of such dynamical systems. For the problem of computing over-approximations, significant advances have continuously been reported in the literature over the last decades (e.g., [20, 25, 21, 9, 19, 6, 11, 18]). For computing under-approximation, methods have initially focused on linear systems (e.g., [17, 14]), but recently, approaches have been proposed to also tackle nonlinear systems (e.g., [28, 15, 12, 8, 30]).

ODEs are, however, an idealized model of the feedback dynamics in control systems. Simply conjoining the ODEs describing the plant dynamics with the ODEs describing control laws may be misleading, as any delay introduced into the feedback loop may induce significantly deviating dynamics. In practice, delays are involved in sensing or actuating by physical devices, in data forwarding to or from the controller, in signal processing in the controller, etc. An appropriate generalization of ODE able to model the delay within the framework of differential equations is delay differential equations (DDEs), as originally suggested by Bellman and Cooke for modeling physical, biological, and chemical processes involving delayed dynamics [4].

DDEs are a class of differential equations where the time derivatives at the current time depend on the solution and possibly its derivatives at previous times as well. The presence of delayed dynamics may invalidate any stability and safety certificate obtained on the related delay-free model, as delays may significantly alter the overall shape of the system dynamics. This situation is illustrated through the following simple example from [16] where arbitrarily small delays have significant effect on state dynamics: the solution of the ODE

$$\dot{x}(t) + 2\dot{x}(t) = -x(t) \tag{1}$$

is asymptotically stable, converging to the equilibrium point $x = 0$ from any initial state. However, the solution of its corresponding DDE

$$\dot{x}(t) + 2\dot{x}(t-\tau) = -x(t) \tag{2}$$

is unstable for any positive delay τ. Therefore, taking time-delay terms into account to either verify or falsify properties of systems by performing reachability analysis is not just desirable, but ought to be imperative for systems that are more accurately modelled by DDEs, especially in safety-critical applications.

The problem of computing over- and/or under-approximations for the reachable sets of DDEs obviously is more challenging than for the proper sub-class of ODEs. Recently, a set-boundary based reachability analysis method being capable of generating over- and under-approximations of reach sets of ODEs was proposed in [30, 29] making use of the homeomorphism property of the ODE's solution mapping. A homeomorphism is a bijection ψ from a topological space X to a topological space Y with the

[4] If the under-approximation intersects a given unsafe set, there is definitely at least one of the trajectories entering the unsafe set, i.e., the system is definitely unsafe.

property that the pre-image $\psi^{-1}(P)$ is an open subset in X if and only if P is an open subset in Y. An important property induced by a homeomorphism from X to Y is that the homeomorphism maps the boundary and interior points of Q onto the boundary and interior points of $\psi(Q)$, respectively. In this vein, the solution mapping to initial value problems (IVP) featuring unique solutions is a homeomorphism between the space of initial values and that of values reached by the solution trajectory at any given time $t \geq 0$. Based on the observation that the DDE will converge to an ODE when the time-lag term tends to zero, this motivates us to explore a class of DDEs with solutions featuring a similar homeomorphism property and to generalize the aforementioned set-boundary based reachability analysis method accordingly.

Membership of a given DDE in the class of DDEs exhibiting the necessary homeomorphism property is determined by conducting a sensitivity analysis on the solution mapping. This sensitivity analysis imposes a bound on the time-lag term as the properties of the solution change when time-lag exceeds certain bounds like the stability border. In an engineering process, this upper bound on time-lag can be considered as an automatically derived design space constraint, asking the development engineers for selection of appropriate components (sensors, processors, actuators, communication networks) guaranteeing sufficiently low latency in the feedback loop.

The main contributions of this paper is the generalization of the set-boundary reachability analysis based method for ODEs to DDEs exposing the necessary homeomorphism property, as detected by the sensitivity analysis. The reachability algorithm is iterative along the time axis and the computations in each iteration are performed in two steps. First step computes an enclosure of the set of states reachable from the boundary of the step's initial state set. Second step derives an over- and under-approximations of the full reachable set by including (excluding, resp.) the obtained boundary enclosure from certain convex combinations of points in this boundary enclosure. We demonstrate the efficacy of our algorithm on two illustrative examples.

Related Work

As mentioned above, the reachability analysis to dynamic systems modeled by delay differential equations (DDEs), especially for computing under-approximations, is in its infancy and thus provides an open area of research.

Zou, Fränzle et al. proposed in [31] a safe enclosure method using interval-based Taylor over-approximation to enclose a set of functions by a parametric Taylor series with parameters in interval form. To avoid dimension explosion incurred by the ever-growing degree of the Taylor-series along the time axis, the method depends on fixing the degree for the Taylor series and moving higher-degree terms into the parametric uncertainty permitted by the interval form of the Taylor coefficients, thereby being able to provide analysis of time-unbounded solutions to DDE. In [23], Prajna et al. extended the barrier certificate methodology for ODEs to the polynomial time-delay differential equations setting, in which the safety verification problem is formulated as a problem of solving sum-of-square programs. The work in [13] presents a technique for simulation-based time-bounded invariant verification of nonlinear networked dynamical systems with delayed interconnections by computing bounds on the sensitivity of trajectories (or solutions) to changes in initial states and inputs of the system. A similar simula-

tion method integrating error analysis of the numeric solving and the sensitivity-related state bloating algorithms was proposed in [7] to obtain safe enclosures of time-bounded reach sets for systems modelled by DDEs. In the aforementioned work, however, the authors focused on over-approximating reachable sets for systems modelled by DDEs with finite or infinite time horizon, not touching on the problem of under-approximation methods of reachable sets for DDEs as needed in system falsification.

In this paper, we infer a class of DDEs with solution mappings featuring an appropriate homeomorphism property with respect to initial states, where membership in the class can be determined by sensitivity analysis. For such a DDE, the boundary of the reachable set is maintained under dynamic evolution, thereby enabling us to construct over- and under-approximations of reachable sets by extending the set-boundary based reachability analysis method for ODEs from [30, 29].

Outline. We formulate the reachability problem of interest and give a brief introduction into nonlinear control systems in Section 2. In Section 3.3, we expose a class of delay differential equations featuring a desirable homeomorphism property for its solutions and present our boundary-based reachability analysis algorithm for computing over- and under-approximations of reachable sets respectively. Then we illustrate our approach on two examples as well as discuss its impact in Section 4. Finally, we conclude our paper in Section 5.

2 Preliminaries

In this section, we formally define the dynamical systems of interest and recall the basic notion of reachability used throughout this paper. The following conventions will be used in the remainder of this paper: the space of continuously differentiable functions on $\mathcal{X}$ is denoted by $\mathcal{C}^1(\mathcal{X})$; for a set Δ, the decorations Δ°, Δ^c and $\partial\Delta$ represent its interior, complement, and boundary respectively; vectors in the $\mathbb{R}^n$ as well as of functions are denoted by boldface letters. The set of $n \times n$ matrices over the field $\mathbb{R}$ of real numbers is denoted by $\mathbb{R}^{n\times n}$.

In this paper we consider systems that can be modelled by delay differential equations (DDEs) of the form

$$\dot{\boldsymbol{x}} = \begin{cases} \boldsymbol{g}(\boldsymbol{x}), & \text{if } t \in [0,\tau), \boldsymbol{x}(0) \in \mathcal{I}_0 \\ \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{x}_\tau), & \text{if } t \in [\tau, K\tau], \end{cases} \tag{3}$$

where $\boldsymbol{x}(t) = (x_1(t), x_2(t), \ldots, x_n(t))^{'} \in \mathcal{X}$, $\boldsymbol{x}_\tau = (x_1(t-\tau), x_2(t-\tau), \ldots, x_n(t-\tau))^{'} \in \mathcal{X}$, $\mathcal{X} \subseteq \mathbb{R}^n$, $K \geq 2$ is a positive integer, $\boldsymbol{g} : \mathcal{X} \mapsto \mathbb{R}^n$ describes the process which the initial function is determined by the initial value $\boldsymbol{x}(0) \in \mathcal{I}_0$, and $\mathcal{I}_0 \subset \mathbb{R}^n$ is a simply connected compact set and $\boldsymbol{f} : \mathcal{X} \times \mathcal{X} \mapsto \mathbb{R}^n$ is globally Lipschitz continuous over the variables $\boldsymbol{x}(t)$ and $\boldsymbol{x}(t-\tau)$. Also, we require that $\boldsymbol{g}(\boldsymbol{x}) \in \mathcal{C}^1(\mathcal{X})$ and $\boldsymbol{g} : \mathcal{X} \mapsto \mathbb{R}^n$ satisfies the Lipschitz continuity condition w.r.t. the variables $\boldsymbol{x}(t)$, guaranteeing that $\dot{\boldsymbol{x}} = \boldsymbol{g}(\boldsymbol{x})$ with initial value $\boldsymbol{x}(0) = \boldsymbol{x}_0 \in \mathcal{I}_0$ has a unique solution on $[0, \tau]$. Therefore, Eq.(3) describes a deterministic process on $[0, K\tau]$. Besides, we assume that max norms $\|\frac{\partial \boldsymbol{f}(\boldsymbol{x},\boldsymbol{y})}{\partial \boldsymbol{x}}\|_{max}$ and $\|\frac{\partial \boldsymbol{f}(\boldsymbol{x},\boldsymbol{y})}{\partial \boldsymbol{y}}\|_{max}$ of the matrices $\|\frac{\partial \boldsymbol{f}(\boldsymbol{x},\boldsymbol{y})}{\partial \boldsymbol{x}}\|$

and $\|\frac{\partial \boldsymbol{f}(\boldsymbol{x},\boldsymbol{y})}{\partial \boldsymbol{y}}\|$ are uniformly bounded for any combination of $\boldsymbol{x} \in \mathcal{X}$ and $\boldsymbol{y} \in \mathcal{X}$, i.e.,

$$\frac{\partial \boldsymbol{f}(\boldsymbol{x},\boldsymbol{y})}{\partial \boldsymbol{x}}\|_{max} \leq M, \|\frac{\partial \boldsymbol{f}(\boldsymbol{x},\boldsymbol{y})}{\partial \boldsymbol{y}}\|_{max} \leq N, \tag{4}$$

where M and N are positive real numbers.

Given System (3) with an initial set $\mathcal{I}_0$, and a finite time duration t, where $0 \leq t \leq K\tau$ and $K \geq 2$ is a positive integer, the set of allowable initial functions selected by $\boldsymbol{g}(\boldsymbol{x})$ is just a set of solutions of the ordinary differential equation (ODE) $\dot{\boldsymbol{x}} = \boldsymbol{g}(\boldsymbol{x})$ initialised in $\mathcal{I}_0$ w.r.t. the time interval $[0, \tau]$. The trajectory of System (3) is defined to be $\boldsymbol{\phi}(t; \boldsymbol{x}_0) = \boldsymbol{x}(t)$, where $\boldsymbol{x}(t)$ is the solution of System (3) that satisfies the initial condition $\boldsymbol{x}(0) = \boldsymbol{x}_0$ at time instant $t = 0$. In addition, we define the reachable set of a given initial set $\mathcal{I}_0$ for any time $t \geq 0$ and its corresponding over- and under-approximations as follows.

Definition 1. *The reachable set $\Omega(t; \mathcal{I}_0)$ at time $t \geq 0$ is a set of states visited by trajectories originating from $\mathcal{I}_0$ at time $t = 0$ after time duration t, i.e.*

$$\Omega(t; \mathcal{I}_0) = \{\boldsymbol{x} : \boldsymbol{x} = \boldsymbol{\phi}(t; \boldsymbol{x}_0), \boldsymbol{x}_0 \in \mathcal{I}_0\}.$$

Definition 2. *An over-approximation of the reachable set $\Omega(t; \mathcal{I}_0)$ is a set $O(t; \mathcal{I}_0)$, where $\Omega(t; \mathcal{I}_0) \subseteq O(t; \mathcal{I}_0)$. In contrast, an under-approximation $U(t; \mathcal{I}_0)$ of the reachable set is a nonempty subset of the reachable set $\Omega(t; \mathcal{I}_0)$.*

Notice that from Definition 2, the over-approximation $O(t; \mathcal{I}_0)$ is an enclosure s.t. $\forall \boldsymbol{x}_0 \in \mathcal{I}_0 : \boldsymbol{\phi}(t; \boldsymbol{x}_0) \in O(t; \mathcal{I}_0)$ holds, where $0 \leq t \leq K\tau$. On the other hand, the under-approximation $U(t; \mathcal{I}_0)$ is a nonempty set s.t. $\forall \boldsymbol{x}(t) \in U(t; \mathcal{I}_0) : \exists \boldsymbol{x}_0 \in \mathcal{I}_0 : \boldsymbol{x}(t) = \boldsymbol{\phi}(t; \boldsymbol{x}_0)$.

Aiming at computing over- as well as under-approximations, we wish to extend the set-boundary based reachability method for ODEs from [30] to DDEs. This method relies on the fact that the solution mapping is a homeomorphism and thus preserves set boundaries, permitting to retrieve safe over- and under-approximations from enclosures of the dynamic images of the boundaries of the initial set. The solution mappings of DDEs in the form of Eq.(3), however, need not be homeomorphisms. Hence, we devote ourselves to exposing a class of systems of the form (3) with solution mappings having that desirable property. We study, in this paper, the following problems:

Problem 1. Which class of systems characterized by Eq. (3) has solution mappings forming a homeomorphism?

Problem 2. How can we efficiently compute over- and under-approximations of the reachable set for the systems described in **Problem 1** if the initial set $\mathcal{I}_0$ is a simply connected compact set?

2.1 Nonlinear Control Systems

Nonlinear control systems are characterized by the presence of nonlinear elements in the right-hand side of the characterizing differential equation. Such non-linearities may

stem from both the system under control (i.e., the plant) and the controller itself. Ordinary differential equations (ODEs) are traditionally used to model the continuous behaviour of such systems. In general, the nonlinear control systems that are modelled by ODEs with a control input are of the following form

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{h}(\boldsymbol{x}(t), \boldsymbol{u}(t)), \tag{5}$$

where $\boldsymbol{x}(0) \in \mathcal{X}_0 \subseteq \mathbb{R}^n$, $\boldsymbol{u}(t) \in \boldsymbol{U} \subseteq \mathbb{R}^m$, and $\mathcal{X}_0$, $\boldsymbol{U}$ are both compact sets. The equation (5) is required to be (globally) Lipschitz-continuous and the input trajectory $\boldsymbol{u}(\cdot) : \mathbb{R}^+ \mapsto \boldsymbol{U}$ is required to be piecewise continuous so that a solution is guaranteed to exist globally in the sense for all $t \geq 0$. For convenience, we denote the space of piecewise continuous functions from $\mathbb{R}^+$ to $\boldsymbol{U}$ as $\mathcal{P}$.

Let us denote the solution to System (5) for a given initial state and an input trajectory by $\chi(t; \boldsymbol{x}_0, \boldsymbol{u}(\cdot))$, where $t \geq 0$, $\boldsymbol{x}(0) = \boldsymbol{x}_0 \in \mathcal{X}_0$ and $\boldsymbol{u}(\cdot) \in \boldsymbol{U}$ is the input trajectory within the time interval $[0, t]$. The reachable set at time $t = r$ can be defined for a set of initial states $\mathcal{X}_0$ and a set of input values $\boldsymbol{U}$ as

$$\mathcal{R}(r) = \{\chi(r; \boldsymbol{x}_0, \boldsymbol{u}) \in \mathbb{R}^n | \boldsymbol{x}_0 \in \mathcal{X}_0, \boldsymbol{u} \in \mathcal{P}\}.$$

Althoff's approaches [3, 1] are among the many methods for computation of over-approximations of the reachable set $\mathcal{R}(r)$. Such methods can also be applied to over-approximating the reachable set for cases involving DDEs of the form (3) by regarding the delay term $\boldsymbol{x}_\tau$ as the time-varying uncertainty $\boldsymbol{u}$ (cf. [13] for such an algorithm).

3 Reachable Sets Computation

This section mainly focuses on solving **Problem 1** and **Problem 2** as presented in Section 2. Firstly, we address **Problem 1** by conducting sensitivity analysis on the solution mappings $\boldsymbol{\phi}(t; \cdot)$ w.r.t. the initial states for DDEs of the form of Eq. (3). This facilitates imposition of a bound constraint on the time-lag term such that the homeomorphism property is guaranteed. Then, addressing **Problem 2**, we generalize the set-boundary based method for reachability analysis of [29, 30] to the computation of safe approximations of reach sets for systems of the form (3). This way, we can construct over- and under-approximations of their reachable sets.

3.1 Sensitivity Analysis Theory

For a system governed by the ODE

$$\dot{\boldsymbol{x}} = \boldsymbol{g}(\boldsymbol{x}),$$

where $t \in [0, \tau]$, its flow mapping $\boldsymbol{\phi}(t; \boldsymbol{x}_0)$ as a function of $\boldsymbol{x}_0$ is differentiable w.r.t. the initial state $\boldsymbol{x}_0$, if $\boldsymbol{g} \in \mathcal{C}^1(\mathcal{X})$ and $\boldsymbol{g}$ is Lipschitz continuous. The sensitivity of solutions at time $t \in [0, \tau]$ to initial conditions is defined by

$$s_{\boldsymbol{x}_0}(t) = \frac{\partial \boldsymbol{\phi}(t; \boldsymbol{x}_0)}{\partial \boldsymbol{x}_0}, \tag{6}$$

where $s_{\boldsymbol{x}_0}(t)$ is a square matrix of order n. The $(i,j)_{th}$ element of $s_{\boldsymbol{x}_0}$ basically represents the influence of variations in the i_{th} coordinate $x_{0,i}$ of $\boldsymbol{x}_0$ on the j_{th} coordinate $x_j(t)$ of $\boldsymbol{\phi}(t;\boldsymbol{x}_0)$. To compute the sensitivity matrix, we first apply the chain rule to get the derivative of $s_{\boldsymbol{x}_0}$ w.r.t. time [10], as follows:

$$\frac{d}{dt}\frac{\partial \boldsymbol{\phi}(t;\boldsymbol{x}_0)}{\partial \boldsymbol{x}_0} = D_{\boldsymbol{g}}(\boldsymbol{\phi}(t;\boldsymbol{x}_0))\frac{\partial \boldsymbol{\phi}(t;\boldsymbol{x}_0)}{\partial \boldsymbol{x}_0},$$

which yields the ODE

$$\dot{s}_{\boldsymbol{x}_0} = D_{\boldsymbol{g}} s_{\boldsymbol{x}_0}$$

describing evolution of sensitivity over time, where $D_{\boldsymbol{g}}$ is the Jacobian matrix of vector field $\boldsymbol{g}$ along the trajectory $\boldsymbol{\phi}(t;\boldsymbol{x}_0)$. This equation is a linear time-varying ODE and the relevant initial value $s_{\boldsymbol{x}_0}(0)$ is the identity matrix $\boldsymbol{I} \in \mathbb{R}^{n\times n}$.

Remark 1. From the definition of the sensitivity matrix $s_{\boldsymbol{x}_0}(t)$, we observe that $s_{\boldsymbol{x}_0}(t)$ is also the Jacobian matrix of the mapping $\boldsymbol{\phi}(t;\cdot) : \mathcal{I}_0 \mapsto \Omega(t;\mathcal{I}_0)$, where $t \in [0,\tau]$.

Lemma 1. *There exists a $\tau^* > 0$ such that the determinant of sensitivity matrix $s_{\boldsymbol{x}_0}(t)$ in Eq. (6) is different from zero for any $t \in [0,\tau^*]$.*

For the proof of Lemma 1, please refer to the Appendix. Assume that the solution mapping $\boldsymbol{\phi}(t;\boldsymbol{x}_0)$ of System (3) for time ranging over $t \in [(k-1)\tau, k\tau]$ and the state variable $\boldsymbol{x}_0 \in \mathcal{I}_0$, could be equivalently reformulated as a continuously differentiable function of the state variable $\boldsymbol{x}((k-1)\tau)$ in $\Omega((k-1)\tau;\mathcal{I}_0)$ and the time variable $t \in [(k-1)\tau, k\tau]$, i.e.,

$$\boldsymbol{\phi}(t;\boldsymbol{x}_0) = \boldsymbol{\psi}_{k-1}(t;\boldsymbol{x}((k-1)\tau),(k-1)\tau),$$

where $k \in \{1,\ldots,K-1\}$, and $\boldsymbol{x}((k-1)\tau) = \boldsymbol{\phi}((k-1)\tau;\boldsymbol{x}_0)$. Also assume the determinant of the Jacobian matrix of the mapping $\boldsymbol{\psi}_{k-1}(t;\boldsymbol{x}((k-1)\tau),(k-1)\tau)$ w.r.t. any state $\boldsymbol{x}((k-1)\tau) \in \Omega((k-1)\tau;\mathcal{I}_0)$ is not zero for any $t \in [(k-1)\tau, k\tau]$. Then, we deduce what follows. For its proof, please refer to the Appendix.

Lemma 2. *Given the above assumptions, the sensitivity matrix $s_{\boldsymbol{x}(k\tau)}(t) = \frac{\partial \boldsymbol{x}(t)}{\partial \boldsymbol{x}(k\tau)}$, $t \in [k\tau,(k+1)\tau]$, for System (3) satisfies the following linear time-varying ODE:*

$$\dot{s}_{\boldsymbol{x}(k\tau)} = \frac{\partial \boldsymbol{f}(\boldsymbol{x},\boldsymbol{x}_\tau)}{\partial \boldsymbol{x}} s_{\boldsymbol{x}(k\tau)} + \frac{\partial \boldsymbol{f}(\boldsymbol{x},\boldsymbol{x}_\tau)}{\partial \boldsymbol{x}_\tau}\frac{\partial \boldsymbol{x}_\tau}{\partial \boldsymbol{x}(k\tau)}, \tag{7}$$

where $\dot{s}_{\boldsymbol{x}(k\tau)} = \frac{ds_{\boldsymbol{x}(k\tau)}}{dt}$, and $s_{\boldsymbol{x}(k\tau)}(k\tau) = \boldsymbol{I} \in \mathbb{R}^{n\times n}$.

From the definition of the sensitivity matrix $s_{\boldsymbol{x}(k\tau)}(t) = \frac{\partial \boldsymbol{x}(t)}{\partial \boldsymbol{x}(k\tau)}$ together with the fact that its determinant is not equal to zero, the solution mapping $\boldsymbol{\phi}(t;\ \cdot) : \mathcal{I}_0 \mapsto \Omega(t;\mathcal{I}_0)$ for $t \in [k\tau,(k+1)\tau]$ could be formulated equivalently as a continuously differentiable function of the state variable $\boldsymbol{x}(k\tau) \in \Omega(k\tau;\mathcal{I}_0)$ for any fixed $t \in [k\tau,(k+1)\tau]$, and this mapping from $\Omega(k\tau;\mathcal{I}_0)$ to $\Omega(t;\mathcal{I}_0)$ for $t \in [k\tau,(k+1)\tau]$ is a continuously differentiable homeomorphism between two topological spaces $\Omega(k\tau;\mathcal{I}_0)$ and $\Omega(t;\mathcal{I}_0)$. This assertion is formalized in Corollary 1.

Corollary 1. *If the determinant of the sensitivity matrix $s_{\boldsymbol{x}(k\tau)}(t)$ w.r.t. any state $\boldsymbol{x}(k\tau) \in \Omega(k\tau;\mathcal{I}_0)$ at time $k\tau$ is not zero for any $t \in [k\tau,(k+1)\tau]$, then $\boldsymbol{\phi}(t;\boldsymbol{x}_0)$ for $\boldsymbol{x}_0 \in \mathcal{I}_0$ and $t \in [k\tau,(k+1)\tau]$ could be equivalently reformulated as a continuously differentiable function of the state variable $\boldsymbol{x}(k\tau) \in \Omega(k\tau;\mathcal{I}_0)$ and the time variable $t \in [k\tau,(k+1)\tau]$, and the state $\boldsymbol{x}(t) = \boldsymbol{\phi}(t;\boldsymbol{x}_0)$ is uniquely determined by the state $\boldsymbol{x}(k\tau)$ for any fixed $t \in [k\tau,(k+1)\tau]$, where $\boldsymbol{x}(k\tau) = \boldsymbol{\phi}(k\tau;\boldsymbol{x}_0)$.*

3.2 Generating a Constraint Bounding the Time-Lag Term

According to what we discussed above, here, we will infer a class of DDEs of the form (3), where the determinant of the corresponding sensitivity matrix $s_{\boldsymbol{x}(k\tau)}(t)$ w.r.t. the state variable $\boldsymbol{x}(k\tau) \in \Omega(k\tau;\mathcal{I}_0)$ at time $k\tau$ is not zero for $t \in [k\tau,(k+1)\tau]$, and $k = 0,\ldots,K-1$. Such a class of equations is derived by appropriately confining the time-lag term of the DDE (3), i.e., τ. In what follows, first, we review the classical result about diagonally dominant matrices from Varah [27].

If a matrix $A \in \mathbb{R}^{n\times n}$ is strictly diagonally dominant, i.e.,

$$\Delta_i(A) = |A_{ii}| - \sum_{j\neq i} |A_{ij}| > 0, \text{ with } 1 \leq i \leq n,$$

where A_{ij} is the entry in the i_{th} row and j_{th} column of the matrix A, then the inverse of the matrix A satisfies the bound

$$\|A^{-1}\|_\infty \leq max_{1\leq i\leq n} \frac{1}{\Delta_i(A)}.$$

Note that, by convention, $\|\cdot\|_\infty$ is the maximum absolute row sum of a matrix. Based on this classical result, we derive a constraint on the time-lag term τ in System (3) rendering the sensitivity matrix mentioned in Lemma 2 strictly diagonally dominant.

Assume that the sensitivity matrix $s_{\boldsymbol{x}((k-1)\tau)}(t)$ is strictly diagonally dominant s.t.

$$\|s_{\boldsymbol{x}((k-1)\tau)}(t)\|_{max} \leq R, \tag{8}$$

$$max_{1\leq i\leq n} \frac{1}{\Delta_i(s_{\boldsymbol{x}((k-1)\tau)}(t))} \leq \epsilon, \tag{9}$$

for any $t \in [(k-1)\tau, k\tau]$, where $k \in \{1,\ldots,K-1\}$, $\epsilon > 1$, and $R > 1$. Then, we construct the bound constraint on the time-lag term τ as follows.

Lemma 3. *Based on Eq. (8) and (9), if the time-lag term is*

$$\tau \leq min\left\{\frac{\epsilon-1}{\epsilon(nMR+N\epsilon)}, \frac{ln\frac{R^2+1}{2}}{\sqrt{n}(2\sqrt{n}M+N\epsilon)}\right\},$$

where M and N are presented in Constraint (4), then $s_{\boldsymbol{x}(k\tau)}(t)$ for $t \in [k\tau,(k+1)\tau]$ is strictly diagonally dominant with the property of $\|s_{\boldsymbol{x}(k\tau)}(t)\|_{max} \leq R$ and $max_{1\leq i\leq n}\frac{1}{\Delta_i(s_{\boldsymbol{x}(k\tau)}(t))} \leq \epsilon$.

Proof. Since the sensitivity matrix $s_{\boldsymbol{x}((k-1)\tau)}(t)$ is strictly diagonally dominant and Eq. (9) holds, the inequality

$$\|s^{-1}_{\boldsymbol{x}((k-1)\tau)}(t)\|_\infty \leq \epsilon,$$

also holds, where $t \in [(k-1)\tau, k\tau]$ and $k \in \{1, \ldots, K-1\}$. Accordingly, this implies that $\|s^{-1}_{\boldsymbol{x}((k-1)\tau)}(t)\|_{max} \leq \epsilon$. This way, according to Lemma 2, the sensitivity matrix $s_{\boldsymbol{x}(k\tau)}(t)$ for $t \in [k\tau, (k+1)\tau]$ w.r.t. the state $\boldsymbol{x}(k\tau)$ satisfies the sensitivity equation

$$\dot{s}_{\boldsymbol{x}(k\tau)} = \frac{\partial \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{x}_\tau)}{\partial \boldsymbol{x}} s_{\boldsymbol{x}(k\tau)} + \frac{\partial \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{x}_\tau)}{\partial \boldsymbol{x}_\tau} \frac{\partial \boldsymbol{x}_\tau}{\partial \boldsymbol{x}(k\tau)}, \text{ with } s_{\boldsymbol{x}(k\tau)}(k\tau) = \boldsymbol{I}. \tag{10}$$

In the following, we employ the comparison principle for ODEs to derive a bound on the solution to Eq. (10).

Let

$$M_d = max_{(k-1)\tau \leq t \leq k\tau} \sqrt{n}(2\sqrt{n}\|\boldsymbol{A}(t)\|_{max} + \|\boldsymbol{b}(t)\|_{max}),$$
$$N_d = max_{(k-1)\tau \leq t \leq k\tau} \sqrt{n}\|\boldsymbol{b}(t)\|_{max},$$

where $\boldsymbol{A}(t) = \frac{\partial \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{x}_\tau)}{\partial \boldsymbol{x}}$ and $\boldsymbol{b}(t) = \frac{\partial \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{x}_\tau)}{\partial \boldsymbol{x}_\tau} \frac{\partial \boldsymbol{x}_\tau}{\partial \boldsymbol{x}(i\tau)}$. It is obvious that $M_d \leq \sqrt{n}(2\sqrt{n}M + N\epsilon)$ and $N_d \leq \sqrt{n}N\epsilon$.

We take the j_{th} column of the sensitivity matrix $s_{\boldsymbol{x}(k\tau)}(t)$ and the matrix $\boldsymbol{b}(t)$ as a vector $\boldsymbol{y}(t)$ and $\boldsymbol{b}_j(t)$, where $j \in \{1, \ldots, n\}$. Let $u(t) = \|\boldsymbol{y}(t)\|_2^2 = \langle \boldsymbol{y}(t), \boldsymbol{y}(t) \rangle$ with $u(k\tau) = 1$, where $\|\boldsymbol{y}(t)\|_2$ is the 2-norm for $\boldsymbol{y}$ and $\langle \cdot, \cdot \rangle$ is an inner product in $\mathbb{R}^n$.

Based on Cauchy-Schwarz inequality and the fact that $2\|\boldsymbol{y}\|_2 \leq \|\boldsymbol{y}\|_2^2 + 1$, we obtain

$$\begin{aligned} \dot{u} &= 2\langle \boldsymbol{y}, \dot{\boldsymbol{y}} \rangle \leq 2\|\boldsymbol{y}\|_2 \|\dot{\boldsymbol{y}}\|_2 = 2\|\boldsymbol{y}\|_2 \|\boldsymbol{A}(t)\boldsymbol{y} + \boldsymbol{b}_j(t)\|_2 \leq 2\|\boldsymbol{y}\|_2^2 \|\boldsymbol{A}(t)\|_2 + 2\|\boldsymbol{y}\|_2 \|\boldsymbol{b}_j(t)\|_2 \\ &\leq 2\|\boldsymbol{A}(t)\|_2 \|\boldsymbol{y}\|_2^2 + \|\boldsymbol{b}_j(t)\|_2 (\|\boldsymbol{y}\|_2^2 + 1) \leq M_d \|\boldsymbol{y}\|_2^2 + N_d = M_d u + N_d. \end{aligned} \tag{11}$$

Applying Gronwall's inequality [5] to Eq. (11), we deduce that

$$u(t) \leq u_0 e^{M_d(t-k\tau)} + \int_{k\tau}^{t} N_d e^{M_d(t-s)} ds = u_0 e^{M_d(t-k\tau)} + \frac{N_d}{M_d} e^{M_d(t-k\tau)} - \frac{N_d}{M_d} \leq R_d,$$

for $k\tau \leq t \leq (k+1)\tau$, where $u_0 = u(k\tau) = 1$, and

$$R_d = \left(1 + \frac{N_d}{M_d}\right) e^{M_d \tau} - \frac{N_d}{M_d}.$$

Therefore, $\|\boldsymbol{y}(t)\|_2^2 \leq R_d$ for $k\tau \leq t \leq (k+1)\tau$. By solving the inequality $R_d \leq R^2$, we conclude that $\|s_{\boldsymbol{x}(k\tau)}(t)\|_{max} \leq R$ for $t \in [k\tau, (k+1)\tau]$ holds if

$$\tau \leq \frac{ln\frac{R^2+1}{2}}{\sqrt{n}(2\sqrt{n}M + N\epsilon)} \ ,$$

where the right side of this inequality could be gained when $M_d = N_d$.

For the sensitivity matrix $s_{\boldsymbol{x}(k\tau)}(t)$ with t ranging in the interval $[k\tau, (k+1)\tau]$, the diagonal element in the i-th row of the matrix $s_{\boldsymbol{x}(k\tau)}(t)$ is equal to

$$1 + \left[\frac{\partial f_i(\boldsymbol{x}, \boldsymbol{x}_\tau)}{\partial \boldsymbol{x}} \frac{\partial \boldsymbol{x}}{\partial x_{k\tau,i}} + \frac{\partial f_i(\boldsymbol{x}, \boldsymbol{x}_\tau)}{\partial \boldsymbol{x}_\tau} \frac{\partial \boldsymbol{x}_\tau}{\partial x_{k\tau,i}} \right]_{t=\xi_i} (t - k\tau),$$

the element in the i_{th} row and j_{th} column is equal to

$$\left[\frac{\partial f_i(\boldsymbol{x},\boldsymbol{x}_\tau)}{\partial \boldsymbol{x}}\frac{\partial \boldsymbol{x}}{\partial x_{k\tau,j}}+\frac{\partial f_k(\boldsymbol{x},\boldsymbol{x}_\tau)}{\partial \boldsymbol{x}_\tau}\frac{\partial \boldsymbol{x}_\tau}{\partial x_{k\tau,j}}\right]_{t=\xi_j}(t-k\tau),$$

where $j \in \{1,\dots,n\}\setminus\{i\}$ and ξ_l, for $l=1,\dots,n$, is some value in $(k\tau,(k+1)\tau)$.

Thus $\Delta_i(s_{\boldsymbol{x}(k\tau)}(t))$ is larger than

$$1-\tau\sum_{j=1}^{n}\left|\frac{\partial f_i(\boldsymbol{x},\boldsymbol{x}_\tau)}{\partial \boldsymbol{x}}\frac{\partial \boldsymbol{x}}{\partial x_{k\tau,j}}+\frac{\partial f_i(\boldsymbol{x},\boldsymbol{x}_\tau)}{\partial \boldsymbol{x}_\tau}\frac{\partial \boldsymbol{x}_\tau}{\partial x_{k\tau,j}}\right|_{t=\xi_j},$$

which in turn is larger than $1-(nMR+N\epsilon)\tau$.

By solving the inequality $\frac{1}{1-(nMR+N\epsilon)\tau} \le \epsilon$, we obtain that $\tau \le \frac{\epsilon-1}{\epsilon(nMR+N\epsilon)}$. Therefore, if

$$\tau \le min\left\{\frac{\epsilon-1}{\epsilon(nMR+N\epsilon)},\frac{ln\frac{R^2+1}{2}}{\sqrt{n}(2\sqrt{n}M+N\epsilon)}\right\},$$

then $\|s_{\boldsymbol{x}(k\tau)}(t)\|_{max} \le R$ and $max_{1\le i\le n}\frac{1}{\Delta_i(s_{\boldsymbol{x}(k\tau)}(t))} \le \epsilon$ hold, and $s_{\boldsymbol{x}(k\tau)}(t)$ is also diagonally dominant for $t\in[k\tau,(k+1)\tau]$ since $\tau \le \frac{\epsilon-1}{\epsilon(nMR+N\epsilon)}$, $1-(nMR+N\epsilon)\tau > 0$ holds. □

Combining Lemma 1 and Lemma 3, we deduce the following theorem.

Theorem 1. *If the time-lag term of DDE (3) is*

$$\tau \le min\left\{\tau^*,\frac{\epsilon-1}{\epsilon(nMR+N\epsilon)},\frac{ln\frac{R^2+1}{2}}{\sqrt{n}(2\sqrt{n}M+N\epsilon)}\right\},$$

where τ^* is from Lemma 1, then the solution mapping $\boldsymbol{\phi}(t;\cdot):\mathcal{I}_0 \mapsto \Omega(t;\mathcal{I}_0)$ to System (3) is a homeomorphism between two topological spaces $\mathcal{I}_0$ and $\Omega(t;\mathcal{I}_0)$ for any $t\in[0,K\tau]$.

When the time-lag τ satisfies the condition presented in Theorem 1, the homeomorphism property in Theorem 1 implies that the solution mapping $\boldsymbol{\phi}(t;\cdot):\mathcal{I}_0 \mapsto \Omega(t;\mathcal{I}_0)$ to System (3), where $t\in[0,K\tau]$, maps the boundary and interior points of the initial set $\mathcal{I}_0$ onto the boundary and interior points of the set $\Omega(t;\mathcal{I}_0)$ respectively. Therefore, the full reachable set induced by the initial set of System (3) could be retrieved by computing the reachable set just of the initial set's boundary. We illustrate Theorem 1 through the following example involving a delay τ that could be caused by sensor circuitry. Determining a bound on that delay could thus help facilitate the choice of appropriate sensors such that the delay τ incurred satisfies the conditions of Theorem 1.

Example 1. Consider a modified model of an electromechanical oscillation of a synchronous machine,

$$\dot{\boldsymbol{x}} = \begin{cases}\boldsymbol{g}(\boldsymbol{x}), & \text{if } t\in[0,\tau), \boldsymbol{x}(0)\in\mathcal{I}_0\\ \boldsymbol{f}(\boldsymbol{x},\boldsymbol{x}_\tau), & \text{if } t\in[\tau,K\tau],\end{cases} \tag{12}$$

with $\boldsymbol{x} = (\delta, w)'$, $\boldsymbol{x}_\tau = (\delta_\tau, w_\tau)$, $\boldsymbol{g}(\boldsymbol{x}) = (g_1(\boldsymbol{x}), g_2(\boldsymbol{x}))' = (0,0)'$, $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{x}_\tau) = (f_1(\boldsymbol{x}, \boldsymbol{x}_\tau), f_2(\boldsymbol{x}, \boldsymbol{x}_\tau))' = (w, 0.2 - 0.7\sin\delta_\tau - 0.05w_\tau)'$, and $\mathcal{I}_0 = [-0.5, 0.5] \times [2.5, 3.5]$, $K = 60$ and $\mathcal{X} = [-100, 100] \times [-100, 100]$. Through simple calculations, we obtain that $M = 1$, $N = 0.7$, $R = 2$ and $\epsilon = 2.5$, thus any $\tau \leq 0.104$ satisfies the condition in Theorem 1. In our experiments, we set $\tau = 0.1$.

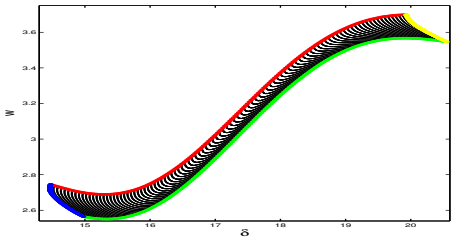

Fig. 1: An illustration of the reachable set for Example 1 at time $t = 6.0$ using simulation methods, (red, green, blue and yellow points – the approximate sampling states reachable from the boundary subsets $[-0.5, -0.5] \times [2.5, 3.5]$, $[0.5, 0.5] \times [2.5, 3.5]$, $[-0.5, 0.5] \times [2.5, 2.5]$ and $[-0.5, 0.5] \times [3.5, 3.5]$ respectively; black points – the approximate sampling states reachable from the entire initial set).

From the result illustrated in Fig. 1, we conclude that the corresponding solution mapping $\boldsymbol{\phi}(6; \cdot) : \mathcal{I}_0 \mapsto \Omega(6; \mathcal{I}_0)$ maps the boundary and interior points of the initial set $\mathcal{I}_0$ onto the boundary and interior points of the set $\Omega(6; \mathcal{I}_0)$ respectively, as the homeomorphism property suggests.

3.3 Constructing Reachable Sets

We in this section extend the set-boundary based reachability analysis method of [29, 30] for nonlinear control systems to reachability computations of System (3) with a time-lag τ satisfying the conditions of Theorem 1. The reduction is based on regarding the delayed state variable $\boldsymbol{x}_\tau$ in System (3) as a control input $\boldsymbol{u}(t)$, and the confinement to set boundaries adds considerably to precision as it significantly reduces the volume of the tube containing all such input trajectories $\boldsymbol{x}_\tau$. In our algorithm we obviously restrict the initial set $\mathcal{I}_0$ to a specific family of computer-representable sets in the $\mathbb{R}^n$ such as polytopes.

Assume that the initial set's boundary can be represented as an union of m subsets from the respective family, that is, $\partial\mathcal{I}_0 = \cup_{i=1}^m I_{0,i}$. For $t \in [0, \tau]$, the system is governed by ODE $\dot{\boldsymbol{x}} = \boldsymbol{g}(\boldsymbol{x})$. Therefore, we can apply any existing reachability analysis technique for ODEs that is able to deal with reachability computations with initial sets of forms such as polytopes, to the computation of an enclosure $\mathcal{B}_{0,t}$ of the reachable set for the initial set's boundary $\partial\mathcal{I}_0$ at time $t \in [0, \tau]$, where $\mathcal{B}_{0,t} = \cup_{i=1}^m B_{0,i}(t)$ and $B_{0,i}(t)$ is an over-approximation of the reachable set at time $t \in [0, \tau]$ starting from the set $I_{0,i}$, for $i = 1, \ldots, m$. The corresponding over-and under-approximations of the reachable set at time t could be constructed by including (excluding, resp.) the set $\mathcal{B}_{0,t}$ from the set obtained from convex combinations of points in $B_{0,i}(t)$, according to [30].

Based on these computations for the initial trajectory segment up to time τ, for $t \in [k\tau, (k+1)\tau]$, $k = 1, \ldots, K-1$, the following steps are used to compute its corresponding over- and under-approximations of the reachable set respectively.

1. Firstly, we compute an enclosure $B_{k,i}(t)$, for $t \in [k\tau, (k+1)\tau]$, of the reachable set $\Omega(t; I_{0,i})$ for System (3) with the initial set $B_{k-1,i}(k\tau)$ and $\boldsymbol{x}_\tau \in B_{k-1,i}(t-\tau)$. This enclosure can be computed by employing reachability analysis methods for nonlinear control systems of the form (5) with a time-varying input $\boldsymbol{u}(t) = \boldsymbol{x}_\tau \in B_{k-1,i}(t-\tau)$. Therefore, $\mathcal{B}_{k,t} = \cup_{i=1}^{m} B_{k,i}(t)$ is an enclosure of the reachable set for the initial set's boundary $\partial\mathcal{I}_0$ at time $t \in [k\tau, (k+1)\tau]$.
2. Secondly, we construct a simply connected compact polytope $O_{k,t}$ such that it covers $\mathcal{B}_{k,t}$. The set $O_{k,t}$ is an over-approximation of the reachable set $\Omega(t; \mathcal{I}_0)$ at time $t \in [k\tau, (k+1)\tau]$ according to Lemma 1 in [30].
3. Thirdly, we construct a simply connected polytope $U_{k,t}$ that satisfies two conditions: (1) the enclosure of the reachable set from the boundary of the initial set, i.e., $\mathcal{B}_{k,t}$, is obtained to be a subset of the enclosure of its complement, and (2) it intersects the interior of the reachable set $\Omega(t; \mathcal{I}_0)$. Then, according to Lemma 2 in [30], $U_{k,t}$ is an under-approximation of the reachable set $\Omega(t; \mathcal{I}_0)$ at time $t \in [k\tau, (k+1)\tau]$.

4 Examples and Discussions

In this section, we test our method on two examples of a two-dimensional system and a seven-dimensional system. Our implementation is based on Althoff's *continuous reachability analyzer (CORA)* [2], which is a MATLAB toolbox for prototype design of algorithms for reachability analysis. All computations are carried out on an i5-3337U 1.8GHz CPU with 4GB running Ubuntu Linux 13.10.

Example 2. Consider a modified Lotka-Volterra two-variables system with a delay τ, given by

$$\dot{\boldsymbol{x}} = \begin{cases} \boldsymbol{g}(\boldsymbol{x}), & \text{if } t \in [0, \tau), \boldsymbol{x}(0) \in \mathcal{I}_0 \\ \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{x}_\tau), & \text{if } t \in [\tau, K\tau] \end{cases} \tag{13}$$

with $\boldsymbol{x} = (x, y)'$, $\boldsymbol{x}_\tau = (x_\tau, y_\tau)'$, $\boldsymbol{g}(\boldsymbol{x}) = (g_1(\boldsymbol{x}), g_2(\boldsymbol{x}))' = (y, -0.2x + y - 0.2x^2 y)'$, $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{x}_\tau) = (f_1(\boldsymbol{x}, \boldsymbol{x}_\tau), f_2(\boldsymbol{x}, \boldsymbol{x}_\tau))' = (y, -0.2x_\tau + y - 0.2x^2 y)'$, $\mathcal{I}_0 = [0.9, 1.1] \times [0.9, 1.1]$ with $\partial\mathcal{I}_0 = \cup_{i=1}^{4} I_{0,i}$ and $\mathcal{X} = [0.5, 3.5] \times [0.2, 1.5]$, where $I_{0,1} = [0.9, 0.9] \times [0.9, 1.1]$, $I_{0,2} = [1.1, 1.1] \times [0.9, 1.1]$, $I_{0,3} = [0.9, 1.1] \times [0.9, 0.9]$ and $I_{0,4} = [0.9, 1.1] \times [1.1, 1.1]$.

In this example, the valuations $M = 2.10, N = 0.2$, $R = 2$ and $\epsilon = 2$ fulfill the condition in Lemma 3. Through simple calculations, $\tau = 0.01$ satisfies the requirement in Theorem 1. Also, K is assigned to 100, i.e. the entire time interval is $[0, 1.0]$. The over- and under-approximation of the reachable set illustrated in Fig. 2 and 3 are represented by polytopes. The computation time for computing over- and under-approximations is 111.56 seconds.

Example 3. Consider a seven-dimensional system with a delay τ[5],

$$\dot{\boldsymbol{x}} = \begin{cases} \boldsymbol{g}(\boldsymbol{x}), & \text{if } t \in [0, \tau), \boldsymbol{x}(0) \in \mathcal{I}_0 \\ \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{x}_\tau), & \text{if } t \in [\tau, K\tau] \end{cases} \tag{14}$$

[5] The delay-free system could be found in the Package CORA.

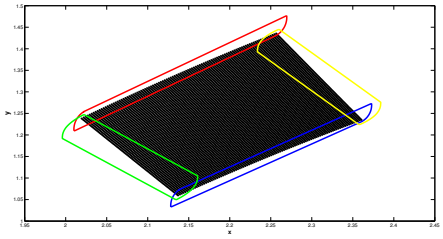

Fig. 2: An illustration of the reachable set of the initial set's boundary for Example 2 at time $t = 1.0$, (red curve – $\partial O(1.0; I_{0,1})$; blue curve – $\partial O(1.0; I_{0,2})$; green curve – $\partial O(1.0; I_{0,3})$; yellow curve– $\partial O(1.0; I_{0,4})$; black points – the approximate sampling states reachable from the initial set $\mathcal{I}_0$ after time duration of 1.0, which are computed using simulation methods).

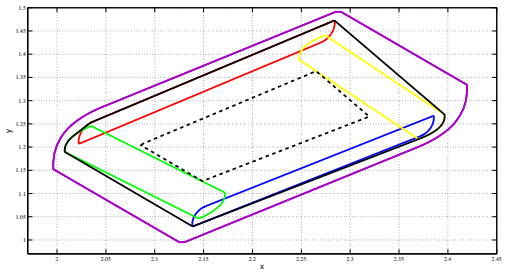

Fig. 3: An illustration of the reachable set of initial set's boundary for Example 2 at time $t = 1.0$, (red curve – $\partial O(1.0; I_{0,1})$; blue curve – $\partial O(1.0; I_{0,2})$; green curve – $\partial O(1.0; I_{0,3})$; yellow curve – $\partial O(1.0; I_{0,4})$; black curve – boundary $\partial O(1.0; \mathcal{I}_0)$ of the over-approximation obtained by our boundary method; black dash curve – boundary $\partial U(1.0; \mathcal{I}_0)$ of the under-approximation obtained by our boundary method; purple curve – boundary $\partial O(1.0; \mathcal{I}_0)$ of less tight over-approximation obtained by extrapolating the entire initial set rather than its boundaries).

with $\boldsymbol{x} = (x_1, \ldots, x_7)'$, $\boldsymbol{x}_\tau = (x_{1,\tau}, \ldots, x_{7,\tau})'$, $\boldsymbol{g}(\boldsymbol{x}) = \boldsymbol{0}$, $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{x}_\tau) = (1.4x_3 - 0.9x_{1,\tau}, 2.5x_5 - 1.5x_2, 0.6x_7 - 0.8x_3x_2, 2.0 - 1.3x_4x_3, 0.7x_1 - 1.0x_4x_5, 0.3x_1 - 3.1x_6, 1.8x_6 - 1.5x_7x_2)'$, $\mathcal{I}_0 = [1.1, 1.3] \times [0.95, 1.15] \times [1.4, 1.6] \times [2.3, 2.5] \times [0.9, 1.1] \times [0.0, 0.2] \times [0.35, 0.55]$ and $\mathcal{X} = [0.5, 1.5] \times [0.5, 1.5] \times [1.0, 2.0] \times [2.0, 3.0] \times [0.5, 1.5,] \times [0.0, 0.5] \times [0.0, 1.0]$.

The valuations $M = 3.9$, $N = 0.9$, $R = 2$ and $\epsilon = 9$ fulfill the condition in Lemma 3. Thus, $\tau \leq 0.01$ satisfies the requirement in Theorem 1. Also, τ and K are assigned to 0.01 and 10 respectively, i.e., the entire time interval is $[0, 0.1]$.

The computed over-approximation at time instant 0.1 is $O(0.1; \mathcal{I}_0) = [1.062, 1.302] \times [1.001, 1.216] \times [1.311, 1.529] \times [2.099, 2.322] \times [0.792, 0.989] \times [0.022, 0.183] \times [0.302, 0.516]$. The computed under-approximation at time instant 0.1 is $U(0.1; \mathcal{I}_0) = [1.113, 1.251] \times [1.052, 1.165] \times [1.362, 1.477] \times [2.150, 2.271] \times [0.843, 0.0.937] \times [0.073, 0.132] \times [0.353, 0.465]$. The computation time for both is 505.03 seconds. The projections for over-and under-approximations at time instants $t = 0.02, 0.04, 0.06, 0.08, 0.1$ on the $x_1 - x_2$ space are illustrated in Fig. 4.

From Fig. 2 that presents the approximation of the reachable set's boundary obtained by applying numerical simulation methods along with the set-boundary based method to Example 2, it is further confirmed that the set-boundary based method is able to produce a valid over-approximation of the reachable set's boundary when the

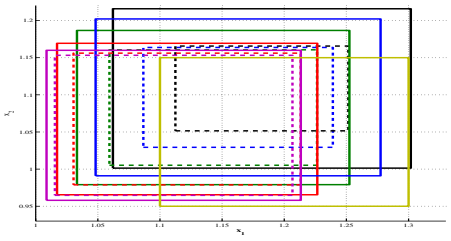

Fig. 4: An illustration of the reachable set on the $x_1 - x_2$ space for Example 3 at times $t = 0.0, 0.02, 0.04, 0.06, 0.08, 0.1$, (yellow solid line – the boundary of the initial set on the $x_1 - x_2$ space at time instant $t = 0.0$; purple, red, green, blue and black solid lines – the boundaries of over-approximations on the $x_1 - x_2$ space at time instants $t = 0.02, 0.04, 0.06, 0.08, 0.1$ respectively; purple, red, green, blue and black dashed lines – the boundaries of under-approximations on the $x_1 - x_2$ space at time instants $t = 0.02, 0.04, 0.06, 0.08, 0.1$ respectively).

delay-lag term τ satisfies the conditions in Theorem 1. Furthermore, it is concluded from Fig. 3 that the set-boundary based method as in Subsection 3.3 is able to output validated over- and under-approximations of the reachable sets. Also, the results in Fig. 3 demonstrate convincingly that the set-boundary based method induces a smaller wrapping effect in performing reachability analysis compared with extrapolating the entire initial set, since the boundaries of the initial set definitely have much smaller volume than the entire initial set. For Example 3, the approximations of the interval form as illustrated in Fig. 4 are computed for the sake of reducing computational burden. Note that the bound imposed for maintaining homeomorphism property applies to the time-lag in the DDE only and is not a bound on the temporal horizon coverable by reach-set computation, which can be arbitrarily larger if only the time-lag suits the condition. The relatively small horizons in these examples are due to the wrapping effect in the underlying reachability techniques, not the method itself, as discussed below.

Next, we should point out that the positive aspect induced by this kind of representation, is that they enable the analysis of some properties such as safety and reliability by reasoning in the theory of linear arithmetic. On the other side, they might not be the best representations of the reachable sets for nonlinear systems since the reachable sets of nonlinear systems modelled by ODEs and DDEs may be far from being convex as demonstrated in Fig. 1, thereby generating poor results when employing polytopes to characterize the reachable sets. In order to remedy this shortcoming of conservativeness induced by polytopes, we will struggle to employ representations of more complex shapes such as semi-algebraic sets in the construction of the reachable sets at the expense of computational efficiency. Another undesirable feature might be in our implementation, is due to the excessive use of previous state information to compute the set of current reachable states from the boundaries of the initial set. In a sense, while computing the set of reachable states at time $t \in [k\tau, (k+1)\tau]$, the entire reachable set of the past states within the time interval $[(k-1)\tau, k\tau]$ is used for the computations rather than the set of reachable states at just time instant $t - \tau$. Therefore, a large amount of spurious states not actually reachable at previous time from the boundaries of the initial set might be introduced, significantly increase the wrapping effect. Due to constructing over- and under-approximations by including (excluding, resp.) the obtained boundary enclosure from certain convex combination of points, a pessimistic over-approximation of the reachable sets from the boundaries of the initial set may reduce the tightness of

computed results accordingly. In order to circumvent this issue, we will extend Taylor-model based reachability analysis for ODEs to the proposed class of DDEs in the future work. Since Taylor models are functions being explicitly dependent on time and state variables, this dependence enables the use of an over-approximation associated with the reachable sets of the boundaries of the initial set at previous time $t - \tau$ rather than within the time interval $[(k-1)\tau, k\tau]$ to over-approximate the set of states reachable from the boundaries of the initial set at current time $t \in [k\tau, (k+1)\tau]$, thereby resulting in a significant reduction in the wrapping effect.

Finally, we should point out that our method, in this paper, is suitable for systems modeled by DDEs of the form (3) with solutions having homeomorphism property. But, it is restricted to a class of DDEs with time-lag term τ satisfying the conditions in Theorem 1. As a future work, we will expand such class of systems by loosing bound constraints on τ. Also, in order to measure the conservativeness on such bounds, we plan to deduce constraints on τ such that the solution to the associated system does not equip with homeomorphism property. Besides, if such homeomorphism property fails, one feasible solution to compute its over- and under-approximations of reachable sets is first to reformulate the associated DDE as an ODE via the method of steps in [26] and then apply the set-boundary based reachability analysis method of [29, 30] to the obtained ODE. However, the formulated ODE suffers an increase of space dimension over reachability time of interest. We will investigate more about this in future work.

5 Conclusion

In this paper, we have exposed a class of delay differential equations (DDEs) exhibiting homeomorphic dependency on initial conditions. Membership in this class is determined by conducting sensitivity analysis of the solution mapping with respect to the initial states, therefrom deriving an upper bound on the time-lag term of the DDE thus ensures homeomorphic dependency. One of the primary benefits of the existence of a corresponding homeomorphism is that state extrapolation can be pursued from the boundaries of the initial set only, rather than the full initial set, as the homeomorphism preserves boundaries and interiors of sets. As (appropriate enclosures of) the boundaries of the initial set have much smaller volume, such an approach tremendously reduces the wrapping effect incurred when using set-based state extrapolation on ODE with inputs as a means for enclosing solutions to the DDE. Furthermore, it allows us to construct an over- and under-approximations of the full reachable set by including (excluding, resp.) the obtained boundary enclosure from certain convex combinations of points in that boundary enclosure. We have illustrated the efficiency of our method on two examples of dimension 2 and 7.

Acknowledgement. This research from Peter N. Mosaad and Martin Fränzle is funded by Deutsche Forschungsgemeinschaft within the Research Training Group "SCARE - System Correctness under Adverse Conditions" (DFG GRK 1765) and from Mingshuai Chen, Yangjia Li, and Naijun Zhan is supported partly by NSFC under grant No. 61625206, by "973 Program" under grant No. 2014CB340701 and by the CAS/SAFEA International Partnership Program for Creative Research Teams. Besides, Yangjia Li is supported partly by NSFC under grant No. 61502467.

References

1. M. Althoff. Reachability analysis of nonlinear systems using conservative polynomialization and non-convex sets. In C. Belta and F. Ivancic, editors, *Proceedings of the 16th international conference on Hybrid systems: computation and control, HSCC 2013, April 8-11, 2013, Philadelphia, PA, USA*, pages 173–182. ACM, 2013.
2. M. Althoff. *CORA 2016 Manual*, 2016. http://www6.in.tum.de/Main/SoftwareCORA.
3. M. Althoff, O. Stursberg, and M. Buss. Reachability analysis of nonlinear systems with uncertain parameters using conservative linearization. In *Proceedings of the 47th IEEE Conference on Decision and Control, CDC 2008, December 9-11, 2008, Cancún, México*, pages 4042–4048. IEEE, 2008.
4. R. Bellman and K. L. Cooke. Differential-difference equations. Technical Report R-374-PR, The RAND Corporation, Santa Monica, California, Jan. 1963.
5. R. Bellman et al. The stability of solutions of linear differential equations. *Duke math. J*, 10(4):643–647, 1943.
6. M. Berz and K. Makino. Verified integration of ODEs and flows using differential algebraic methods on high-order taylor models. *Reliable Computing*, 4(4):361–369, 1998.
7. M. Chen, M. Fränzle, Y. Li, P. N. Mosaad, and N. Zhan. Validated simulation-based verification of delayed differential dynamics. In J. S. Fitzgerald, C. L. Heitmeyer, S. Gnesi, and A. Philippou, editors, *FM 2016: Formal Methods - 21st International Symposium, Limassol, Cyprus, November 9-11, 2016, Proceedings*, volume 9995 of *Lecture Notes in Computer Science*, pages 137–154, 2016.
8. X. Chen, S. Sankaranarayanan, and E. Ábrahám. Under-approximate flowpipes for non-linear continuous systems. In *Formal Methods in Computer-Aided Design, FMCAD 2014, Lausanne, Switzerland, October 21-24, 2014*, pages 59–66. IEEE, 2014.
9. A. Chutinan and B. H. Krogh. Computing polyhedral approximations to flow pipes for dynamic systems. In *Decision and Control, 1998. Proceedings of the 37th IEEE Conference on*, volume 2, pages 2089–2094. IEEE, 1998.
10. A. Donzé and O. Maler. Systematic simulation using sensitivity analysis. In A. Bemporad, A. Bicchi, and G. C. Buttazzo, editors, *Hybrid Systems: Computation and Control, 10th International Workshop, HSCC 2007, Pisa, Italy, April 3-5, 2007, Proceedings*, volume 4416 of *Lecture Notes in Computer Science*, pages 174–189. Springer, 2007.
11. A. Girard. Reachability of uncertain linear systems using zonotopes. In M. Morari and L. Thiele, editors, *Hybrid Systems: Computation and Control, 8th International Workshop, HSCC 2005, Zurich, Switzerland, March 9-11, 2005, Proceedings*, volume 3414 of *Lecture Notes in Computer Science*, pages 291–305. Springer, 2005.
12. E. Goubault, O. Mullier, S. Putot, and M. Kieffer. Inner approximated reachability analysis. In M. Fränzle and J. Lygeros, editors, *17th International Conference on Hybrid Systems: Computation and Control (part of CPS Week), HSCC'14, Berlin, Germany, April 15-17, 2014*, pages 163–172. ACM, 2014.
13. Z. Huang, C. Fan, and S. Mitra. Bounded invariant verification for time-delayed nonlinear networked dynamical systems. *Nonlinear Analysis: Hybrid Systems*, 23:211–229, 2017.
14. S. Kaynama, J. N. Maidens, M. Oishi, I. M. Mitchell, and G. A. Dumont. Computing the viability kernel using maximal reachable sets. In T. Dang and I. M. Mitchell, editors, *Hybrid Systems: Computation and Control (part of CPS Week 2012), HSCC'12, Beijing, China, April 17-19, 2012*, pages 55–64. ACM, 2012.
15. M. Korda, D. Henrion, and C. N. Jones. Inner approximations of the region of attraction for polynomial dynamical systems. *IFAC Proceedings Volumes*, 46(23):534–539, 2013.
16. Y. Kuang. *Delay differential equations: with applications in population dynamics*, volume 191, page 11. Academic Press, 1993.

17. A. B. Kurzhanski and P. Varaiya. Ellipsoidal techniques for reachability analysis. In N. A. Lynch and B. H. Krogh, editors, *Hybrid Systems: Computation and Control, Third International Workshop, HSCC 2000, Pittsburgh, PA, USA, March 23-25, 2000, Proceedings*, volume 1790 of *Lecture Notes in Computer Science*, pages 202–214. Springer, 2000.
18. A. B. Kurzhanski and P. Varaiya. Ellipsoidal techniques for hybrid dynamics: the reachability problem. In *New Directions and Applications in Control Theory*, pages 193–205. Springer, 2005.
19. C. Le Guernic and A. Girard. Reachability analysis of linear systems using support functions. *Nonlinear Analysis: Hybrid Systems*, 4(2):250–262, 2010.
20. R. E. Moore. Automatic local coordinate transformations to reduce the growth of error bounds in interval computation of solutions of ordinary differential equations. *Error in digital computation*, 2:103–140, 1965.
21. M. Neher, K. R. Jackson, and N. S. Nedialkov. On taylor model based integration of ODEs. *SIAM J. Numerical Analysis*, 45(1):236–262, 2007.
22. S. Prajna and A. Jadbabaie. Safety verification of hybrid systems using barrier certificates. In R. Alur and G. J. Pappas, editors, *Hybrid Systems: Computation and Control, 7th International Workshop, HSCC 2004, Philadelphia, PA, USA, March 25-27, 2004, Proceedings*, volume 2993 of *Lecture Notes in Computer Science*, pages 477–492. Springer, 2004.
23. S. Prajna and A. Jadbabaie. Methods for safety verification of time-delay systems. In *Proceedings of the 44th IEEE Conference on Decision and Control*, pages 4348–4353. IEEE, 2005.
24. S. Ratschan and Z. She. Safety verification of hybrid systems by constraint propagation based abstraction refinement. In M. Morari and L. Thiele, editors, *Hybrid Systems: Computation and Control, 8th International Workshop, HSCC 2005, Zurich, Switzerland, March 9-11, 2005, Proceedings*, volume 3414 of *Lecture Notes in Computer Science*, pages 573–589. Springer, 2005.
25. O. Stauning and K. Madsen. *Automatic validation of numerical solutions*. PhD thesis, Technical University of DenmarkDanmarks Tekniske Universitet, Department of Informatics and Mathematical ModelingInstitut for Informatik og Matematisk Modellering, 1997.
26. S. R. Taylor. Probabilistic properties of delay differential equations. 2004.
27. J. M. Varah. A lower bound for the smallest singular value of a matrix. *Linear Algebra and its Applications*, 11(1):3–5, 1975.
28. T. Wang, S. Lall, and M. West. Polynomial level-set method for polynomial system reachable set estimation. *IEEE Trans. Automat. Contr.*, 58(10):2508–2521, 2013.
29. B. Xue, A. Easwaran, N.-J. Cho, and M. Franzle. Reach-avoid verification for nonlinear systems based on boundary analysis. *IEEE Transactions on Automatic Control*, 2016.
30. B. Xue, Z. She, and A. Easwaran. Under-approximating backward reachable sets by polytopes. In S. Chaudhuri and A. Farzan, editors, *Computer Aided Verification - 28th International Conference, CAV 2016, Toronto, ON, Canada, July 17-23, 2016, Proceedings, Part I*, volume 9779 of *Lecture Notes in Computer Science*, pages 457–476. Springer, 2016.
31. L. Zou, M. Fränzle, N. Zhan, and P. N. Mosaad. Automatic verification of stability and safety for delay differential equations. In D. Kroening and C. S. Pasareanu, editors, *Computer Aided Verification - 27th International Conference, CAV 2015, San Francisco, CA, USA, July 18-24, 2015, Proceedings, Part II*, volume 9207 of *Lecture Notes in Computer Science*, pages 338–355. Springer, 2015.

Appendix

The proof of Lemma 1:

Proof. From Eq. (6), we obtain that

$$s^{ij}_{\boldsymbol{x}_0}(t) = \boldsymbol{I}^{ij} + \boldsymbol{J}^{ij}t,$$

where $\boldsymbol{J}^{ij} = \Big(D_{\boldsymbol{g}}(\boldsymbol{\phi}(t;\boldsymbol{x}_0))s_{\boldsymbol{x}_0}(t)\Big)^{ij}_{t=\tau_{ij}}$, τ_{ij} lies between 0 and t, $\boldsymbol{s}^{ij}_{\boldsymbol{x}_0}$ is the $(i,j)_{th}$ element of the matrix $\boldsymbol{s}_{\boldsymbol{x}_0}$ and $\boldsymbol{J}^{ij}$ is the $(i,j)_{th}$ element of the matrix $D_{\boldsymbol{g}}(\boldsymbol{\phi}(t;\boldsymbol{x}_0))s_{\boldsymbol{x}_0}(t)$ with $t = \tau_{ij}$. Also, since $\boldsymbol{g}(\boldsymbol{x}) \in \mathcal{C}^1(\mathcal{X})$, i.e. $\boldsymbol{g}(\cdot) : \mathcal{X} \mapsto \mathbb{R}^n$ is a continuously differentiable function, the element in the matrix $D_{\boldsymbol{g}} = \frac{\partial \boldsymbol{g}}{\partial \boldsymbol{x}}$ is bounded over an arbitrary compact set covering the reachable set $\cup_{t\in[0,\tau_1]}\Omega(t;\mathcal{I}_0)$ in the set $\mathcal{X}$, where τ_1 can be any number in $(0,\tau]$ such that $\cup_{t\in[0,\tau_1]}\Omega(t;\mathcal{I}_0) \subseteq \mathcal{X}$. The bounded property also applies to the matrix $s_{\boldsymbol{x}_0}(t)$. Consequently, a lower bound for all elements of the matrix $\boldsymbol{J}$ exists. Thus, $lim_{t\to 0}s_{\boldsymbol{x}_0}(t) = \boldsymbol{I}$ implies that there exists a $\tau^* \in (0,\tau_1]$ s.t. the sensitivity matrix $s_{\boldsymbol{x}_0}(t)$ for $t \in [0,\tau^*]$ is diagonally dominant. The conclusion follows from this fact. □

The proof of Lemma 2:

Proof. Since the determinant of the Jacobian matrix of the mapping $\boldsymbol{x}(t) = \boldsymbol{\psi}_{k-1}(t;\boldsymbol{x}((k-1)\tau,(k-1)\tau)$ w.r.t. any state $\boldsymbol{x}((k-1)\tau) \in \Omega((k-1)\tau;\mathcal{I}_0)$ is not zero for $t \in [(k-1)\tau, k\tau]$, then for any fixed $t \in [(k-1)\tau, k\tau]$, the mapping

$$\boldsymbol{x}(t) = \boldsymbol{\psi}_{k-1}(t;\ \cdot\ ,(k-1)\tau) : \Omega((k-1)\tau;\mathcal{I}_0) \longmapsto \Omega(t;\mathcal{I}_0)$$

is a bijection and its inverse mapping from $\Omega(t;\mathcal{I}_0)$ to $\Omega((k-1)\tau;\mathcal{I}_0)$ is continuously differentiable. Thus, the sensitivity matrix $s_{\boldsymbol{x}(k\tau)}(t)$ for $t \in [k\tau,(k+1)\tau]$ satisfies the sensitivity equation:

$$\dot{s}_{\boldsymbol{x}(k\tau)} = \frac{\partial \boldsymbol{f}(\boldsymbol{x},\boldsymbol{x}_\tau)}{\partial \boldsymbol{x}} s_{\boldsymbol{x}(k\tau)} + \frac{\partial \boldsymbol{f}(\boldsymbol{x},\boldsymbol{x}_\tau)}{\partial \boldsymbol{x}_\tau}\frac{\partial \boldsymbol{x}_\tau}{\partial \boldsymbol{x}(k\tau)},$$

with $s_{\boldsymbol{x}(k\tau)}(k\tau) = \boldsymbol{I} \in \mathbb{R}^{n\times n}$. □