Reach-Avoid Verification for Nonlinear Systems Based on Boundary Analysis

Bai Xue, Arvind Easwaran, Nam-Joon Cho, and Martin Fränzle

***Abstract*—In this technical note, we propose a set-boundary based method to verify reach-avoid properties of non-linear dynamical systems with parametric uncertainty, which works under the assumption that the initial set is a compact set. In comparison to the conventional approach employing safely overapproximating state extrapolation on the full volume of the initial set, our boundary-based method applies such state extrapolation only to the initial set's boundary, and thus to a set of significantly smaller volume. This can help enhance precision and reduce computational burden when solving reach-avoid verification problems, especially for cases with large initial sets and/or large time horizons. Furthermore, our boundary-based method lifts existing reachability-analysis techniques with their often confined geometric representations of reachable sets (like interval boxes, zonotopes, polyhedra, ellipsoids) to considerably more complex geometric shapes, where the boundary of the set is representable as a finite union of such shapes. The resulting benefits brought by our boundary-based method in reach-avoid verification are illustrated through several examples.**

***Index Terms*—Boundary analysis, reachability analysis, reach-avoid verification.**

I. Introduction

Reach-avoid verification of nonlinear systems deals with the problem of rigorously proving that an—often uncertain—dynamical system will eventually reach a desirable set of states while avoiding another set of bad or undesirable states. Reachability analysis, which involves computing reachable state sets, plays a fundamental role in the reach-avoid verification of nonlinear systems. Due to the fact that exact reachable sets for nonlinear systems are very hard to compute, an over-approximation is often computed, which is sufficient for verifying reach-avoid properties whenever the over-approximation is tight enough. There are diverse selection of algorithms for computing it by various representations such as zonotopes [1], [2], interval boxes [3], polyhedra [4], [5], oriented rectangular hulls [6], and ellipsoids [7].

Overly pessimistic over-approximations, however, render many reach-avoid properties unverifiable in practice [8]. This pessimism mainly arises due to the *wrapping effect*, which is the propagation and accumulation of over-approximation error through the iterative computation in the construction of reachable sets. As the extent of the wrapping effect correlates strongly with the volume of the initial set, techniques that partition the initial state space and independently compute reachable sets of those partitions are often used to reduce the wrapping effect [8], [9], especially for large initial sets or/and large time horizons. Such partitioning may, however, induce extensive demand on computation time and memory, often rendering the existing reachability analysis techniques not suitable for complex real-world applications [8]. Not being forced to explore the full, i.g. exponential in the dimensionality, number of partitions could help such procedures tremendously. This is the theme of this article, which explores means of computing the full reachable state space based on state-exploratory analysis of just a small sub-volume of the initial state set, namely a set enclosing its boundary.

Some advances have previously been reported in the literature along this line. The solution to a Hamilton-Jacobi partial differential equation corresponds exactly to the boundary of the reachable set [10] and level-set methods based on finite difference scheme are employed to numerically approximate the solution [11]. Appropriate corner points of reachable sets, called bracketing systems, are used in [12] to bound the full reachable sets by exploiting monotonicity properties of systems under consideration, and automatic detection of the underlying monotonicity properties as well as locally relaxing them through a combination of enclosure methods has been implemented in the iSAT-ODE solver for bounded model-checking of hybrid systems [13].

In this technical note, we generalize the corner-point method into a *boundary-based method*, which fits all nonlinear systems in which their corresponding vector field functions satisfy the condition of local Lipschitz continuity, from the perspective that a small sub-volume of the initial state set reduces the wrapping effect in performing reachability analysis, thereby relaxing the strong monotonicity properties necessary for Müller's theorem [12] underlying the corner-point method. Our boundary-based method is based on the initial set's boundary, which is of smaller volume than the entire initial set, and thus induces a smaller wrapping effect and can be covered by much smaller partitions should partitioning nevertheless be necessary. Given a parametric ordinary differential equation with a compact initial set, we only apply the existing reachability analysis techniques to compute an over-approximation of the reachable set of the initial set's boundary, and check whether it satisfies the specified property in our boundary-based method. If the verification result is positive, we can conclude that the design of the system modelled by the given ordinary differential equation is safe. We illustrate the benefits of our boundary-based method in solving the reach-avoid verification problems through several experimental studies drawn from related work. These experiments are based on the Taylor-model based flowpipe computation Flow* [14], [15] and the interval-based reachability library IOLAVaBE by Eggers, which incorporates VNODE-LP [19] and bracketing enclosures [12] as in iSAT-ODE [13]. The immediate benefits of the boundary-based method, which also manifest in our benchmarks, are the following:

Manuscript received March 2, 2016; revised August 15, 2016; accepted September 21, 2016. Date of publication October 6, 2016; date of current version June 26, 2017. This work was supported in part by the NTU-NHG Ageing Research Grant (ARG/14015) and by the Deutsche Forschungsgemeinschaft within the SFB-TR 14 Automatic Analysis and Verification of Complex Systems (AVACS). Recommended by Associate Editor A. Girard.

B. Xue and M. Fränzle are with the Carl von Ossietzky Universität Oldenburg, Germany (e-mail: bai.xue@uni-oldenburg.de; fraenzle@informatik.uni-oldenburg.de).

A. Easwaran and N-J. Cho are with the Nanyang Technological University, Singapore (e-mail: arvinde@ntu.edu.sg; njcho@ntu.edu.sg).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TAC.2016.2615599

1) Due to state sets of considerably smaller volume being handled, it helps to reduce computational burden and enhance accuracy when solving reach-avoid verification problems, especially for cases with large initial sets and/or large time horizons.
2) It relaxes restrictions imposed by most of the existing reach-set computation techniques concerning the shapes of representable state sets by lifting these methods to sets having finite unions of the aforementioned shapes as a boundary, which makes a difference in cases like zonotopes.

II. Preliminaries

In this section, we formally define the dynamic systems of interest, and formulate the reach-avoid verification problem under consideration in this technical note. The following notions will be used throughout this technical note: for a set Δ, its interior, complement, and boundary are denoted by Δ°, Δ^c, and $\partial\Delta$, respectively. Also, vectors are denoted by boldface letters.

Consider the following parametric ordinary differential equation system:

$$\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}, \boldsymbol{w}), \boldsymbol{x}(t_0) = \boldsymbol{x}_0 \in \mathcal{X}_0, \boldsymbol{w} \in \mathcal{W} \tag{1}$$

where $\boldsymbol{f} : \mathbb{R}^n \times \mathcal{W} \mapsto \mathbb{R}^n$ is nonlinear with dimension n and the compact set $\mathcal{W} \subset \mathbb{R}^m$ is an uncertainty domain for the parameter vector $\boldsymbol{w}$, and the compact set $\mathcal{X}_0 \subset \mathbb{R}^n$ with $\mathcal{X}_0^\circ \neq \emptyset$ represents the enclosure of initial values. Besides, we assume $\boldsymbol{f}(\cdot, \boldsymbol{w})$ is Lipschitz continuous for every $\boldsymbol{w} \in \mathcal{W}$, assuring existence and uniqueness of the trajectories of the system (1) over some time interval $[t_0, \delta]$ with $\delta > t_0$, and the trajectory of the system (1) over the time interval $[t_0, \delta]$ is defined to be $\boldsymbol{\phi}(t; \boldsymbol{x}_0, t_0, \boldsymbol{w}) = \boldsymbol{x}(t)$, where $\boldsymbol{x}(t)$ is the solution to the system in (1) with the initial condition $\boldsymbol{x}_0 \in \mathcal{X}_0$ and parameter value $\boldsymbol{w} \in \mathcal{W}$ at time instant t_0. Note that in this technical note, we only consider cases where the parameter vector $\boldsymbol{w} \in \mathcal{W}$ is constant over the time interval $[t_0, \delta]$.

The reach-avoid verification problem for systems defined by Equation (1), which is the focus of this technical note, is as follows.

Definition 1 (Reach-Avoid (RA) Problem): Given a set $\mathcal{X} \subset \mathbb{R}^n$, which is partitioned into a set $\mathcal{X}_{safe}$ satisfying $\mathcal{X}_0 \subseteq \mathcal{X}_{safe}$, a set $\mathcal{X}_{unsafe}$ satisfying $\mathcal{X}_0 \cap \mathcal{X}_{unsafe} = \emptyset$ and a fixed time instant T satisfying $t_0 < T \leq \delta$, verify that for any combination of $\boldsymbol{x}_0 \in \mathcal{X}_0$ and $\boldsymbol{w} \in \mathcal{W}$, $\boldsymbol{\phi}(\tau; \boldsymbol{x}_0, t_0, \boldsymbol{w}) \in \mathcal{X}_{safe}$ for all $\tau \in [t_0, T]$ and $\boldsymbol{\phi}(T; \boldsymbol{x}_0, t_0, \boldsymbol{w}) \in \mathcal{X}_{goal}$, where $\mathcal{X}_{goal} \subseteq \mathcal{X}_{safe}$ is a compact simply connected set.[1]

This RA problem can be solved by performing reachability analysis of the system, which relies on reachable set computations. In Definition 2, we define the reachable set of $\mathcal{X}_0$.

Definition 2 (Reachable Set): Given a system of the form in Equation (1), a state space $\mathcal{X}$ and a compact set $\mathcal{X}_0$, the reachable set of $\mathcal{X}_0$ at the time instant $t > t_0$ is defined to be $\Omega(t; \mathcal{X}_0, t_0, \mathcal{W}) = \{\boldsymbol{x} : \boldsymbol{x} = \boldsymbol{\phi}(t; \boldsymbol{x}_0, t_0, \boldsymbol{w}), \boldsymbol{x}_0 \in \mathcal{X}_0, \boldsymbol{w} \in \mathcal{W}\}$. The reachable set of $\mathcal{X}_0$ over the time interval $[t_0, \tau]$ is defined to be $\Omega([t_0, \tau]; \mathcal{X}_0, t_0, \mathcal{W}) = \cup_{t \in [t_0, \tau]} \Omega(t; \mathcal{X}_0, t_0, \mathcal{W})$.

The RA problem can then be equivalently formulated as a problem of verifying that $\Omega([t_0, T]; \mathcal{X}_0, t_0, \mathcal{W}) \subseteq \mathcal{X} \setminus \mathcal{X}_{unsafe}$ and $\Omega(T; \mathcal{X}_0, t_0, \mathcal{W}) \subseteq \mathcal{X}_{goal}$.

The exact computation of the reachable set $\Omega(\tau; \mathcal{X}_0, t_0, \mathcal{W})$, $\tau \in [t_0, T]$, is a challenging problem for general nonlinear systems, since most nonlinear systems do not have closed solutions. Thus as mentioned previously in the introduction, an over-approximation is often computed [8]. Formally, we definite an over-approximation of the reachable set in Definition 3.

Definition 3 (Over-Approximation): A set $\Psi(t; \mathcal{X}_0, t_0, \mathcal{W})$ is called an over-approximation of $\Omega(t; \mathcal{X}_0, t_0, \mathcal{W})$ if $\Omega(t; \mathcal{X}_0, t_0, \mathcal{W}) \subseteq \Psi(t; \mathcal{X}_0, t_0, \mathcal{W})$. Similarly, a set $\Psi([t_0, \tau]; \mathcal{X}_0, t_0, \mathcal{W})$ is called an over-approximation of $\Omega([t_0, \tau]; \mathcal{X}_0, t_0, \mathcal{W})$ if $\Omega([t_0, \tau]; \mathcal{X}_0, t_0, \mathcal{W}) \subseteq \Psi([t_0, \tau]; \mathcal{X}_0, t_0, \mathcal{W})$.

According to Definition 3, the RA problem can be relaxed to the classical approximate reachability analysis problem: Compute $\Psi(\tau; \mathcal{X}_0, t_0, \mathcal{W})$ for $\forall \tau \in [t_0, T]$ such that $\Psi([t_0, T]; \mathcal{X}_0, t_0, \mathcal{W}) \subseteq \mathcal{X} \setminus \mathcal{X}_{unsafe}$ and $\Psi(T; \mathcal{X}_0, t_0, \mathcal{W}) \subseteq \mathcal{X}_{goal}$ hold. If an over-approximation $\Psi(\tau; \mathcal{X}_0, t_0, \mathcal{W})$ for $\forall \tau \in [t_0, T]$ can be computed for the system represented by Equation (1), then we can conclude that the RA problem has been solved. Note that we only consider the case where the time instant T is fixed in this note, the more complex case of T not being fixed will be investigated in our future work. As mentioned, the wrapping effect often impedes the application of reachability analysis to real problems. In this technical note, we address the limitation of solving the RA problem by only performing the reachability analysis of the initial set's boundary: Compute $\Psi(\tau; \partial\mathcal{X}_0, t_0, \mathcal{W})$ for $\forall \tau \in [t_0, T]$ such that $\Psi([t_0, T]; \partial\mathcal{X}_0, t_0, \mathcal{W}) \subseteq \mathcal{X} \setminus \mathcal{X}_{unsafe}$ and $\Psi(T; \partial\mathcal{X}_0, t_0, \mathcal{W}) \subseteq \mathcal{X}_{goal}$ hold.

III. Solving Reach-Avoid Verification Problems by Boundary Sets

In this section, we formulate how to address the RA problem by only computing reachable sets of the initial set's boundary rather than the entire initial set. We first present the pertained theory that enables us to solve the RA problem by performing reachability analysis based on the initial set's boundary, and then elucidate our algorithm.

Our theory, which mainly consists of three lemmas, in this technical note is built on the following theorem, which discover a relation between two sets under homeomorphic maps.

Theorem 1: [17, Corollary 6.7] Let A and B be arbitrary subsets of $\mathbb{R}^n$, and let $h : A \to B$ be a homeomorphism. Then h maps interior points onto interior points, and boundary points onto boundary points.

According to the Lipschitz assumption on $\boldsymbol{f}$, we obtain that $\boldsymbol{\phi}(t; \cdot, t_0, \boldsymbol{w}) : \mathcal{X}_0 \to \Omega(t; \mathcal{X}_0, t_0, \boldsymbol{w})$ is a homeomorphism between the two topological spaces $\mathcal{X}_0$ and $\Omega(t; \mathcal{X}_0, t_0, \boldsymbol{w})$ for any fixed $\boldsymbol{w} \in \mathcal{W}$. Therefore, following from Theorem 1, we derive a corollary formulating a connection between the initial set's boundary and the set reachable from the entire initial set.

Corollary 1: If $\mathcal{X}_0$ is a non-empty compact set with interior $\mathcal{X}_0^\circ \neq \emptyset$ then $\Omega(t; \mathcal{X}_0, t_0, \boldsymbol{w})$ is also a non-empty compact set with $\Omega(t; \mathcal{X}_0, t_0, \boldsymbol{w})^\circ \neq \emptyset$ and $\partial\Omega(t; \mathcal{X}_0, t_0, \boldsymbol{w}) = \Omega(t; \partial\mathcal{X}_0, t_0, \boldsymbol{w})$ for $\forall \boldsymbol{w} \in \mathcal{W}$ and $\forall t \in [t_0, T]$.

According to Corollary 1, for a fixed $\boldsymbol{w} \in \mathcal{W}$, the boundary of the reachable set of $\mathcal{X}_0$ at time instant t is equal to the reachable set of the boundary of $\mathcal{X}_0$ at time instant t. Thus, $\cup_{\boldsymbol{w} \in \mathcal{W}} \partial\Omega(t; \mathcal{X}_0, t_0, \boldsymbol{w}) = \cup_{\boldsymbol{w} \in \mathcal{W}} \Omega(t; \partial\mathcal{X}_0, t_0, \boldsymbol{w}) = \Omega(t; \partial\mathcal{X}_0, t_0, \mathcal{W})$ and $\cup_{t \in [t_0, T]} \cup_{\boldsymbol{w} \in \mathcal{W}} \partial\Omega(t; \mathcal{X}_0, t_0, \boldsymbol{w}) = \cup_{t \in [t_0, T]} \cup_{\boldsymbol{w} \in \mathcal{W}} \Omega(t; \partial\mathcal{X}_0, t_0, \boldsymbol{w}) = \Omega([t_0, T]; \partial\mathcal{X}_0, t_0, \mathcal{W})$.

Based on the above findings, we showcase three important lemmas, displaying that estimating $\cup_{\boldsymbol{w} \in \mathcal{W}} \partial\Omega(t; \mathcal{X}_0, t_0, \boldsymbol{w})$ and $\cup_{t \in [t_0, T]} \cup_{\boldsymbol{w} \in \mathcal{W}} \partial\Omega(t; \mathcal{X}_0, t_0, \boldsymbol{w})$ is sufficient to solve the RA problem. The first lemma is to verify that the trajectories starting from the initial set $\mathcal{X}_0$ do not leave the region $\mathcal{X}$ over the time interval $[t_0, T]$. The second one is to verify that the trajectories starting from the initial set $\mathcal{X}_0$ do not enter the unsafe region $\mathcal{X}_{unsafe}$. The last one is to verify that the trajectories starting from the initial set $\mathcal{X}_0$ will enter the target region at time instant $t = T$.

[1] A set is simply connected if there are no holes in it to prevent the continuous shrinking of each closed arc to a point [16].

Lemma 1: If $\cup_{t\in[t_0,T]}\cup_{\boldsymbol{w}\in\mathcal{W}}\partial\Omega(t;\mathcal{X}_0,t_0,\boldsymbol{w})\subseteq\mathcal{X}$ and $\mathcal{X}_0\subseteq\mathcal{X}$, then $\Omega([t_0,T];\mathcal{X}_0,t_0,\mathcal{W})\subseteq\mathcal{X}$.

Proof: Assume that there exist $\boldsymbol{x}_0\in\mathcal{X}_0$, $\tau\in[t_0,T]$ and $\boldsymbol{w}_0$ such that $\boldsymbol{\phi}(\tau;\boldsymbol{x}_0,t_0,\boldsymbol{w}_0)\notin\mathcal{X}$. For simplicity, $\boldsymbol{\phi}(\tau;\boldsymbol{x}_0,t_0,\boldsymbol{w}_0)$ is denoted by $\boldsymbol{x}_{\tau,\boldsymbol{w}_0}$. Since $\cup_{t\in[t_0,T]}\cup_{\boldsymbol{w}\in\mathcal{W}}\partial\Omega(t;\mathcal{X}_0,t_0,\boldsymbol{w})\subseteq\mathcal{X}$ holds, $\boldsymbol{x}_0\in\mathcal{X}_0^\circ$ according to Theorem 1. Due to the fact that $\mathcal{X}_0\subseteq\mathcal{X}$ and $\boldsymbol{x}_{\tau,\boldsymbol{w}_0}\notin\mathcal{X}$, there exists $\tau'\in[t_0,\tau]$ satisfying $\boldsymbol{\phi}(\tau';\boldsymbol{x}_0,t_0,\boldsymbol{w}_0)\in\partial\mathcal{X}_0$. Let $\boldsymbol{x}_{\tau',\boldsymbol{w}_0}=\boldsymbol{\phi}(\tau';\boldsymbol{x}_0,t_0,\boldsymbol{w}_0)$, then according to the semigroup property of the solution mapping $\boldsymbol{\phi}(t;\boldsymbol{x}_0,t_0,\boldsymbol{w}_0)$[2], $\boldsymbol{\phi}(\tau;\boldsymbol{x}_0,t_0,\boldsymbol{w}_0)=\boldsymbol{\phi}(\tau-\tau'+t_0;\boldsymbol{x}_{\tau',\boldsymbol{w}_0},t_0,\boldsymbol{w}_0)\notin\mathcal{X}$ holds, contradicting the fact that $\cup_{t\in[t_0,T]}\cup_{\boldsymbol{w}\in\mathcal{W}}\partial\Omega(t;\mathcal{X}_0,t_0,\boldsymbol{w})\subseteq\mathcal{X}$. Therefore, the conclusion that $\Omega([t_0,T];\mathcal{X}_0,t_0,\mathcal{W})\subseteq\mathcal{X}$ is proven.

Lemma 2: If $\cup_{t\in[t_0,T]}\cup_{\boldsymbol{w}\in\mathcal{W}}\partial\Omega(t;\mathcal{X}_0,t_0,\boldsymbol{w})\cap\mathcal{X}_{unsafe}=\emptyset$ and $\mathcal{X}_0\cap\mathcal{X}_{unsafe}=\emptyset$, then $\Omega([t_0,T];\mathcal{X}_0,t_0,\mathcal{W})\cap\mathcal{X}_{unsafe}=\emptyset$.

Proof: Assume there exist $\tau\in[t_0,T]$ and $\boldsymbol{w}_0\in\mathcal{W}$ such that $\Omega(\tau;\mathcal{X}_0,t_0,\boldsymbol{w}_0)\cap\mathcal{X}_{unsafe}\neq\emptyset$. Let $\boldsymbol{x}_{\tau,\boldsymbol{w}_0}\in\Omega(\tau;\mathcal{X}_0,t_0,\boldsymbol{w}_0)\cap\mathcal{X}_{unsafe}$, then there is a point $\boldsymbol{x}_0\in\mathcal{X}_0$ such that $\boldsymbol{x}_{\tau,\boldsymbol{w}_0}=\boldsymbol{\phi}(\tau;\boldsymbol{x}_0,t_0,\boldsymbol{w}_0)$. For the reason that $\mathcal{X}_0\cap\mathcal{X}_{unsafe}=\emptyset$ and $\boldsymbol{x}_{\tau,\boldsymbol{w}_0}\in\mathcal{X}_{unsafe}$, there exists $\tau'\in[t_0,\tau]$ such that $\boldsymbol{\phi}(\tau';\boldsymbol{x}_0,t_0,\boldsymbol{w}_0)\in\partial\mathcal{X}_0$. Let $\boldsymbol{x}_{\tau',\boldsymbol{w}_0}=\boldsymbol{\phi}(\tau';\boldsymbol{x}_0,t_0,\boldsymbol{w}_0)$. According to Theorem 1 and the semigroup property of the solution mapping $\boldsymbol{\phi}(t;\boldsymbol{x}_0,t_0,\boldsymbol{w}_0)$, $\boldsymbol{x}_{\tau,\boldsymbol{w}_0}=\boldsymbol{\phi}(\tau-\tau'+t_0;\boldsymbol{x}_{\tau',\boldsymbol{w}_0},t_0,\boldsymbol{w}_0)\in\partial\Omega(\tau-\tau'+t_0;\mathcal{X}_0,t_0,\boldsymbol{w}_0)$ holds, contradicting the fact that $\cup_{t\in[t_0,T]}\cup_{\boldsymbol{w}\in\mathcal{W}}\partial\Omega(t;\mathcal{X}_0,t_0,\boldsymbol{w})\cap\mathcal{X}_{unsafe}=\emptyset$. Thus, $\cup_{t\in[t_0,T]}\Omega(t;\mathcal{X}_0,t_0,\mathcal{W})\cap\mathcal{X}_{unsafe}=\emptyset$.

Lemma 3: If $\cup_{\boldsymbol{w}\in\mathcal{W}}\partial\Omega(T;\mathcal{X}_0,t_0,\boldsymbol{w})\subseteq\mathcal{X}_{goal}$, then $\Omega(T;\mathcal{X}_0,t_0,\mathcal{W})\subseteq\mathcal{X}_{goal}$.

Proof: For $n=1$, where n is the number of dimensions of the system represented by (1), the fact that the conclusion holds can be confirmed easily. Thus, in the following we just prove that the conclusion holds for $n\geq 2$.

Assume that there exist $\boldsymbol{x}_0\in\mathcal{X}_0$ and $\boldsymbol{w}_0\in\mathcal{W}$ such that $\boldsymbol{\phi}(T;\boldsymbol{x}_0,t_0,\boldsymbol{w}_0)\notin\mathcal{X}_{goal}$. Since $\cup_{\boldsymbol{w}\in\mathcal{W}}\partial\Omega(T;\mathcal{X}_0,t_0,\boldsymbol{w})\subseteq\mathcal{X}_{goal}$, $\boldsymbol{x}_0\in\mathcal{X}_0^\circ$ can be assured from Theorem 1.

For the reason that $\mathcal{X}_{goal}$ is a simply connected compact set, its complement $\mathcal{X}_{goal}^c$ is open and connected. Furthermore, $\mathcal{X}_{goal}^c$ is path-connected [18, Proposition 1], implying that there exists a continuous path $l(r):[0,1)\mapsto\mathbb{R}^n$ such that $l(r)\in\mathcal{X}_{goal}^c$ for $\forall r\in[0,1)$, $l(0)=\boldsymbol{\phi}(T;\boldsymbol{x}_0,t_0,\boldsymbol{w}_0)$ and $lim_{r\to1}\|l(r)\|=+\infty$. Since $\boldsymbol{x}_0\in\mathcal{X}_0^\circ$, there is $\epsilon_0>0$ such that $\Omega(T;\mathbb{U}(\boldsymbol{x}_0;\epsilon_0),t_0,\boldsymbol{w}_0)\subset\mathcal{X}_{goal}^c$, where $\mathbb{U}(\boldsymbol{x}_0;\epsilon_0)=\{\boldsymbol{x}:\|\boldsymbol{x}-\boldsymbol{x}_0\|\leq\epsilon_0\}$ and $\mathbb{U}(\boldsymbol{x}_0;\epsilon_0)\subseteq\mathcal{X}_0$. Assume r_1 is the maximum value such that $l(r_1)\in\partial\Omega(\boldsymbol{x}_0;\mathbb{U}(\boldsymbol{x}_0;\epsilon_0),t_0,\boldsymbol{w}_0)$ and $\boldsymbol{\phi}(T;\boldsymbol{x}_1,t_0,\boldsymbol{w}_0)=l(r_1)$. In the case that $\boldsymbol{x}_1\in\partial\mathcal{X}_0$, this contradicts the fact that $\cup_{\boldsymbol{w}\in\mathcal{W}}\partial\Omega(T;\mathcal{X}_0,t_0,\boldsymbol{w})\subseteq\mathcal{X}_{goal}$; otherwise, the above process is repeated to find $\boldsymbol{x}_2,\boldsymbol{x}_3,\ldots$, and r_2, r_3, …, where $r_1\leq r_2\leq r_3\leq\ldots$. In case of a point belonging to $\partial\mathcal{X}_0$ among the points $\boldsymbol{x}_2,\boldsymbol{x}_3,\ldots$, a contradiction is obtained and the proof is finished; otherwise, due to the fact that $\{r_i\}_{i=1}^{+\infty}$ is an increasing sequence and bounded, $lim_{i\to+\infty}r_i=\overline{r}$, where $0<\overline{r}\leq1$.

1) $\overline{r}<1$: since $l(r)$ is a continuous function over r, $lim_{i\to+\infty}l(r_i)=l(\overline{r})$ and $lim_{i\to+\infty}\boldsymbol{\phi}(T;\boldsymbol{x}_i,t_0,\boldsymbol{w}_0)=l(\overline{r})$ hold, and $l(\overline{r})\in\mathcal{X}_{goal}^c$. Considering that the map $\boldsymbol{\phi}(T;\cdot,t_0,\boldsymbol{w}_0):\mathcal{X}_0\to\Omega(T;\mathcal{X}_0,t_0,\boldsymbol{w}_0)$ is bijective and continuous, there is a point $\overline{\boldsymbol{x}}$ such that $lim_{i\to+\infty}\boldsymbol{x}_i=\overline{\boldsymbol{x}}$. Further, $\boldsymbol{\phi}(T;\overline{\boldsymbol{x}},t_0,\boldsymbol{w}_0)=l(\overline{r})$, implying that $\overline{\boldsymbol{x}}\in\mathcal{X}_0^\circ$. Starting with $\overline{\boldsymbol{x}}$ and $\overline{r}$, we repeat the above process to obtain $\overline{\boldsymbol{x}}_1,\overline{\boldsymbol{x}}_2,\ldots,\overline{\boldsymbol{x}}_i,\ldots$, and $\overline{r}_1$, $\overline{r}_2$, …, $\overline{r}_i$, …, until the limit of the sequence $\{r_1,r_2,\ldots,\overline{r}_1,\overline{r}_2,\ldots\}$ is equal to one, where $\overline{r}_1\leq\overline{r}_2\leq\ldots$. Then $lim_{i\to+\infty}\|\boldsymbol{\phi}(T;\overline{\boldsymbol{x}}_i,t_0,\boldsymbol{w}_0)\|=lim_{i\to+\infty}\|l(\overline{r}_i)\|=+\infty$. Therefore, $lim_{i\to+\infty}\|\overline{\boldsymbol{x}}_i\|=+\infty$, contradicting the fact that $\Omega(T;\mathcal{X},t_0,\boldsymbol{w}_0)$ is a compact set.

2) $\overline{r}=1$: the same contradiction is obtained as above. Therefore, $\Omega(T;\mathcal{X}_0,t_0,\mathcal{W})\subseteq\mathcal{X}_{goal}$ holds.

Remark 1: If T is of compact interval form rather than a constant, the following statement similar to that in Lemma 3 still holds: If $\cup_{\boldsymbol{w}\in\mathcal{W}}\cup_{t\in T}\partial\Omega(t;\mathcal{X}_0,t_0,\boldsymbol{w})\subseteq\mathcal{X}_{goal}$, $\Omega(T;\mathcal{X}_0,t_0,\mathcal{W})\subseteq\mathcal{X}_{goal}$.

Lemmas 1, 2, and 3 together imply that knowing the states reachable from the boundary of the initial set $\mathcal{X}_0$ is sufficient to solve the RA problem. This is formally stated in Theorem 2.

Theorem 2: Given a system of the form in Equation (1), if the set of states reachable from the boundary of the compact initial set $\mathcal{X}_0$ satisfy the following conditions: 1). stay in the constrained set $\mathcal{X}$ within the time interval $[0,T]$; 2). can not enter the unsafe set $\mathcal{X}_{unsafe}$ within the time interval $[0,T]$; 3). enter the specified compact simply connected set $\mathcal{X}_{goal}$ at time instant $t=T$, then the RA problem is solved positively.

However, it is challenging to compute the exact boundary of the reachable set. Thus, we resort to computing its over-approximation. Clearly, if $\cup_{t\in[t_0,T]}\cup_{\boldsymbol{w}\in\mathcal{W}}\partial\Omega(t;\mathcal{X}_0,t_0,\boldsymbol{w})$ and $\cup_{\boldsymbol{w}\in\mathcal{W}}\partial\Omega(T;\mathcal{X}_0,t_0,\boldsymbol{w})$ are replaced with their corresponding over-approximations in Lemmas 1–3, the conclusions of Lemmas 1–3 still hold. As mentioned previously, $\cup_{t\in[t_0,T]}\cup_{\boldsymbol{w}\in\mathcal{W}}\partial\Omega(t;\mathcal{X}_0,t_0,\boldsymbol{w})=\cup_{t\in[t_0,T]}\cup_{\boldsymbol{w}\in\mathcal{W}}\Omega(t;\partial\mathcal{X}_0,t_0,\boldsymbol{w})=\Omega([t_0,T];\partial\mathcal{X}_0,t_0,\mathcal{W})$ and $\cup_{\boldsymbol{w}\in\mathcal{W}}\partial\Omega(T;\mathcal{X}_0,t_0,\boldsymbol{w})=\Omega(T;\partial\mathcal{X}_0,t_0,\mathcal{W})$. Thus, over-approximations of $\Omega([t_0,T];\partial\mathcal{X}_0,t_0,\mathcal{W})$ and $\Omega(T;\partial\mathcal{X}_0,t_0,\mathcal{W})$ are computed in our algorithm below.

For our algorithm to solve the RA problem with an assumption that a time grid $t_0<t_1<\ldots<t_N=T$ with a step size h is adopted, we first compute an over-approximation $\Psi([t_j,t_{j+1}];\partial\mathcal{X}_0,t_0,\mathcal{W})$, and then check whether $\Psi([t_j,t_{j+1}];\partial\mathcal{X}_0,t_0,\mathcal{W})\subseteq\mathcal{X}$ and $\Psi([t_j,t_{j+1}];\partial\mathcal{X}_0,t_0,\mathcal{W})\cap\mathcal{X}_{unsafe}=\emptyset$ holds (when $j=N$, $\Psi(T;\partial\mathcal{X}_0,t_0,\mathcal{W})\subseteq\mathcal{X}_{goal}$ needs to be verified). In the case that the answer is negative to any of these checks, the RA problem remains unsolved. Otherwise, the RA problem is solved successfully.

In the above algorithm, an over-approximation of the reachable set of the initial set's boundary needs to be computed. Any existing method can be used to compute it. Depending on the form of $\partial\mathcal{X}_0$, e.g., polytopes, zonotopes, rectangles, etc., we can choose corresponding efficient methods.

Remark 2: In some cases where the exact boundary of the initial set is difficult to obtain, performing reachability analysis on an over-approximation of the initial set's boundary can also be used to solve the RA problem. This can be applied to some cases where either the exact boundary of the initial set is hard to compute, or where covering it by the shapes of partitions offered by the particular reach-set computation method employed requires an enormous number of sets. In both cases, an over-approximation will help reduce the computational effort. Note that the overapproximation may also be piecewise, covering the boundary by a partitioning. While such a partitioned overapproximation may look superficially similar to a partitioning of the whole initial state set, please observe that in general it will be much smaller, as it does not cover the interior of the set.

Remark 3: If the initial set is not of full dimension, implying that the initial set's boundary coincides with the initial set itself, our boundary-based method can still help to reduce the computational burden in solving the RA problem: while the initial set is not full-dimensional, subsequent overapproximations presumably will be due to the wrapping effect. Once they get large, a shift to the boundary-based method may become worthwhile.

[2]If the parameter $\boldsymbol{w}_0\in\mathcal{W}$ varies over time, i.e., $\boldsymbol{w}_0$ is of the form $\boldsymbol{w}_0(t)$, then the solution mapping $\boldsymbol{\phi}(t;\boldsymbol{x}_0,t_0,\boldsymbol{w}_0)$ of the system (1) does not satisfy the semigroup property. This case will be investigated in our future work.

TABLE I
PERFORMANCE ILLUSTRATIONS

Ex.	O.T.M.E	time	O.T.M.B	time
1	5	23.90	2	1.93
2	≥ 5	> 5400	2	1132.05
3	7	5328.65	5	2123.31

Ex.	N.S.E.	time	N.S.B1	time	N.S.B2	time
3	128	6057.21	–	–	14	2123.31
4	81	13384.25	32	5344.02	20	1035.13

ALL TIMES ARE IN SECONDS. EX.: EXAMPLE, O.T.M.E.: ORDER OF TAYLOR MODELS BASED ON ENTIRE INITIAL SETS, O.T.M.B.: ORDER OF TAYLOR MODELS BASED ON INITIAL SETS' BOUNDARIES, N.S.E.: NUMBER OF EQUAL SIZED SUBSETS COVERING THE INITIAL SET, N.S.B1: NUMBER OF EQUAL SIZED SUBSETS OVER-APPROXIMATING THE INITIAL SET'S BOUNDARY, AS SHOWN IN RED IN FIG. 1, N.S.B2: NUMBER OF EQUAL SIZED SUBSETS COMPRISING THE INITIAL SET'S BOUNDARY, AS SHOWN IN GREEN IN FIG. 1. NOTE THAT IN THE COLUMNS TITLED 'N.S.B1' AND 'TIME', '-' MEANS THAT NO EXPERIMENTS ARE PERFORMED IN THIS CONTEXT.

TABLE II
FLOW* PARAMETERS FOR COMPUTATIONS

Ex.	S.S.	R.E.	P.D.	F.O.	C.F.	P.C.
1	0.01	0.1	QR	2, 5	10^{-15}	32
2	0.003	0.01	QR	2, 5	10^{-15}	32
3	0.01	0.01	identity	5,7	10^{-7}	32
4	0.01	10^{-4}	QR	4	10^{-15}	32

S.S.: STEP SIZE, R.E.: REMAINDER ESTIMATION, P.D.: PRECONDITION, F.O.: FIXED ORDERS, C.F.: CUTOFF, P.C.:PRECISION. NOTE THAT IN THE COLUMN TITLED 'F.O.', '2, 5' MEANS THAT TAYLOR MODELS OF ORDER 2 AND 5 ARE USED IN OUR BOUNDARY BASED METHOD AND THE ENTIRE INITIAL SET BASED TAYLOR MODEL METHOD RESPECTIVELY. THIS ALSO APPLIES TO '5, 7'. UNLIKE EXAMPLES 1–3, PARAMETER VALUES 'IDENTITY' AND '10^{-7}' FOR P. D. AND C. F. ARE USED RESPECTIVELY IN EXAMPLE 3 SINCE THE SYSTEM IN EXAMPLE 3 IS HIGH DIMENSIONAL AND THESE PARAMETER VALUES WILL HELP TO REDUCE THE COMPUTING TIME, COMPARED TO THE PARAMETER VALUES 'QR' AND '10^{-15}'.

IV. EXAMPLES AND DISCUSSIONS

In this section, we demonstrate our boundary-based method on six examples and discuss the findings. The implementation is based on the reachability analysis packages Flow* (Version 2.0.0) [15] and IOLAVaBE [13]. All computations were performed on an i5-3337U 1.8 GHz CPU with 4 GB RAM running Ubuntu Linux 13.10.

A. Examples

We illustrate the two aforementioned benefits of our boundary-based method in solving RA problems. The first benefit is reducing computational burden while maintaining accuracy, which is shown on Examples 1–4. The Examples 1–3 illustrate this by reducing the order of Taylor models necessary for obtaining a sufficiently tight enclosure, and Example 3 and 4 illustrate this by reducing the number of partitions used for controlling the wrapping effect by means of iterating small sets. The second important benefit is the flexibility gained in the geometric shapes of initial sets, which is the focus of Examples 5 and 6. The implementations in Examples 1–4 are based on the Taylor model package Flow*. The performance comparison between our boundary-based method and the entire initial set-based method can be found in Table I for these four examples. The corresponding Flow* parameters used for computations are presented in Table II. Examples 5 and 6 are based on the package IOLAVaBE.

Example 1: Consider the Brusselator studied in [14]

$$\begin{cases} \dot{x}_1 = A + x_1^2 x_2 - 1.5x_1 - x_1 \\ \dot{x}_2 = 1.5x_1 - x_1^2 x_2 \end{cases}$$

with $\mathcal{W}=\{A : A \in [1.0, 1.1]\}, \mathcal{X}=\mathbb{R}^2, \mathcal{X}_0 = [0.0, 1.0] \times [0.0, 1.0]$, $\mathcal{X}_{unsafe} = [1, 2] \times [4, 5]$, $\mathcal{X}_{goal} = [-0.1, 1.2] \times [0.2, 2.3]$, $t_0 = 0$, and $T = 1.52$.

Example 2: Consider a glucose-insulin system. As to how to derive its dynamic equations, please refer to the supplemental material

$$\begin{cases} \dot{G} = -(0.02649256301 + X)G + 0.02649256301 \times 90 \\ \dot{X} = -pX + 1.281692067 \times 10^{-5}(I - 7) \\ \dot{I} = -0.26973230345(I - 7) \end{cases},$$

with $\mathcal{W} = \{p : p \in [0.01843609572, 0.02543609572]\}$, $\mathcal{X}_0 = [275, 280] \times [0, 0.001] \times [490, 510]$, $\mathcal{X}_{unsafe} = \{(G, X, I) : G \leq 60\}$, $\mathcal{X} = \{(G, X, I) : G \geq 0, X \geq -0.001, I \geq 0\}$, $t_0 = 0$, $T = 180$ and $\mathcal{X}_{goal} = \{(G, X, I) : 79 \leq G \leq 110, -0.001 \leq X \leq 0.001, 6.99 \leq I \leq 7.01\}$.

Example 3: Consider a seven-dimensional biological system[3]

$$\begin{cases} \dot{x}_1 = -0.4x_1 + 5x_3x_4 \\ \dot{x}_2 = 0.4x_1 - x_2 \\ \dot{x}_3 = x_2 - 5x_3x_4 \\ \dot{x}_4 = 5x_5x_6 - 5x_3x_4 \\ \dot{x}_5 = -5x_5x_6 + 5x_3x_4 \\ \dot{x}_6 = wx_7 - 5x_5x_6 \\ \dot{x}_7 = -wx_7 + 5x_5x_6 \end{cases}$$

with $\mathcal{W} = \{w : w \in [0.49, 0.51]\}$, $\mathcal{X} = \mathbb{R}^7$, $\mathcal{X}_0 = [0.99, 1.01] \times [0.99, 1.01] \times [0.99, 1.01] \times [0.99, 1.01] \times [0.99, 1.01] \times [0.99, 1.01] \times [0.99, 1.01]$, $\mathcal{X}_{unsafe} = [3, 4] \times \ldots \times [3, 4]$, $\mathcal{X}_{goal} = [0.5, 3.5] \times [0.5, 1.5] \times [-0.5, 1.0] \times [-1, 3] \times [-1, 3] \times [-1, 1] \times [0, 1.5]$, $t_0 = 0$ and $T = 3.8$.

For Examples 1–3, subdivision operations for the initial sets and their boundaries are not taken into account. The numbers of subsets covering the initial set's boundary are, respectively, 4, 6, and 14 for these three examples[4], where each subset corresponds to $\{\boldsymbol{x} \in \mathcal{X}_0 : x_i = \underline{x}_i^0\}$ or $\{\boldsymbol{x} \in \mathcal{X}_0 : x_i = \overline{x}_i^0\}$, $i \in \{1, \ldots, n\}$, and $\mathcal{X}_0 = [\underline{x}_1^0, \overline{x}_1^0] \times \ldots \times [\underline{x}_n^0, \overline{x}_n^0]$. The RA problems in these three examples can be solved using our boundary-based method with Taylor models of order 2, 2, and 5, respectively. If the initial set is used for computations however, Taylor models of order 5 and 7 have to be used for Examples 1 and 3 respectively. For Example 2, even if we increase the order of the Taylor model to 5, the formulated RA problem cannot be solved after running the simulation for 5400 s. It is observed from Table I that our boundary-based method increases the efficiency of solving the RA problems by 1138%, 377% and 151% for these three examples respectively, compared to the entire initial set-based method implemented in Flow*.

Example 4: Consider the Van-der-Pol oscillator system,

$$\begin{cases} \dot{x} = y \\ \dot{y} = w(1 - x^2)y - x \end{cases}$$

[3]The model is from http://ths.rwth-aachen.de/research/hypro/biological-model-i/.

[4]Note that the number of subsets comprising an interval's boundary in an n-dimensional Euclidean space is $2n$.

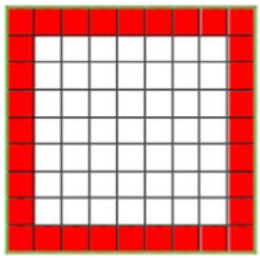

Fig. 1. Partitions for the Initial Set $\mathcal{X}_0$.

with $\mathcal{W} = \{w : w \in [0.99, 1.01]\}$, $\mathcal{X} = \mathbb{R}^2$, $\mathcal{X}_0 = [1.0, 1.5] \times [2.0, 2.5]$, $\mathcal{X}_{unsafe} = [-0.5, 0.5] \times [-0.5, 0.5]$, $\mathcal{X}_{goal} = [1, 2] \times [-1, 0]$, $t_0 = 0$, and $T = 15$.

For solving the RA problem in Example 4, subdividing either the initial set or its boundary has to be employed. Here we apply uniform subdivision techniques to the initial set and its boundary. Other subdivision techniques can also be applied to our computations. The corresponding minimum number of subdivisions and their computation times are presented in Table I. Thus it is observed that our boundary-based method increases the efficiency of solving the RA problem by 151% for this example, compared to the entire initial set-based method implemented in Flow*. Note that these improvements are obtained when boundaries are approximated using subsets as shown in red in Fig. 1. The improvement can be further enhanced if exact boundaries are used for computations, making our boundary-based method 1193% more efficient than the entire initial set-based method implemented in Flow*. We also investigate this benefit by applying the above subdivision operation to Example 3 based on the parameter inputs presented in Table II except the order of Taylor models used. The RA problem in Example 3 can be solved by applying Flow* to 2^7 equal-sized subdivisions covering the initial set. Since each subdivision is of smaller volume compared with the entire initial set, the corresponding minimal order of the used Taylor models is reduced to 4. In contrast, the problem can be solved by performing computations on only 14 subsets comprising the initial set's boundary using our boundary-based method, as mentioned previously. From Table I, we obtain that our boundary-based method increases the efficiency of solving this RA problem by 185%. Besides, we have applied the way of increasing the order of the used Taylor model to Example 4 using the same inputs listed in Table I except the order of the used Taylor models. For Example 4, both the entire initial set-based method and our boundary-based method cannot solve the RA problem with the Taylor model of order 12. For the the entire initial set-based method, Flow* cannot proceed past reachability time 9.82 with the computation time 23434.89 s. However, our boundary-based method with the Taylor model of order 6 can perform reachability analysis until the time instant 10.14 with the computation time 1170.96 s.

Example 5: Consider the system in Example 1 with $\mathcal{X}_0 = \{\boldsymbol{x} : -y \leq 0 \wedge -2x + y \leq -1.8 \wedge 2x + y \leq 2\}$, $\mathcal{W} = \{A : A \in [0.99, 1.01]\}$, $\mathcal{X}_{unsafe} = [2, 3] \times [2, 3]$, $\mathcal{X}_{goal} = [0.45, 0.55] \times [0.70, 0.90]$, $t_0 = 0$, and $T = 1$. Note that $\partial\mathcal{X}_0 = A_1 \cup A_2 \cup A_3$, where $A_1 = \{\boldsymbol{x} : \boldsymbol{x} = u_1 + s_1\alpha_1 | \alpha_1 \in \boldsymbol{\alpha}_1\}$, $A_2 = \{\boldsymbol{x} : \boldsymbol{x} = u_2 + s_2\alpha_2 | \alpha_2 \in \boldsymbol{\alpha}_2\}$, $A_3 = \{\boldsymbol{x} : \boldsymbol{x} = u_3 + s_3\alpha_3 | \alpha_3 \in \boldsymbol{\alpha}_3\}$, where $u_1 = \begin{pmatrix} 0.95 \\ 0 \end{pmatrix}$, $u_2 = \begin{pmatrix} 0.925 \\ 0.05 \end{pmatrix}$, $u_3 = \begin{pmatrix} 0.975 \\ 0.05 \end{pmatrix}$, $s_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $s_2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, $s_3 = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$, $\boldsymbol{\alpha}_1 = \begin{pmatrix} [-0.05\ 0.05] \\ [0\ 0] \end{pmatrix}$, $\boldsymbol{\alpha}_2 = \begin{pmatrix} [-0.025\ 0.025] \\ [0\ 0] \end{pmatrix}$ and $\boldsymbol{\alpha}_3 = \begin{pmatrix} [-0.025\ 0.025] \\ [0\ 0] \end{pmatrix}$.

Example 6: Consider the system in Example 3 with $\mathcal{W} = \{w : w \in [0.49, 0.51]\}$, $\mathcal{X} = \mathbb{R}^7$, $\mathcal{X}_{unsafe} = [3, 4] \times \ldots \times [3, 4]$, $\mathcal{X}_{goal} = [1.9, 2.1] \times [0.8, 0.9] \times [0.1, 0.3] \times [0.8, 1.1] \times [0.9, 1.2] \times [0.1, 0.3] \times [1.7, 1.9]$, $t_0 = 0$, $T = 0.8$, and $\mathcal{X}_0 = A_0 \bigcup \cup_{i=1}^{7}$

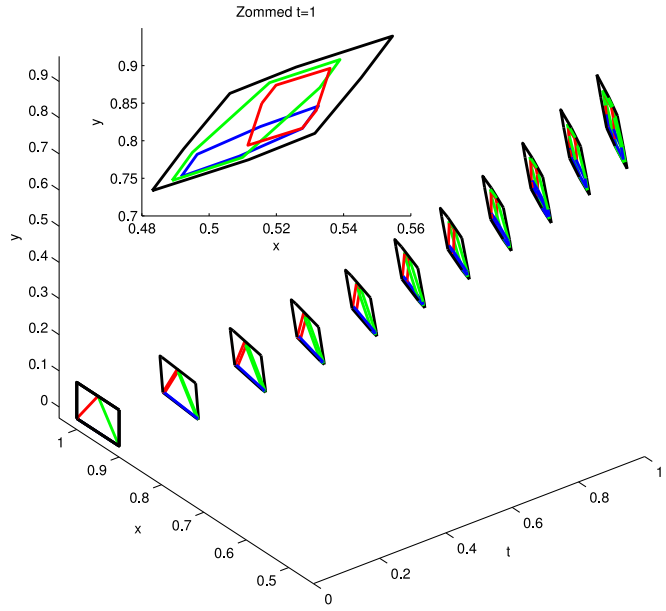

Fig. 2. Reachable sets obtained by the entire initial set-based method and our boundary-based method at time instants $t = 0, 0.1, \ldots, 1$.(Blue Region—Reachable sets of A_1; Green Region—Reachable sets of A_2; Red Region—Reachable sets of A_3; Black Region—Reachable sets of the interval hull $[0.9, 1] \times [0, 0.1]$ of $\mathcal{X}_0$.)

$\cup_{j=1, j\neq i}^{7} (A_{i,j} \cup B_{i,j} \cup C_{i,j} \cup D_{i,j})$, where $A_0 = \{\boldsymbol{x} : x_i \in [0.999, 1.001], i = 1, \ldots, 7\}$, $A_{i,j} = \{\boldsymbol{x} : x_i = 0.999, x_j \in [0.998, 0.999], x_k \in [0.999, 1.001], k = 1, \ldots, 7, k \neq i, k \neq j\}$, $B_{i,j} = \{\boldsymbol{x} : x_i = 0.999, x_j \in [1.001, 1.002], x_k \in [0.999, 1.001], k = 1, \ldots, 7, k \neq i, k \neq j\}$, $C_{i,j} = \{\boldsymbol{x} : x_i = 1.001, x_j \in [0.998, 0.999], x_k \in [0.999, 1.001], k = 1, \ldots, 7, k \neq i, k \neq j\}$, and $D_{i,j} = \{\boldsymbol{x} : x_i = 1.001, x_j \in [1.001, 1.002], x_k \in [0.999, 1.001], k = 1, \ldots, 7, k \neq i, k \neq j\}$. Note that $\partial\mathcal{X}_0 = \bigcup_{i=1}^{7}(E_i \cup F_i)$, where $E_i = \{\boldsymbol{x} : x_i = 0.999, x_j \in [0.998, 1.002], j = 1, \ldots, 7, j \neq i\}$, and $F_i = \{\boldsymbol{x} : x_i = 1.001, x_j \in [0.998, 1.002], j = 1, \ldots, 7, j \neq i\}$.

In Example 5, the initial set $\mathcal{X}_0$ is a triangle and its boundary is piecewise of the zonotope form. IOLAVaBE cannot deal with systems with initial sets represented by triangles, but can handle systems with initial sets represented by zonotopes. If we use the package IOLAVaBE combining the entire initial set method to solve the RA problem, an over-approximation of the initial set $\mathcal{X}_0$ has to be employed as an input, thus increasing the wrapping effect. Herein, we use the interval hull $[0.9, 1] \times [0, 0.1]$ of the set $\mathcal{X}_0$ to perform computations. The RA problem cannot be solved. However, the package can directly incorporate our boundary-based method without employing an over-approximation of the initial set's boundary. The RA problem can be solved successfully using our boundary-based method. All the above computations take few time, thus we do not present them here. The results produced by IOLAVaBE based on the entire initial set-based method and our boundary-based method are illustrated in Fig. 2 below. Note that the enlarged picture of the reachable set computed for $t = 1$ in Fig. 2 clearly demonstrates the additional flexibility in geometric shapes provided by our boundary-based method. According to Lemma 3, the simply connected compact set of the smallest volume, which encloses the reachable set of $\cup_{i=1}^{3} A_i$ at time instant $t = 1$, is an over-approximation of the reachable set of $\mathcal{X}_0$ at time instant $t = 1$. Our boundary-based method reduces the error in the construction of the reachable set at time instant $t = 1$ by about 38% as opposed to the entire initial set-based method. For this benefit, we will explore it further in our future work. For Example 6, the shape of the initial set $\mathcal{X}_0$ is very complicated.

The number of its elements is 169. However, the number of elements of $\partial\mathcal{X}_0$ is 14. The RA problem is solved based on the package IOLAVaBE combining our boundary-based method. The computation time is 1.81 s. However, the computation time is 16.73 s if all elements of the set $\mathcal{X}_0$ are applied. It is observed that our boundary-based method increases the efficiency of solving the RA problem by 824.31% for this example, compared to the entire initial set-based method.

B. Discussions

When the results returned by applying Taylor models to the entire initial are too pessimistic, either increasing orders of Taylor series expansions or splitting of the initial set into smaller subsets have to be used. For the former, the benefit of our boundary-based method is illustrated through Examples 1–3. It is observed that lower order Taylor models can be employed such that RA problems can be solved more efficiently, compared to the entire initial set-based method. The underlying reason is that the boundary is of smaller volume than the initial set, permitting lower order Taylor models to be employed for computations while still maintaining accuracy. Since the computational complexity of Taylor model methods increases exponentially with both the number of the state variables and the order of Taylor series expansion, our boundary-based method brings significant benefits by reducing computational loads in solving RA problems, especially for high dimensional problems. For the latter, i.e., splitting the initial set into smaller subsets, our boundary analysis will help to apply the Taylor model technique to subsets covering the initial set's boundary, thus reducing computational effort substantially in solving the RA problems. This benefit can be gained for any full dimensional compact initial set when subdivisions need to be employed for accuracy. Especially, since the exact boundary of an interval can be obtained, the computation burden can be reduced further if it is used for computations. This is illustrated in Example 4. Furthermore, regarding that the number of subsets comprising the interval initial set's boundary increases polynomially in the dimension, our boundary-based method is highly promising in improving the scalability of existing reachability analysis techniques dealing with cases with initial sets of the interval form such as Taylor model methods, as investigated through Example 3.

Further, most of the existing reachability analysis techniques for nonlinear systems are limited to systems with initial sets of states represented by a specific family of forms [20], e.g., intervals, zonotopes and polytopes. Our boundary-based method can help to generalize these techniques to deal with cases where only the initial set's boundary is restricted to the pertinent geometric shape. In Examples 5 and 6 we use the technique implemented in IOLAVaBE as an example to illustrate this. Under the assumption that the initial set is of full dimension, IOLAVaBE is confined to initial sets represented by zonotopes, which are obtained from linear transformations of intervals. However, our boundary-based method can help to extend the technique implemented in IOLAVaBE to deal with initial sets of more general forms, as illustrated in Examples 5 and 6.

V. Conclusion

The boundary-based approach to computing reachable sets proposed in this article offers two benefits when computing reachable sets or, more generally, solving reach-avoid problems of nonlinear dynamical systems: first, it helps fight the wrapping effect by applying state extrapolation to sets of smaller volume. The consequence is that the same accuracy in computing reach sets can be obtained with considerably lower computational effort, as higher-order Taylor enclosures or fine-granular partitions of state sets can be avoided. Second, it alleviates the restriction of existing reachability-analysis techniques to confined geometric representations of reachable sets by enabling their application to considerably more complex geometric shapes, where the boundary of the set is representable as a finite union of such shapes.

Acknowledgement

The authors are grateful to M. Althoff and S. Steinhorst from TU Munich for helpful discussions, and to X. Chen from RWTH Aachen for support with Flow*. Moreover, the authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the technical note.

References

[1] A. Girard, "Reachability of uncertain linear systems using zonotopes," in *Proc. ACM Int. Conf. Hybrid Systems: Computation and Control (HSCC)*, pp. 291–305, 2005.
[2] M. Althoff, O. Stursberg and M. Buss, "Reachability analysis of nonlinear systems with uncertain parameters using conservative linearization," in *Proc. IEEE Conf. Decision and Control (CDC)*, pp. 4042–4048, 2008.
[3] L. Benvenuti, D. Bresolin, A. Casagrande, P. Collins, A. Ferrari, E. Mazzi, A. Sangiovanni-Vincentelli and T. Villa, "Reachability computation for hybrid systems with Ariadne," in *Proc. Int. Fed. Autom. Control (IFAC)*, pp. 8960–8965, 2008.
[4] A. Chutinan and B. H. Krogh, "Computational techniques for hybrid system verification," *IEEE Trans. Autom. Control*, vol. 48, no. 1, pp. 64–75, 2003.
[5] E. Asarin, T. Dang and A. Girard, "Reachability analysis of nonlinear systems using conservative approximation," in *Proc. ACM Int. Conf. Hybrid Systems: Computation and Control (HSCC)*, pp. 20–35, 2003.
[6] O. Stursberg and B. H. Krogh, "Efficient representation and computation of reachable sets for hybrid systems," in *Proc. ACM Int. Conf. Hybrid Systems: Computation and Control (HSCC)*, pp. 482–497, 2003.
[7] A. Kurzhanski and P. Varaiya, "Ellipsoidal techniques for reachability analysis," in *Proc. ACM Int. Conf. Hybrid Systems: Computation and Control (HSCC)*, pp. 202–214, 2000.
[8] J. Lunze and F. Lamnabhi-Lagarrigue, editors. *Handbook of Hybrid Systems Control: Theory, Tools, Applications*. Cambridge, U.K.:Cambridge University Press, 2009.
[9] T. Dang, O. Maler and R. Testylier, "Accurate hybridization of nonlinear systems," in *Proc. ACM Int. Conf. Hybrid Systems: Computation and Control (HSCC)*, pp. 11–20, 2010.
[10] C. J. Tomlin, J. Lygeros and S. S. Sastry, "A game theoretic approach to controller design for hybrid systems," *Proc. IEEE*, vol. 88, no. 7, pp. 949–970, 2000.
[11] I. M. Mitchell, A. M. Bayen and C. J. Tomlin, "A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamics games," *IEEE Trans. Autom. Control*, vol. 50, no. 7, pp. 947–957, 2005.
[12] N. Ramdani, N. Meslem and Y. Candau, "A hybrid bounding method for computing an over-approximation for the reachable set of uncertain nonlinear systems," *IEEE Trans. Autom. Control*vol. 54, pp. 2352–2364, 2009.
[13] A. Eggers, N. Ramdani, N. Nedialkov and M. Fränzle, "Improving the SAT modulo ODE approach to hybrid systems analysis by combining different enclosure methods," *Software & Syst. Model.*, pp. 1–28, 2012.
[14] X. Chen, E. Ábrahám and S. Sankaranarayanan, "Taylor model flowpipe construction for non-linear hybrid systems," in *Proc. IEEE Real-Time Systems Symp. (RTSS)*, pp. 183–192, 2012.
[15] X. Chen, E. Abraham and S. Sankaranarayanan, "FLOW*: An analyzer for non-linear hybrid systems," in *Proc. Int. Conf. Computer-Aided Verification*, pp. 258–263, 2013.
[16] B. Mendelson, *Introduction to Topology: 3rd Edition*. Chelmsford, MA: Courier Corporation, pp. 112, Apr. 26, 2012.
[17] W. S. Massey, *A Basic Course in Algebraic Topology*. Springer Science & Business Media, p. 216, 1991.
[18] I. Kriz and A. Pultr. *Introduction to Mathematical Analysis*. New York: Springer, p. 49, 2013.
[19] N. S. Nedialkov, *VNODE-LP: A Validated Solver for Initial Value Problems in Ordinary Differential Equations*. Tech. Rep. TR CAS-06-06-NN, Mc-Master University, , Hamilton, ON, Canada, 2006.
[20] M. Clark, X. Koutsoukos, R. Kumar, I. Lee, G. Pappas, L. Pike, J. Porter and O. Sokolsky, *A Study on Run Time Assurance for Complex Cyber Physical Systems*. Tech. Rep., Air Force Research Lab, Wright-Patterson AFB, OH, 2013.