Under-approximate Flowpipes for Non-linear Continuous Systems

Xin Chen
RWTH Aachen University, Germany
xin.chen@cs.rwth-aachen.de

Sriram Sankaranarayanan
University of Colorado, Boulder, CO
srirams@colorado.edu

Erika Ábrahám
RWTH Aachen University, Germany
abraham@cs.rwth-aachen.de

***Abstract*—We propose an approach for computing under- as well as over-approximations for the reachable sets of continuous systems which are defined by non-linear Ordinary Differential Equations (ODEs). Given a compact and connected initial set of states, described by a system of polynomial inequalities, we compute under-approximations of the set of states reachable over time. Our approach is based on a simple yet elegant technique to obtain an accurate Taylor model over-approximation for a backward flowmap based on well-known techniques to over-approximate the forward map. Next, we show that this over-approximation can be used to yield both over- and under-approximations for the forward reachable sets. Based on the result, we are able to conclude "may" as well as "must" reachability to prove properties or conclude the existence of counterexamples. A prototype of the approach is implemented and its performance is evaluated over a reasonable number of benchmarks.**

I. Introduction

In this paper, we present an approach for computing under-approximations of the reachable sets of continuous systems described by ODEs. Continuous systems arise in a variety of domains including biological systems, control systems and aggregate mean field models of parameterized systems. Computing over-approximations of the reachable set of discrete, continuous and hybrid systems is a fundamental primitive for verifying safety properties. There has been much progress towards reachable set over-approximations for linear as well as non-linear continuous or hybrid systems through the use of invariant computation [1], [2], [3], conservative abstraction on dynamics [4], [5], [6], flowpipe construction [7], [8], [9], [10], [11], level sets [12], [13], [14], and advanced interval arithmetic techniques [15], [16], [17], [18], [19]. However, less attention has been given to the problem of finding reachable set under-approximations.

Whereas over-approximations represent states that "may" be reachable, under-approximations characterize states that "must" be reachable. As a result, under-approximations can be used to show that the system must reach a given target (or unsafe) set. The presence of under- as well as over-approximations can help us prove "reach-while-avoid" properties that are common in many control systems: the system must reach a specified target set of states, while avoiding a set of unsafe states. Under-approximations also help us judge the quality of related over-approximations by comparing the states that "may" be reachable with the states that "must" be reachable. Besides, under-approximation techniques are also crucial in finding counterexamples for continuous and hybrid systems, and could be extended to carry out Counterexample-Guided Abstraction Refinement (CEGAR) for these systems [20].

Our approach in this paper is based on the use of Taylor Model-based techniques that have been used for over-approximations [16], [19]. Starting from a given ODE $\dot{\vec{x}} = f(\vec{x})$ and an initial set X_0 defined by polynomial inequalities, we seek to derive an under-approximation Ω_t of the reachable set X_t at time $t > 0$. The basic idea for deriving an under-approximation starts by first deriving an *over-approximate backward flowmap* Φ that maps a state $\vec{x}_t \in \Omega_t$ potentially reachable at time t to a set of possible initial states $\Phi(\vec{x}_t)$. This can be seen (roughly) as an over-approximate pre-condition of the state $\vec{x}_t$. Next, we prove that a topologically connected set Ω_t which does not intersect the boundary of X_t is an under-approximation of it, if $\Phi(\vec{x}) \subseteq X_0$ for some $\vec{x} \in \Omega_t$. The condition of topological connctedness is an important technicality that must be checked for a set Ω_t before it can be identified as an under-approximation. Our approach integrates interval arithmetic approaches using higher order Taylor models [16], [19] with techniques from computational topology for proving connectedness [21]. The contributions of this paper are summarized as follows:

1) We show how Taylor model arithmetic can be used to over-approximate a backward flowmap (in addition to the forward flowmap). A key feature of our approach is that we mostly reuse the calculations for the forward map to also derive the backward map, using the structure of the Lagrange remainder in the Taylor series expansion.

2) We use the *Taylor model backward flowmap* to construct under-approximations. In doing so, it becomes necessary to prove that a set implicitly defined by polynomial inequalities is connected. We prove the property of *star-connectedness* through repeated satisfiability checks.

3) Finally, we have implemented our approach based on the computational library of Flow* [22]. We provide experimental evaluation on a set of interesting and challenging benchmarks.

A. Related Work

As mentioned earlier, a significant volume of work has been devoted to the problem of finding over-approximations of the reachable states of continuous systems. Surprisingly, very little work has been focused on under-approximations. The main reason is the hardness of the task.

ISBN: 978-0-9835678-4-4.

Several techniques of under-approximating reachable sets are introduced in [23], [24] for the systems defined by linear ODEs. However, they can not be easily extended to handle non-linear systems which are most often found in applications.

The idea of using over-approximations of backward flowmaps to compute reachable set under-approximations has been discussed elsewhere [25], [26]. Nevertheless, very few existing methods or tools can handle the job efficiently. We propose a more applicable method based on TM representations and does not require splitting the state space too often.

Under-approximation techniques have also received attention from the interval analysis community. The technique of modal (Kaucher) intervals provides a framework for under-approximations using intervals [27]. This was used to provide under-approximations of reachable sets for programs by Goubault et al. [28]. The recent work of Goubault et al. uses modal intervals with affine forms to provide under-approximations for the reachable sets of continuous systems [29]. In contrast, our approach relies on Taylor model based over-approximations, but of the backward flowmap rather than the forward map. Therefore, we are able to provide a higher-order technique for generating under-approximations in contrast to the first order approach of Goubault et al. using affine forms. Given the very recent nature of Goubault et al.'s contribution, we are unable to provide an experimental comparison of our techniques. However, a detailed comparison is planned as part of our extended version, in the future.

The work of Bai Xue and Zhikun She is yet another important contribution to the problem of under-approximating reachable sets of continuous systems, that inspired our approach in this paper [30]. Their approach is similar to ours in the use of backward flowmaps to compute under-approximations. A key difference, however is that Xue and She use an over-approximation of the boundary of the reachable set to find under-approximations. In our experience, the boundary of these sets if often complex and requires a fine subdivision of the state-space. Our approach, in comparison, avoids gridding the boundary. Instead, we are left with the problem of proving topological connectedness of a set, which is also hard in practice. Furthermore, the modification of Taylor models to compute backward flowmap over-approximations is a unique contribution of this paper.

Recently, Gao et al. presented a relaxed notion of δ-satisfiability to build constraint solvers for non-linear real arithmetic [31]. δ-satisfiability argues that a formula is unsatisfiable, or a δ-perturbation of it is satisfiable. By adjusting δ, the approach handles complex formulae involving real functions such as the flowmaps of ODEs. It has been implemented in the constraint solver dReal [32], and the tool dReach focusing on the analysis of non-linear systems [33]. Our approach has many fundamental differences: dReach attempts to answer a single reachability query using constraint solving, whereas our approach builds representations for reachable set segments that can be used to answer more complex queries. Our approach finds guaranteed over- and under-approximations, but does not reason about perturbations. Finally, the approach presented here can be a primitive inside a tool such as dReach, providing a more powerful approach to reachability analysis.

II. Preliminaries

Let $\mathbb{R}$ denote the set of real values. A set of variables $x_1, \ldots, x_n$, is collectively written as a vector $\vec{x}$. For a vector $\vec{x}$, we use x_i to denote its i-th component. Let $\mathbb{I}$ denote the set of all intervals $I = [a, b] \subseteq \mathbb{R}$ with $a, b \in \mathbb{R}$ and $a \leq b$. Multi-dimensional intervals are Cartesian products of intervals, and we continue to call them *intervals* in the paper. Given a variable or function $x(t)$ of time, we use $\dot{x}$ to denote the time derivative of x. Given a set S, we use $\mathtt{Int}(S)$ to denote the smallest interval enclosure of S.

Definition 1 (Continuous system)**.** *An n-dimensional* continuous system $\mathcal{S}$ *is defined by an ODE $\dot{\vec{x}} = f(\vec{x})$, wherein $\vec{x}$ is a $n \times 1$ vector of* state variables *and the function f denotes the* vector field *which associates each state $\vec{c} \in \mathbb{R}^n$ a derivative vector $f(\vec{c}) \in \mathbb{R}^n$.*

Executions of a continuous system $\mathcal{S}$ correspond to the time trajectories of the ODE. We assume that the function f defining the ODE is (locally) Lipschitz continuous in $\mathbb{R}^n$. This guarantees that for each $\vec{x}_0 \in \mathbb{R}^n$, there exists a unique solution $\vec{x}(t)$ defined over some interval of existence $(-T(\vec{x}_0), T(\vec{x}_0))$, with initial condition $\vec{x}(0) = \vec{x}_0 \in \mathbb{R}^n$ [34]. Here $(-T(\vec{x}_0), T(\vec{x}_0))$ is the interval of existence and depends, in general, on the initial condition $\vec{x}_0$. We denote the value $\vec{x}(t)$ for any time $t \in (-T(\vec{x}_0), T(\vec{x}_0))$ by $\varphi_f(\vec{x}_0, t)$. We assume that for the models considered in this paper, the solutions exist for $T(\vec{x}_0) > T$, where T is a time horizon of interest. The function $\varphi_f(\vec{x}_0, t)$ is also called the *flowmap* which is *forward* if $t \geq 0$, and *backward* otherwise. In the rest of the paper, we assume that the dynamics $f(\vec{x})$ are given by a multivariate polynomial over $\vec{x}$.

The reachable set of a continuous system defined by $\dot{\vec{x}} = f(\vec{x})$ from an initial set $X_0 \subseteq \mathbb{R}^n$ is the set of flows $\{\varphi_f(\vec{x}_0, t) \,|\, \vec{x}_0 \in X_0\}$. For simplicity, we denote it by $\varphi_f(X_0, t)$ if $\varphi_f(\vec{x}_0, t)$ exists for all $\vec{x}_0 \in X_0$ in the time interval of interest. Given a time interval $\Delta \in \mathbb{I}$, the image of the map $\varphi_f(X_0, t)$ with $t \in \Delta$, is called a *flowpipe*.

Since we assume Lipschitz continuous ODEs, the map from $\vec{x}_0 \in X_0$ to $\varphi_f(\vec{x}_0, t)$ is *bijective*. Ideally, we wish to compute the map φ_f by solving the given ODE analytically. However, this cannot be done exactly, since most of the ODEs do not have closed form solutions. A typical approach is to approximate a solution by a Taylor polynomial which can be computed based on the higher-order Lie derivatives of the vector field. We will address it in Sect. IV.

Definition 2 (Lie derivative)**.** *Given an ODE $\dot{\vec{x}} = f(\vec{x})$ with n variables, the* Lie derivative *of a differentiable function $g(\vec{x}, t)$ w.r.t. f is defined by*

$$\mathcal{L}_f(g) = \sum_{i=1}^{n} \left(\frac{\partial g}{\partial x_i} \cdot f_i \right) + \frac{\partial g}{\partial t}$$

wherein f_i denotes the i-th component of f. If g is k times differentiable, the higher-order Lie derivatives of it are defined

ISBN: 978-0-9835678-4-4.

recursively by

$$\mathcal{L}_f^{m+1}(g) = \mathcal{L}_f(\mathcal{L}_f^m(g)) \ \ for \ \ m = 1, 2, \ldots, k-1$$

In the rest of the section, we give a brief introduction of Taylor models (TMs). TMs were introduced by Berz and Makino to provide a framework for constructing high-order over-approximations of continuous functions as well as common operations over them. They are described in detail elsewhere [35]. A *Taylor model (TM)* is denoted by a pair (p, I) such that p is a polynomial over a closed and bounded domain and I is an interval which represents a remainder. Given a function $f(\vec{x})$ over D, we say that it is over-approximated by the TM $(p(\vec{x}), I)$ if $f(\vec{x}) \in p(\vec{x}) + I$ for all $\vec{x} \in D$. Intuitively, the TM maps any $\vec{x} \in D$ to an interval which contains $f(\vec{x})$. In the paper, we always use TM to mean a TM over-approximation.

TMs are closed under arithmetic operations of addition, scaling, multiplication and integration. The arithmetic over TMs can be viewed as a higher-order *interval arithmetic* [36]. Given two intervals $[a_1, b_1], [a_2, b_2] \in \mathbb{I}$, their sum and product are defined by $[a_1, b_1] + [a_2, b_2] = [a_1 + a_2, b_1 + b_2]$ and $[a_1, b_1] \cdot [a_2, b_2] = [\min\{a_1 \cdot a_2, a_1 \cdot b_2, b_1 \cdot a_2, b_1 \cdot b_2\}, \max\{a_1 \cdot a_2, a_1 \cdot b_2, b_1 \cdot a_2, b_1 \cdot b_2\}$ respectively. Then for two functions f, g over the same domain, if their TMs are given by (p_1, I_1), (p_2, I_2) respectively, a TM for $f + g$ can be computed by directly adding the polynomial and remainder part respectively, i.e., $(p_1 + p_2, I_1 + I_2)$, while an order k TM for their product $f \cdot g$ can be computed by

$$(\, p_1 \cdot p_2 - r_k\, ,\ I_1 \cdot B(P_2) + I_2 \cdot B(P_1) + I_1 \cdot I_2 + B(r_k)\,)$$

wherein $B(p)$ denotes an interval enclosure of the range of p, and the *truncated part* r_k consists of the terms in $p_1 \cdot p_2$ of degrees $> k$. By TM arithmetic, we may compute an over-approximation for a complex function based on the TMs of its components.

TMs can be applied to provide over-approximations for flowpipes. They serve a dual purpose: they are used to conservatively approximate the *flowmap* $\varphi_f(\vec{x}_0, t)$ by a TM (p, I) for some $\vec{x}_0 \in X_0$ and $t \in \Delta \in \mathbb{I}$, such that

$$\forall \vec{x}_0 \in X_0,\ \forall t \in \Delta,\ \varphi_f(\vec{x}_0, t) \in p(\vec{x}_0, t) + I$$

They also serve as implicit definition of the flowpipe that over-approximates the image of φ_f over the set $\vec{x}_0 \in X_0$ and $t \in \Delta$. That is, a flowpipe $\varphi_f(X_0, t)$ for some $X_0 \subseteq \mathbb{R}^n$ and $t \in \Delta \in \mathbb{I}$ can be over-approximated by a TM $(p(\vec{x}_0, t), I)$ with $\vec{x}_0 \in X_0$ and $t \in \Delta$. Such a TM is also called a *TM flowpipe*, its computation is presented in Sect. IV.

III. Under-approximation technique at a glance

In this section, we present a brief sketch of our over- and under-approximate flowpipe computation technique. This section will serve to motivate the description of our approach through the rest of this paper.

Given a Lipschitz continuous ODE $\dot{\vec{x}} = f(\vec{x})$ and a compact and connected initial set X_0. We want to compute an under-approximation for the flowpipe $X_t : \varphi_f(X_0, t)$ with $t \in \Delta$ for some small time interval Δ. To do so, we seek to compute a set $\mathfrak{F}_t$ which *strictly* contains ∂X_t, i.e., the boundary of X_t. Since X_t is still compact and connected (see [34]), we may conclude that a connected set Ω_t which does not intersect ∂X_t is an under-approximation of X_t if Ω_t contains some state in X_t. To ensure these properties, we could (i) prove that Ω_t does not intersect $\mathfrak{F}_t$, and (ii) find a state in $\Omega_t \cap X_t$. An illustration is presented in Figure 1.

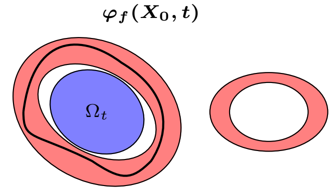


Fig. 1. Illustration of the main idea. The red region denotes the boundary over-approximation $\mathfrak{F}_t$, which is computed as a system of polynomial inequalities and could be disconnected.

It will be shown that a backward flowmap over-approximation plays a key role in achieving both (i) and (ii). In Sect. IV, we show how such an over-approximation can be effectively derived as a TM (p_b, I_b). The computation of $\mathfrak{F}_t$ based on (p_b, I_b) is described in Sect. V, where we also give a method to verify a reachable state by using (p_b, I_b).

IV. TMs for forward and backward flowmaps

In the section, we introduce a modified TM flowpipe construction approach which is an extention of our previous work [19]. A key feature of it is the derivation of a TM that approximates the backward flowmap by reusing the calculations for the forward map.

A. Modified TM flowpipe construction

Given an n-dimensional continuous system defined by $\dot{\vec{x}} = f(\vec{x})$, and a time step δ, the reachable set for a bounded time horizon $[0, T]$ and an initial set $X_0 \subseteq \mathbb{R}^n$ is over-approximated by a finite sequence of TMs $\mathcal{F}_1, \ldots, \mathcal{F}_N$, wherein $N = \lceil \frac{T}{\delta} \rceil$. For all $1 \leq i \leq N$, $\mathcal{F}_i$ over-approximates the image $\varphi_f(X_0, t)$ with $t \in [(i-1)\delta, i\delta]$. The TMs are computed iteratively, such that the segment $\mathcal{F}_i$ is used to compute the initial set for the subsequent TM. In the i-th iteration, we assume that the local initial set is given by a TM X_l. The i-th TM flowpipe $\mathcal{F}_i$ is computed by the following two steps.

Step 1: Compute a Taylor polynomial p_f for the forward flow $\varphi_f(X_l, t)$ up to order k in t. The polynomial p_f can be derived as the following Taylor polynomial of $\varphi_f(X_l, t)$,

$$p_f(\vec{x}_l, t) = \vec{x}_l + \mathcal{L}_f(\vec{x}_l) \cdot t + \cdots + \mathcal{L}_f^k(\vec{x}_l) \cdot \frac{t^k}{k!} \qquad (1)$$

wherein $\vec{x}_l \in X_l$ and we simply denote $\mathcal{L}_f^j(\vec{x})|_{\vec{x}=\vec{x}_l}$ by $\mathcal{L}_f^j(\vec{x}_l)$ for $1 \leq j \leq k$. Unlike our previous work, the degrees of $\vec{x}_l$ in p_f are not limited.

Step 2: Evaluate a safe remainder interval I_f for p_f over $t \in [0, \delta]$. The purpose is to find an interval I_f such that

ISBN: 978-0-9835678-4-4. Copyright owned jointly by the authors and FMCAD Inc.

the TM $(p_f(\vec{x}_l,t),I_f)$ is an over-approximation of $\varphi_f(\vec{x}_l,t)$ over $\vec{x}_l \in X_l$ and $t \in [0,\delta]$. As we have the assumption that f is at least locally Lipschitz continuous, then an interval I_f is sufficient (or safe) if the *Picard operator*

$$\mathbb{P}_f(g)(\vec{x}_l,t) = \vec{x}_l + \int_0^t f(g(\vec{x}_l,s))\ ds \tag{2}$$

is *contractive* over (p_f,I_f) (see [16], [19]). To find such an interval, we may start with an estimation I_e which could be incorrect, and then conservatively check the contractiveness of the Picard operation by means of TM arithmetic. If it can not be verified, we enlarge the interval I_e until we obtain a contractive interval. The resulting interval I_e may be further refined by repeatedly performing the Picard operation on (p_f,I_e). We then set $I_f = I_e$. Unlike previous work, we only truncate the polynomial terms whose degrees of t are larger than k. Afterwards, if $i > 1$, the TM $\mathcal{F}_i$ can be derived by substituting X_l in the place of $\vec{x}_l$ in (p_f,I_f) by TM arithmetic, otherwise it is the first iteration and we simply rename $\vec{x}_l$ by $\vec{x}_0$.

B. Compute over-approximations for backward flowmaps

The flowpipe construction presented thus far only produces a TM that over-approximates the forward flowmap from X_0 to X_t : $\varphi_f(X_0,t)$ for $t \in [0,T]$, and the under-approximation approach requires over-approximations for the backward flowmaps.

Even though the backward flowmap is conceptually obtained by negating the time variable, a TM over-approximation for the backward flowmap is not easy to obtain. A simple way to do that is performing a backward flowpipe computation from an over-approximation of X_t which is obtained by a forward one. However, it is not only time consuming but also inaccurate, since the overestimation generated in the forward computation is also considered in estimating the remainder intervals for the backward flowmaps by the Picard operation. Thus, we need a method to obtain backward over-approximations without using flowpipe construction.

We introduce a novel method to generate accurate backward over-approximations by reusing the calculation of the forward modified TM flowpipe construction. Let us fix a time $t \geq 0$ and consider the initial set X_l for the i-th step of the forward flowpipe construction. Let us denote $Y_l(t) = \varphi_f(X_l,t)$, as the image of the forward flowmap for any $t \in [0,\delta]$. We assume that φ_f is over-approximated by a TM $(p_f(\vec{x}_l,t),I_f)$, wherein $\vec{x}_l \in X_l$. Our goal is to construct a TM (p_b,I_b) that over-approximates the flowmap from Y_l back to X_l.

Constructing p_b It is easy to see that while $\varphi_f(\vec{x}_0,t)$ for $\vec{x}_0 \in X_0, t \geq 0$ represents the forward map, the backward map is represented by $\varphi(\vec{y}_0,-t)$ where $\vec{y}_0 \in \varphi_f(X_0,t), t \geq 0$. Therefore, its Taylor expansion is related to that of $\varphi(\vec{x}_0,t)$ when $t \geq 0$. Using this observation, the polynomial p_b is derived from p_f by syntactically replacing $\vec{x}_l$, the variables denoting the starting state, by $\vec{y}_l$, the variables denoting the ending state. Likewise, we replace the time variable t by $-t$. The renaming of $\vec{x}_l$ is not technically necessary, we do it to distinguish the domains of the TMs for forward and backward

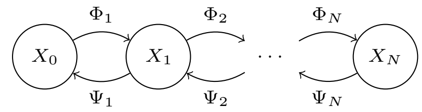


Fig. 2. Flowmap automaton

flowmaps. The challenge remains to construct the remainder interval I_b. In doing so, we wish to avoid computing Picard operation by TM arithmetic which could potentially introduce a large overestimation.

The Lagrange remainder term of p_f at some $\vec{x}_l \in X_l$ and $t \in [0,\delta]$ is

$$\varepsilon(\vec{x}_l,t) = \frac{1}{(k+1)!}\mathcal{L}_f^{k+1}(\varphi_f(\vec{x}_l,\xi)) \cdot t^{k+1} \tag{3}$$

wherein ξ is between 0 and t. Then an interval enclosure $\mathcal{E}(X_l,[0,\delta])$ of all $\varepsilon(\vec{x}_l,t)$ over $\vec{x}_l \in X_l$ and $t \in [0,\delta]$ can be evaluated as

$$\frac{1}{(k{+}1)!}\mathcal{L}_f^{k+1}(\mathtt{Int}(\{\varphi_f(\vec{x}_l,\xi)|\vec{x}_l \in X_l, \xi \in [0,\delta]\}))\cdot([0,\delta])^{k+1}$$

Similarly, since the remainder term for p_b at some $\vec{y}_l \in Y_l(t)$ and $t \in [0,\delta]$ can be expressed by $\varepsilon(\vec{y}_l,-t)$ such that ξ is between 0 and $-t$. An interval enclosure of those remainders over $\vec{y}_l \in Y_l(t)$ and $t \in [0,\delta]$ could be obtained as $\mathcal{E}(Y_l(\delta),[-\delta,0])$. By Lemma 3, we have that $\mathcal{E}(Y_l(\delta),[-\delta,0]) = (-1)^{k+1} \cdot \mathcal{E}(X_l,[0,\delta])$. In other words, I_b can be computed as an interval enclosure of $(-1)^{k+1} \cdot \mathcal{E}(X_l,[0,\delta])$.

Lemma 3. *For an order* $k \geq 0$ *and a time interval* $[0,\delta]$*, we have that*

$$\mathcal{E}(Y_l(\delta),[-\delta,0]) = (-1)^{k+1} \cdot \mathcal{E}(X_l,[0,\delta])$$

Although the interval $\mathtt{Int}(\{\varphi_f(\vec{x}_l,\xi)\,|\,\vec{x}_l \in X_l, \xi \in [0,\delta]\})$ is hard to compute, we may obtain an interval enclosure $I_{\vec{x}}$ for it from an interval evaluation of $\mathcal{F}_i$, and hence

$$I_\varepsilon = \frac{1}{(k+1)!}\mathcal{L}_f^{k+1}(I_{\vec{x}}) \cdot ([0,\delta])^{k+1} \tag{4}$$

is an interval enclosure of $\mathcal{E}(X_l,[0,\delta])$. At last, we have the safe remainder interval $I_b = (-1)^{k+1} \cdot I_\varepsilon$.

Notice that I_b is sufficiently large for any point in $(p_f(\vec{x}_l,t),I_f)$ with $\vec{x}_l \in X_l$, $t \in [0,\delta]$, i.e., $\mathcal{F}_i$. In other words, for any point $\vec{y}_l \in (p_f(\vec{x}_l,t),I_f)$, $(p_b(\vec{y}_l,t),I_b)$ defines an over-approximation for the backward map $\varphi_f((p_f(\vec{x}_l,t),I_f),-t)$. The reason is that I_ε is computed based on the over-approximation $\mathcal{F}_i$.

The TMs of the forward and backward flowmaps computed in all time steps can be organized as an automaton shown in Fig.2. For $1 \leq i \leq N$, the state X_i denotes the exact reachable set $\varphi_f(X_0,i\delta)$. The forward edge $\Phi_i(\vec{x}_l,t)$ denotes the forward TM $(p_f(\vec{x}_l,t),I_f)$ in the i-th time step, while the backward edge $\Psi_i(\vec{y}_l,t)$ is the backward TM $(p_b(\vec{y}_l,t),I_b)$ there. When we take $t = \delta$, they are over-approximations of the maps between the states. Then for any $\tau \in [0,T]$, an order k TM for the backward map from $\varphi_f(X_0,\tau)$ to X_0

ISBN: 978-0-9835678-4-4.

can be obtained by composing the TMs along the path from X_i to X_0 such that $\tau \in [(i-1)\delta, i\delta]$. It can be done by Algorithm 1. In the TM computation, we take the TM flowpipe $\mathcal{F}_i$ with $t = \tau - (i-1)\delta$ as the range of $\vec{y}_l$. To achieve a good accuracy, some preconditioning techniques proposed for intervals [37] and TMs [38] can be applied. Additionally, we may also consider the case that τ ranges in a time interval by taking an additional variable t.

Algorithm 1 Composing TMs for backward flows

```
Π ← Ψ_i(y_l, τ − (i − 1)δ);          # by TM arithmetic
for all j = i − 1 to 1 do
    Π ← Ψ_j(Π, δ);                    # by TM arithmetic
end for
return Π;
```

V. Under-approximation generation

In the section, we show how flowpipe under-approximations can be generated based on the TMs of backward flowmaps.

A. Main theorem

Given an n-dimensional continuous system defined by $\dot{\vec{x}} = f(\vec{x})$. If the initial set is defined by $X_0 = \{\vec{x} \in \mathbb{R}^n \mid \bigwedge_{i=1}^{m}(p_i(\vec{x}) \le 0)\}$ which is *compact* and *connected*, then the reachable set at time $t \ge 0$ can be characterized by

$$\varphi_f(X_0, t) = \{\vec{x} \in \mathbb{R}^n \mid \bigwedge_{i=1}^{m}(p_i(\varphi_f(\vec{x}, -t)) \le 0)\} \tag{5}$$

which is also compact and connected (see [34]). Intuitively, a state $\vec{x}$ is in $\varphi_f(X_0, t)$ iff the backward flow maps it to a state in X_0 at time $-t$. We present an example in Fig. 3 to show such evolution of a constraint. Given a time point $t = \tau$, if $(p_b(\vec{x}), I_b)$ is a TM for the backward flowmap from $\varphi_f(X_0, \tau)$ to X_0, then we may compute an order k TM $(\phi_i(\vec{x}), [\ell_i, v_i])$ for $p_i(\varphi_f(\vec{x}, -\tau))$ from evaluating $p_i((p_b(\vec{x}), I_b))$ by TM arithmetic for all $1 \le i \le m$. Such a TM of the backward flowmap as well as a TM $\mathcal{F}$ of $\varphi_f(X_0, \tau)$ can be obtained using the forward as well as backward flowmap computation presented in Sect. IV by taking a TM of X_0. Then the constrained flowpipe $\mathcal{F}_o = \{\vec{x} \in \mathcal{F} \mid \bigwedge_{i=1}^{m}(\phi_i(\vec{x}) + \ell_i \le 0)\}$ defines a refined over-approximation of the reachable set $\varphi_f(X_0, \tau)$ since $\mathcal{F}$ is derived based on a TM of X_0, while an under-approximation of $\varphi_f(X_0, \tau)$ can be computed as a *connected* subset Ω of $\mathcal{F}_u = \{\vec{x} \in I_{\mathcal{F}} \mid \bigwedge_{i=1}^{m}(\phi_i(\vec{x}) + u_i \le 0)\}$ wherein $I_{\mathcal{F}}$ is an interval enclosure of $\mathcal{F}$ and $u_i = v_i + \epsilon$ for some $\epsilon > 0$, if $\Omega \cap \varphi_f(X_0, \tau) \ne \emptyset$. The purpose to raise those upper bounds is to ensure that $\mathcal{F}_u$ has no intersection with the boundary of $\varphi_f(X_0, \tau)$ which is strictly over-approximated by $\mathfrak{F}_\tau = \mathcal{F}_o \backslash \mathcal{F}_u$. The detail is explained in the proof of Theorem 4.

Theorem 4. *The constrained flowpipe $\mathcal{F}_o$ is an over-approximation of $\varphi_f(X_0, \tau)$. For any* connected *subset Ω of $\mathcal{F}_u$, if $\varphi_f(X_0, \tau) \cap \Omega \ne \emptyset$, then Ω is an under-approximation of $\varphi_f(X_0, \tau)$.*

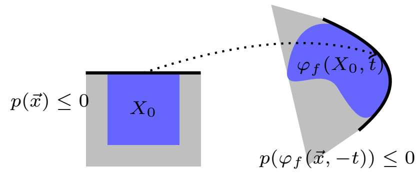


Fig. 3. Evolution of a constraint $p(\vec{x}) \le 0$

Proof. We first prove the over-approximation. Since the TM $(\phi_i(\vec{x}), [\ell_i, u_i])$ is an over-approximation of $p_i(\varphi_f(\vec{x}, -\tau))$ for $1 \le i \le m$, more precisely, we have that

$$\phi_i(\vec{x}) + \ell_i \le p_i(\varphi_f(\vec{x}, -\tau)) < \phi_i(\vec{x}) + u_i \tag{6}$$

for all $\vec{x} \in \varphi_f(X_0, \tau)$. Then for any $\vec{x} \in \varphi_f(X_0, \tau)$, the implication $p_i(\varphi_f(\vec{x}, -\tau)) \le 0 \to \phi_i(\vec{x}) + \ell_i \le 0$ holds, and hence $\varphi_f(X_0, \tau) \subseteq \{\vec{x} \in \mathbb{R}^n \mid \bigwedge_{i=1}^{m}(\phi_i(\vec{x}) + \ell_i \le 0)\}$. Since $\varphi_f(X_0, \tau) \subseteq \mathcal{F}$, we conclude that $\varphi_f(X_0, \tau) \subseteq \mathcal{F}_o$.

We turn to the under-approximation. The boundary of $\varphi_f(X_0, \tau)$ is given by

$$\partial\varphi_f(X_0, \tau) = \left(\bigcup_{i=1}^{m}\{\vec{x} \in \mathbb{R}^n \mid p_i(\varphi_f(\vec{x}, -\tau)) = 0\}\right) \cap \varphi_f(X_0, \tau)$$

Then the set $S = \{\vec{x} \in \mathbb{R}^n \mid \phi_i(\vec{x}) + u_i \le 0\}$ does not intersect $\partial\varphi_f(X_0, \tau)$. The reason is that for any $\vec{x} \in S$, if $\vec{x} \in \varphi_f(X_0, \tau)$ there is $p_i(\varphi_f(\vec{x}, -\tau)) < 0$ for all $1 \le i \le m$ by the inequality (6), otherwise $p_i(\varphi_f(\vec{x}, -\tau)) > 0$ for all $1 \le i \le m$. It is also the case for all subsets of S. Therefore, any *connected* subset of $S(t)$ either is entirely contained in $\varphi_f(X_0, \tau)$ or has no intersection with $\varphi_f(X_0, \tau)$. Since $\mathcal{F}_u \subseteq S$, we conclude that $\Omega \subset \varphi_f(X_0, \tau)$ for any connected set $\Omega \subseteq \mathcal{F}_u$ if $\varphi_f(X_0, \tau) \cap \Omega \ne \emptyset$. □

By taking t as an additional variable over a small time interval Δ, Theorem 4 can be extended to produce under- as well as over-approximation for the reachable set over Δ.

B. Methodologies to find an under-approximation

From Theorem 4, we need three steps to compute an under-approximation of the TM $\mathcal{F}$ for the reachable set $\varphi_f(X_0, \tau)$. The first step is to obtain a subset Ω of $\mathcal{F}_u$. It can be done by taking Ω as $\mathcal{F}_u$ or a subset of it. Then in the second step, we need to prove that Ω is connected, and ensure that the intersection $\Omega \cap \varphi_f(X_0, \tau)$ is nonempty in the third step. There are various ways to achieve this, we present some methods based on interval arithmetic. Again, the following methods can be extended to handle the reachable set over a time interval by taking an additional variable t.

Taking $\Omega = \mathcal{F}_u$. To limit the underestimation, we mainly consider the case that $\Omega = \mathcal{F}_u$. Then it requires to verify that $\mathcal{F}_u$ is a connected set. Since it is defined by a system of polynomial inequalities, to verify its connectedness is at least as hard as solving the same problem on a *basic closed semialgebraic set*, and it is intractable in general (see [39]). Fortunately, we could use the sufficient condition given in [21] on which the connectedness may possibly be proved efficiently. The idea is to find a *star point* in $\mathcal{F}_u$.

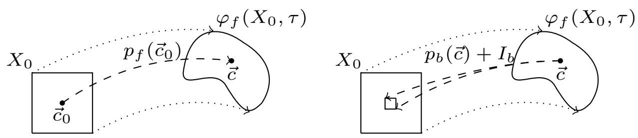


Fig. 4. **(L)** Compute a candidate star point $\vec{c}$, and **(R)** verify $\vec{c}$ is reachable

Given a set S, a point $s^* \in S$ is a *star point* if for any $s \in S$ the line segment connecting s^*, s is contained in S. Furthermore, if S has a star point then it is connected. To find a star point in $\mathcal{F}_u$, we may first compute a candidate point $\vec{c} \in \mathcal{F}_u$. Assume that the forward flowmap from X_0 to $\varphi_f(X_0,\tau)$ is over-approximated by $(p_f(\vec{x}), I_f)$. The point $\vec{c}$ can be computed as $p_f(\vec{c}_0)$ wherein $\vec{c}_0$ is an approximation of the geometric center of X_0. Fig. 4(**right**) shows the idea. When the TM order is sufficiently high, the inclusion $\vec{c} \in \mathcal{F}_u$ can be ensured. To verify that $\vec{c}$ is a star point in $\mathcal{F}_u$, as stated by Theorem 5 and Corollary 6, we may prove the unsatisfiability of the constraints

$$\phi_i(\vec{x}) + u_i = 0 \ \wedge \ \sum_{j=1}^{n}\left(\frac{\partial \phi_i}{\partial x_j}\cdot(x_j - c_j)\right) \leq 0$$

over $\vec{x} \in I_{\mathcal{F}}$ for all $1 \leq i \leq m$. This may be efficiently done by using *Interval Constraint Propagation (ICP)* [40].

Theorem 5 ([21])**.** *Given a set $S = \{\vec{x} \in D \subset \mathbb{R}^n \mid \psi(x) \leq 0\}$ wherein D is a convex set and ψ has continuous derivatives in D. For any $\vec{c} \in S$, if the constraint*

$$\psi(\vec{x}) = 0 \ \wedge \ \sum_{i=1}^{n}\left(\frac{\partial \psi}{\partial x_i}\cdot(x_i - c_i)\right) \leq 0$$

is unsatisfiable *for $\vec{x} \in D$, then $\vec{c}$ is a star point in S.*

Corollary 6. *Given a set $S = \{\vec{x} \in D \subset \mathbb{R}^n \mid \bigwedge_{i=1}^{m}(\psi_i(x) \leq 0)\}$ wherein D is a convex set and $\psi_1, \ldots, \psi_m$ have continuous derivatives in D. If $\vec{c}$ is a star point in $S_i = \{\vec{x} \in D \mid \psi_i(x) \leq 0\}$ for all $1 \leq i \leq m$, then it is also a star point in S.*

In the last step, we should prove that the intersection $\mathcal{F}_u \cap \varphi_f(X_0,\tau)$ is nonempty. To do so, we assume that the backward flowmap from X_0 to $\varphi_f(X_0,\tau)$ is over-approximated by the TM $(p_b(\vec{x}), I_b)$ based on the method in Sect. IV-B. Then, as we pointed out, I_b is safe for all states in (p_f, I_f). Hence we may check whether the interval $p_b(\vec{c}) + I_b$ is included by X_0. If so, then $\vec{c}$ is in $\varphi_f(X_0,\tau)$, and $\mathcal{F}_u$ is an under-approximation of $\varphi_f(X_0,\tau)$. The idea is illustrated in Fig. 4 (**Left**). It will be shown in Sect. VI that the three steps succeed in most of our experiments. A simple example is given as below.

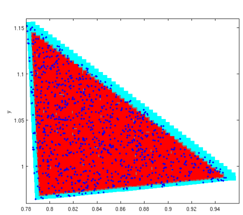


Fig. 5. Sets $\mathcal{F}_o$, $\mathcal{F}_u$

Example 7. *We consider the Moore-Greitzer model of a jet engine described in [41]. It is the continuous system defined by the following ODE.*

$$\begin{cases} \dot{x} &= -y - 1.5\cdot x^2 - 0.5\cdot x^3 - 0.5 \\ \dot{y} &= 3\cdot x - y \end{cases}$$

The initial set is given by the simplex

$$X_0 = \{(x,y) \in \mathbb{R}^2 \mid -x \leq -0.9 \wedge -y \leq -0.9 \wedge x+y-2 \leq 0\}$$

We try to compute the under-approximation $\mathcal{F}_u$ as well as the over-approximation $\mathcal{F}_o$ at $t = 0.04$ based on the TMs of the forward and backward flowmaps. Those TMs are computed on the interval enclosure $I_{X_0} = \{(x,y) \mid x \in [0.9, 1.1], y \in [0.9, 1.1]\}$ of X_0. An interval enclosure of the TM flowpipe $\mathcal{F}$ at time 0.04 is

$$I_{\mathcal{F}} = \left\{(x,y) \;\middle|\; \begin{array}{l} x \in [0.78063344, 0.95902894], \\ y \in [0.96380802, 1.1772562] \end{array}\right\}$$

By transferring the constraints defining X_0 to the time 0.04, we obtain the polynomials ϕ_1, ϕ_2, ϕ_3 and constant bounds $\ell_1, \ell_2, \ell_3, u_1, u_2, u_3$ in the definition of $\mathcal{F}_u$, $\mathcal{F}_o$:

$$\begin{aligned} \phi_1 = &-4.0810848e\text{-}2\cdot y - 9.9877519e\text{-}1\cdot x - 3.3480961e\text{-}5\cdot y^2 \\ &-2.4637920e\text{-}3\cdot x\cdot y - 6.0550400e\text{-}2\cdot x^2 - 3.6608001e\text{-}7\cdot y^3 \\ &-3.7006081e\text{-}5\cdot x\cdot y^2 - 1.4139012e\text{-}3\cdot x^2\cdot y - 2.3644942e\text{-}2\cdot x^3 \\ &-1.1520000e\text{-}7\cdot x\cdot y^3 - 7.8739201e\text{-}6\cdot x^2\cdot y^2 \\ &-2.4417472e\text{-}4\cdot x^3\cdot y - 3.2465277e\text{-}3\cdot x^4 \end{aligned}$$

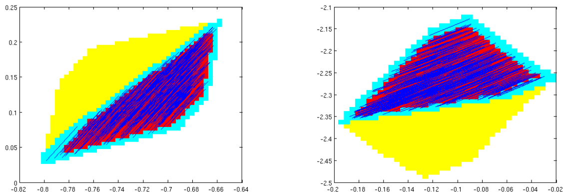
$$\begin{aligned} \phi_2 = &-1.0383459\cdot y + 1.2238309e\text{-}1\cdot x + 1.0022399e\text{-}6\cdot y^2 \\ &+9.8899199e\text{-}5\cdot x\cdot y + 3.6712367e\text{-}3\cdot x^2 + 7.6799999e\text{-}9\cdot y^3 \\ &+1.0828799e\text{-}6\cdot x\cdot y^2 + 5.4915839e\text{-}5\cdot x^2\cdot y + 1.3629942e\text{-}3\cdot x^3 \\ &+1.7280000e\text{-}7\cdot x^2\cdot y^2 + 7.2460800e\text{-}6\cdot x^3\cdot y + 1.2865439e\text{-}4\cdot x^4 \end{aligned}$$

$$\begin{aligned} \phi_3 = &\,1.0791566\cdot y + 8.7639208e\text{-}1\cdot x + 3.2478719e\text{-}5\cdot y^2 \\ &+2.3648927e\text{-}3\cdot x\cdot y + 5.6879162e\text{-}2\cdot x^2 + 3.5840000e\text{-}7\cdot y^3 \\ &+3.5923200e\text{-}5\cdot x\cdot y^2 + 1.3589852e\text{-}3\cdot x^2\cdot y \\ &+2.2281947e\text{-}2\cdot x^3 + 1.1519999e\text{-}7\cdot x\cdot y^3 + 7.7011199e\text{-}6\cdot x^2\cdot y^2 \\ &+2.3692863e\text{-}4\cdot x^3\cdot y + 3.1178732e\text{-}3\cdot x^4 \end{aligned}$$

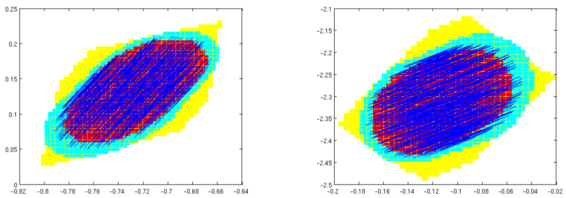
$$\begin{array}{lll} \ell_1 = 0.88000760, & \ell_2 = 0.90121569, & \ell_3 = -1.9812255 \\ u_1 = 0.88000946, & u_2 = 0.90121597, & u_3 = -1.9812233 \end{array}$$

We choose the point $\vec{c}_0 = (0.95, 0.95) \in X_0$ and its image under the forward flowmap approximation p_f is $\vec{c} = (0.82910752, 1.0171865)$ which can be easily verified by iSAT [42] as a star point in $\mathcal{F}_u$. Therefore $\mathcal{F}_u$ is connected. To ensure that the intersection of $\mathcal{F}_u$ and the reachable set at $t = 0.04$ is nonempty, we compute the interval image of $\vec{c}$ under the TM of the backward flowmap and it is contained in X_0. Hence, $\mathcal{F}_u$ is an under-approximation of the reachable set at $t = 0.04$. To visualize the sets $\mathcal{F}_u$ and $\mathcal{F}_o$, we plot the grids with a specified size that intersect $\mathcal{F}_o$ in cyan, and the grids that are covered by $\mathcal{F}_u$ in red. They are shown in Fig. 5. Besides, we also give the simulations [1] in blue.

To further investigate the performance of our method, we consider to under- as well as over-approximate a flowpipe over a time step. We set the step-size $\delta = 0.02$ and compute the TMs of forward and backward flowmaps for the time horizon $[0, 3]$. *In Fig. 6(a) and 6(b) respectively, we plot the set $\mathcal{F}_o$ in cyan, the set $\mathcal{F}_u$ in red and the unconstrained TM flowpipe $\mathcal{F}$ in yellow for t ranges in a time step. Additionally, we also plot the similar approximation sets in Fig. 6(c) and 6(d) for the ellipsoidal initial set $\{(x,y) \in \mathbb{R}^2 \mid (x-1)^2 + (y-1)^2 \leq 0.01\}$.*



(a) $t \in [0.98, 1]$ from the simplex (b) $t \in [2.98, 3]$ from the simplex



(c) $t \in [0.98, 1]$ from the ellipsoid (d) $t \in [2.98, 3]$ from the ellipsoid

Fig. 6. Reachable set under- and over-approximations for the jet engine model. Numerical simulations are given in blue.

Other methods. The under-approximate set Ω may also be defined as a geometric object, such as a set of connected boxes or polytopes. To do so, we may follow the methods presented in [43] and [44]. The main idea is to first randomly generate a set of points in $\mathcal{F}_u$, and then successively bloat each point to a set which is made as large as possible but still contained in $\mathcal{F}_u$. Then Ω is the union of those sets which are connected to the others. To verify that Ω intersects the exact reachable set $\varphi_f(X_0, \tau)$, we may just compute the images of those random points under the backward TM map, if at least one of them is in X_0, then Ω is an under-approximation of $\varphi_f(X_0, \tau)$.

VI. Experiments

We implemented our approach based on the TM library of FLOW* [22]. The experiments are described as follows.

System models. We select 9 non-linear continuous systems whose dimensions range from 2 to 7. In order to evaluate our method on tough examples, some chaotic systems are also included. They are Lorenz system, Rössler attractor and Shimizu-Morioka system [45].

Initial sets. We want to handle the initial sets defined by polynomial constraints. Such a set is usually not TM definable but the TM forward and backward flowmaps can be computed on a TM of it. In our experiments, we consider two initial sets for each system: a *simplex* defined by $S_0 = \{\vec{x} \in \mathbb{R}^n \,|\, (\bigwedge_{i=1}^{n}(-x_i + a_i - r \leq 0)) \wedge (\sum_{i=1}^{n} x_i - \sum_{i=1}^{n} a_i) \leq 0\}$, and an *ellipsoid* defined by $E_0 = \{\vec{x} \in \mathbb{R}^n \,|\, \sum_{i=1}^{n}(x_i - a_i)^2 \leq r^2\}$. The constants $\vec{a}$ and r for the systems are listed as follows: *jet engine*: $\vec{a} = (1, 1)$, $r = 0.1$; *Brusselator*: $\vec{a} = (0.95, 0.05)$, $r = 0.05$; *Rössler attractor*: $\vec{a} = (0, -8.4, 0)$, $r = 0.1$; *Lorentz system*: $\vec{a} = (15, 15, 36)$, $r = 0.01$; *Shimizu-Morioka system*: $\vec{a} = (15, 15, 36)$, $r = 0.01$; *Lotka-Volterra system [46]*: $\vec{a} = (0.5, 0.5, 0.5, 0.5)$, $r = 0.1$; *coupled Van-der-Pol system*: $\vec{a} = (1, 1, 1, 1)$, $r = 0.1$; *Watt steam governor [47]*: $\vec{a} = (0, 0, 0, 0, 0)$, $r = 0.1$; *biological system [48]*: $\vec{a} = (0.1025, \ldots, 0.1025)$, $r = 0.0025$. Notice that these initial sets are at least in the same scale as those typically used in evaluating verified integration methods. Also, we evaluate the accuracy of an approximation at the end of the time horizon.

[1]A numerical simulation is only an approximation whose error bound is not guaranteed. However, it usually can be made very accurate.

TABLE I
EVALUATION OF THE APPROXIMATIONS FOR $\vec{x}(T)$ WITH INITIAL SETS AS *simplices*. **VAR**: # VARIABLES, $\boldsymbol{\delta}$: STEP-SIZES, $\boldsymbol{k}$: TM ORDERS, **TIME**: TOTAL RUNNING TIME.

#	systems	var	T	δ	k	time (s)	$\gamma_{\min}$
1	jet engine	2	4	0.02	4	56	∼0.8
2	jet engine	2	5	0.02	4	71	∼0.75
3	Brusselator	2	3	0.02	4	55	∼0.7
4	Brusselator	2	4	0.02	4	89	∼0.55
5	Rössler	3	1.5	0.01	5	165	∼0.5
6	Rössler	3	1.6	0.01	5	178	Fail
7	Lorenz	3	0.5	0.01	5	35	∼0.65
8	Lorenz	3	0.6	0.01	5	45	∼0.35
9	Shimizu-Morioka	3	1	0.01	5	58	∼0.7
10	Shimizu-Morioka	3	1.2	0.01	5	69	∼0.3
11	Lotka-Volterra	4	1	0.01	4	297	∼0.4
12	coupled Van-der-Pol	4	4	0.01	4	118	∼0.45
13	steam governor	5	2.5	0.01	5	16	∼0.35
14	biological system	7	0.2	0.002	3	632	∼0.25

Results. Since the exact accuracy evaluation is very hard, we intuitively only measure the widths w.r.t. a set of directions. Given an over-approximation S_o, an under-approximation S_u and a set of vectors V, we conservatively compute the widths of S_o, S_u w.r.t. each $\vec{v} \in V$: $\gamma_o(\vec{v}) \geq |\max\{\vec{v}^T \cdot \vec{x} \,|\, \vec{x} \in S_o\} + \max\{-\vec{v}^T \cdot \vec{x} \,|\, \vec{x} \in S_o\}|$ and $\gamma_u(\vec{v}) \leq |\max\{\vec{v}^T \cdot \vec{x} \,|\, \vec{x} \in S_u\} + \max\{-\vec{v}^T \cdot \vec{x} \,|\, \vec{x} \in S_u\}|$. Then we compute the minimum width ratio $\gamma_{\min} = \min\{\gamma_u(\vec{v})/\gamma_o(\vec{v}) \,|\, \vec{v} \in V\}$ which gives an intuitive evaluation on the accuracy, i.e., the larger the value the better the approximation. In Table I and II, we present the experimental results on our benchmarks. The over- and under-approximations are the sets $\mathcal{F}_o$ and $\mathcal{F}_u$ respectively at time T. The vectors are selected along the dimensions (axis-aligned). It can be seen that our method found a valid under-approximation in most cases, and even could handle chaotic behaviors in reasonably long time horizons.

On one hand, our prototype produces interesting results on most of the benchmark examples. Since interval (as well as TM) based integration methods are very sensitive to the size of the initial set and the length of the time horizon, our under-approximation method underperforms on hard case studies, such as the test #6. However, there is still a lot of room for engineering improvements to our prototype implementations.

Acknowledgments. This work was supported by the DFG project HyPro, and in part, by the US National Science Foundation (NSF) under award # CNS-0953941. All opinions expressed are those of the authors and not necessarily of DFG or NSF.

References

[1] S. Sankaranarayanan, H. Sipma, and Z. Manna, “Constructing invariants for hybrid systems,” in *Proc. HSCC’04*, ser. LNCS, vol. 2993. Springer, 2004, pp. 539–554.

[2] S. Gulwani and A. Tiwari, “Constraint-based approach for analysis of hybrid systems,” in *Proc. CAV’08*, ser. LNCS, vol. 5123. Springer, 2008, pp. 190–203.

TABLE II
EVALUATION OF THE UNDER-APPROXIMATIONS FOR $\vec{x}(T)$ WITH INITIAL SETS AS *ellipsoids*. LEGENDS: SEE TABLE I.

#	systems	var	T	δ	k	time (s)	$\gamma_{\min}$
1	jet engine	2	4	0.02	4	45	∼0.8
2	jet engine	2	5	0.02	5	185	∼0.7
3	Brusselator	2	3	0.02	4	43	∼0.65
4	Brusselator	2	4	0.01	4	138	∼0.5
5	Rössler	3	1.5	0.01	5	153	∼0.4
6	Rössler	3	1.6	0.01	5	167	Fail
7	Lorenz	3	0.5	0.01	5	31	∼0.5
8	Lorenz	3	0.6	0.01	5	44	∼0.2
9	Shimizu-Morioka	3	1	0.01	5	55	∼0.5
10	Shimizu-Morioka	3	1.2	0.01	5	67	∼0.1
11	Lotka-Volterra	4	1	0.01	4	261	∼0.25
12	coupled Van-der-Pol	4	4	0.01	4	105	∼0.3
13	steam governor	5	2.5	0.01	5	16	∼0.2
14	biological system	7	0.2	0.002	3	581	∼0.15

[3] A. Platzer and E. Clarke, "Computing differential invariants of hybrid systems as fixedpoints," *FMSD*, vol. 35, no. 1, pp. 98–120, 2009.

[4] T. A. Henzinger, B. Horowitz, R. Majumdar, and H. Wong-Toi, "Beyond HYTECH: Hybrid systems analysis using interval numerical methods," in *Proc. HSCC'00*, ser. LNCS, vol. 1790. Springer, 2000, pp. 130–144.

[5] G. Frehse, "PHAVer: Algorithmic verification of hybrid systems past HyTech," in *HSCC*, ser. LNCS, vol. 2289. Springer, 2005, pp. 258–273.

[6] T. Dang, O. Maler, and R. Testylier, "Accurate hybridization of nonlinear systems," in *Proc. HSCC '10*. ACM, 2010, pp. 11–20.

[7] A. Chutinan and B. Krogh, "Computing polyhedral approximations to flow pipes for dynamic systems," in *Proc. CDC'98*. IEEE, 1998.

[8] E. Asarin, T. Dang, and O. Maler, "The d/dt tool for verification of hybrid systems," in *CAV*, ser. LNCS, vol. 2404. springer, 2002, pp. 365–370.

[9] A. Girard, "Reachability of uncertain linear systems using zonotopes," in *Proc. HSCC'05*, ser. LNCS, vol. 3414. Springer, 2005, pp. 291–305.

[10] C. Le Guernic and A. Girard, "Reachability analysis of hybrid systems using support functions," in *Proc. CAV'09*, ser. LNCS, vol. 5643. Springer, 2009, pp. 540–554.

[11] G. Frehse, C. Le Guernic, A. Donzé, S. Cotton, R. Ray, O. Lebeltel, R. Ripado, A. Girard, T. Dang, and O. Maler, "SpaceEx: Scalable verification of hybrid systems," in *Proc. CAV'11*, ser. LNCS, vol. 6806. Springer, 2011, pp. 379–395.

[12] I. M. Mitchell and C. Tomlin, "Level set methods for computation in hybrid systems," in *Proc. HSCC'00*, ser. LNCS, vol. 1790. Springer, 2000, pp. 310–323.

[13] S. Osher and R. Fedkiw, *Level Set Methods and Dynamic Implicit Surfaces*. Springer, 2002.

[14] I. M. Mitchell and J. A. Templeton, "A toolbox of hamilton-jacobi solvers for analysis of nondeterministic continuous and hybrid systems," in *Proc. HSCC'05*, ser. LNCS, vol. 3414. Springer, 2005, pp. 480–494.

[15] N. S. Nedialkov, K. R. Jackson, and G. F. Corliss, "Validated solutions of initial value problems for ordinary differential equations," *Applied Mathematics and Computation*, vol. 105, no. 1, pp. 21–68, 1999.

[16] M. Berz and K. Makino, "Verified integration of ODEs and flows using differential algebraic methods on high-order Taylor models," *Reliable Computing*, vol. 4, pp. 361–369, 1998.

[17] N. Ramdani and N. S. Nedialkov, "Computing reachable sets for uncertain nonlinear hybrid systems using interval constraint-propagation techniques," *Nonlinear Analysis: Hybrid Systems*, vol. 5, no. 2, pp. 149–162, 2011.

[18] P. Prabhakar and M. Viswanathan, "A dynamic algorithm for approximate flow computations," in *Proc. HSCC'11*. ACM, 2011, pp. 133–142.

[19] X. Chen, E. Ábrahám, and S. Sankaranarayanan, "Taylor model flowpipe construction for non-linear hybrid systems," in *Proc. RTSS'12*. IEEE, 2012, pp. 183–192.

[20] P. Prabhakar, P. S. Duggirala, S. Mitra, and M. Viswanathan, "Hybrid automata-based cegar for rectangular hybrid systems," in *Proc. VMCAI'13*, ser. LNCS, vol. 7737. Springer, 2013, pp. 48–67.

[21] N. Delanoue, L. Jaulin, and B. Cottenceau, "Using interval arithmetic to prove that a set is path-connected," *Theoretical Computer Science*, vol. 351, no. 1, pp. 119 – 128, 2006.

[22] X. Chen, E. Ábrahám, and S. Sankaranarayanan, "Flow*: An analyzer for non-linear hybrid systems," in *Proc. of CAV'13*, ser. LNCS, vol. 8044. Springer, 2013, pp. 258–263.

[23] A. Girard, C. Le Guernic, and O. Maler, "Efficient computation of reachable sets of linear time-invariant systems with inputs," in *Proc. HSCC'06*, ser. LNCS, vol. 3927. Springer, 2006, pp. 257–271.

[24] C. Le Guernic, "Reachability analysis of hybrid systems with linear continuous dynamics," Ph.D. dissertation, Université Joseph Fourier, 2009.

[25] G. Frehse, B. H. Krogh, and R. A. Rutenbar, "Verifying analog oscillator circuits using forward/backward abstraction refinement," in *Proc. DATE'06*, 2006, pp. 257–262.

[26] I. M. Mitchell, "Comparing forward and backward reachability as tools for safety analysis," in *HSCC*, ser. LNCS, vol. 4416. Springer, 2007, pp. 428–443.

[27] E. Gardeñes, M. Sainz, L. Jorba, R. Calm, R. Estela, H. Mielgo, and A. Trepat, "Modal intervals," *Reliable Computing*, vol. 7, no. 2, pp. 77–111, 2001.

[28] E. Goubault and S. Putot, "Under-approximations of computations in real numbers based on generalized affine arithmetic," in *Proc. SAS'07*, ser. LNCS, vol. 4634. Springer, 2007, pp. 137–152.

[29] E. Goubault, O. Mullier, and S. P. amd M. Kieffer, "Inner approximated reachability analysis," 2014, to Appear (April 2014).

[30] B. Xue, "Computing rigor quadratic lyapunov functions and under-approximate reachable sets for ordinary differential equations," Ph.D. dissertation, Beihang University, 2013.

[31] S. Gao, J. Avigad, and E. Clarke, "δ-complete decision procedures for satisfiability over the reals," in *IJCAR*, ser. LNCS, vol. 7365, 2012, pp. 286–300.

[32] S. Gao, S. Kong, and E. M. Clarke, "dReal: An SMT solver for nonlinear theories over the reals," in *CADE*, ser. LNCS, vol. 7898. Springer, 2013, pp. 208–214.

[33] S. Gao, S. Kong, and E. Clarke, "Satisfiability modulo ODEs," in *FMCAD*, Oct 2013, pp. 105–112.

[34] J. D. Meiss, *Differential Dynamical Systems*. SIAM publishers, 2007.

[35] K. Makino and M. Berz, "Taylor models and other validated functional inclusion methods," *J. Pure and Applied Mathematics*, vol. 4, no. 4, pp. 379–456, 2003.

[36] R. E. Moore, R. B. Kearfott, and M. J. Cloud, *Introduction to Interval Analysis*. SIAM, 2009.

[37] R. J. Lohner, "Computation of guaranteed enclosures for the solutions of ordinary initial and boundary value problems," in *Computational ordinary differential equations*, 1992, pp. 425–435.

[38] K. Makino and M. Berz, "Suppression of the wrapping effect by taylor model-based verified integrators: Long-term stabilization by preconditioning," *International Journal of Differential Equations and Applications*, vol. 10, no. 4, pp. 353 – 384, 2005.

[39] S. Basu, R. Pollack, and M.-F. Roy, *Algorithms in Real Algebraic Geometry*. Springer, 2006.

[40] F. Benhamou and L. Granvilliers, "Continuous and interval constraints," in *Handbook of Constraint Programming*. Elsevier, 2006, pp. 571–590.

[41] E. M. Aylward, P. A. Parrilo, and J.-J. E. Slotine, "Stability and robustness analysis of nonlinear systems via contraction metrics and SOS programming," *Automatica*, vol. 44, no. 8, pp. 2163 – 2170, 2008.

[42] M. Fränzle, C. Herde, T. Teige, S. Ratschan, and T. Schubert, "Efficient solving of large non-linear arithmetic constraint systems with complex Boolean structure," *Journal on Satisfiability, Boolean Modeling and Computation*, vol. 1, pp. 209–236, 2007.

[43] S. Sankaranarayanan, A. Chakarov, and S. Gulwani, "Static analysis for probabilistic programs: Inferring whole program properties from finitely many paths," in *Proc. PLDI'13*, vol. 48. ACM, 2013, pp. 447–458.

[44] A. Kanade, R. Alur, F. Ivancic, S. Ramesh, S. Sankaranarayanan, and K. C. Shashidhar, "Generating and analyzing symbolic traces of simulink/stateflow models," in *Proc. CAV'09*, ser. LNCS, vol. 5643. Springer, 2009, pp. 430–445.

[45] A. L. Shil'nikov, "On bifurcations of the Lorenz attractor in the Shimizu-Morioka model," *Phys. D*, vol. 62, no. 1-4, pp. 338–346, 1993.

[46] J. A. Vano, J. C. Wildenberg, M. B. Anderson, J. K. Noel, and J. C. Sprott, "Chaos in low-dimensional Lotka-Volterra models of competition," *Nonlinearity*, vol. 19, no. 10, pp. 2391–2404, 2006.

[47] J. Sotomayor, L. F. Mello, and D. de Carvalho Braga, "Bifurcation analysis of the Watt governor system," *Comput. Appl. Math.*, vol. 26, no. 1, 2007.

[48] E. Klipp, R. Herwig, A. Kowald, C. Wierling, and H. Lehrach, *Systems Biology in Practice: Concepts, Implementation and Application*. Wiley-Blackwell, 2005.